UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

“PROPUESTA DE NORMAS, POLÍTICAS Y PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE REDES DE COMPUTADORAS (CON ENFOQUE BASADO EN PROCESOS DE CALIDAD)”.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

CRISTIAN AMAURY LÓPEZ DEHESA

EDGAR LUCIANO PALACIOS

DIRECTOR: ING. HERIBERTO OLGUÍN ROMO

CIUDAD UNIVERSITARIA, 2006.

Agradecimientos.

“A todas aquellas personas que han creído en mí y en la culminación de este sueño. A todas aquellas personas que de alguna u otra manera han formado parte de esta aventura que concluye hoy. A todas aquellas personas que siempre han estado ahí para levantarme cada vez que he caído, gracias por estar ahí”.

A mi familia, a mi madre Yolanda Dehesa, a mi padre Faustino López y a mi hermano Caleb López, gracias por llegar conmigo hasta al final de la carrera y hacerla más amena día con día.

A ti mamá por darme la fuerza y la entereza para afrontar cada día que he vivido, no sabes cuánto te quiero. Gracias por estar junto a mí en todos los momentos buenos y malos por los que he pasado; por ser siempre la persona que más ha creído en mí, este trabajo es para ti mamá.

A ti papá por enseñarme que no hay cosa más sagrada que el trabajo, por enseñarme desde pequeño a no rehuir a mis problemas y enfrentarme siempre a ellos. Gracias por estar ahí siempre en los momentos más necesarios de mi vida.

A mi hermano por hacerme los días más felices desde que tengo noción de la vida. Gracias por el apoyo y el soporte que me has dado durante todo lo que hemos realizado juntos y por todo lo que falta porvenir en el futuro.

A Miriam por ser muchas veces fuente de inspiración para hacer cosas que nunca me hubiera propuesto hacer. Por ser mi mejor amiga, nunca te terminaría de agradecer todo lo que has hecho por mí.

A mis otros padres Alicia y Pedro, que sin ellos y su apoyo nunca hubiera llegado hasta donde estoy ahora, por todos los días de mi vida que he pasado con ustedes mil gracias.

A la memoria de mis abuelos Catalina, Cruz, Maurilio y Rodolfo, que sin ustedes no hubiera sido posible el que estuviera aquí. Siempre he pensado que están allá arriba guiando mi camino y que nunca han dejado de existir, mientras siga creyendo en ustedes siempre estarán aquí conmigo.

A mi compañero de tesis y gran amigo de la carrera Edgar Luciano Palacios por el esfuerzo y la dedicación a este trabajo, mil gracias.

Cristian Amaury López Dehesa.
Septiembre de 2006.

Agradecimientos

Agradezco a mis padres Elia y Juan por el apoyo que siempre me brindaron; por que en mis logros y fracasos ahí estuvieron, por que mis alegrías y desvelos los hicieron suyos, por enseñarme que en la vida lo que más vale es la honestidad y el trabajo duro. Por eso y mucho más les doy todo mi amor y mi respeto.

A mis tías Paula, Josefina y Martina, les doy las gracias por su comprensión y por ser, cada una a su modo, como una madre para mí.

A mi tío Carlos, por que parte de él me hizo entrar a esta universidad y a esta mi facultad de Ingeniería.

A Erick, le doy las gracias por su apoyo, por su compresión y por tener en él más que un hermano, un amigo. A Magda su esposa, le agradezco por apoyarme igualmente.

A Salvador, por todas esas charlas y todos los momentos que me ayudaron a formar mi carácter, ¡Gracias hermano!

A Yesenia y Yusdivia, por que siempre seré Edgarín para ellas, por su cariño y su ejemplo, por que para mi son mis hermanas.

A mis niñas Karen y Sharon, por que cuando estoy cansado y a punto de rendirme, siempre me animan con sus sonrisas y su cariño.

A mi compañero y amigo Amaury por su amistad y franqueza, por su apoyo y determinación, por que sin él no hubiera sido posible terminar este trabajo.

A todo los profesores que me enseñaron que el ser ingeniero va más allá de los números y las ecuaciones.

Mi reconocimiento a Gilbertito, ¡Que razón tenias!

Agradezco a nuestro asesor de tesis, Heriberto Olguín Romo por todo su apoyo.

A todos mis compañeros y amigos que conocí a lo largo de la carrera, gracias.

Por supuesto, no puedo dejar de agradecer a mi Universidad la grandiosa UNAM, por que más allá de darme una educación, me dio un estilo de vida, ¡Gracias!

Edgar Luciano Palacios
Septiembre de 2006

ÍNDICE

CAPÍTULO 3: NORMATIVIDAD PARA REDES DE COMPUTADORAS

CAPÍTULO 4: POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE REDES DE COMPUTADORAS

CAPÍTULO 5: INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA

INTRODUCCIÓN

Hoy en día cualquier empresa moderna necesita ser más competitiva, debe poder adaptarse y evolucionar conforme los nuevos requerimientos que el cliente exige, de la misma manera, debe contar con una normatividad adecuada que le permita realizar estos cambios de la forma más eficaz, sin comprometer en lo absoluto la calidad de su servicio.

Muchos de los problemas que aquejan hoy en día a las instituciones o empresas mexicanas, son causados debido al poco interés que se muestra en el desarrollo e implementación de una documentación adecuada; este problema se ve reflejado en la mayoría de los procesos que intervienen dentro de la cadena productiva de las mismas. Si a eso agregamos el poco o total desconocimiento de términos tales como procedimientos, normas o calidad, nos lleva a un panorama poco alentador en cuanto al nivel competitivo que puedan ofrecer las empresas en sus diferentes ámbitos.

La idea principal, es contar con las certificaciones en los procedimientos que se realizan dentro de una organización; pero el fin de tales certificaciones no es simplemente que las empresas lideres sean evaluadas y aprobadas por algún organismo certificador; la verdadera tarea consiste en sostener el nivel al que se llegó durante todo el trabajo de certificación, y mantener una mejora continua en cada procedimiento por el que se fue certificado. Por ello, cada vez se hace más importante el contar con políticas, normas y procedimientos, que nos permitan obtener fácil acceso a la información y sobretodo que ayuden al personal a lograr niveles mayores de eficiencia y calidad.

Siendo más específicos, en el campo de las redes de computadoras, vemos con interés que no existe una normatividad común para la implantación de éstas, lo cual implica una baja calidad en su instalación; existe además, abundante información acerca de la administración y mantenimiento de la red que muchas veces es poco clara y concisa; así como, problemas que inician desde la planeación e instalación de las redes de computadoras, lo que no permite aprovechar en su totalidad todo su potencial.

Este trabajo se ha escrito con el propósito de proveer una propuesta de políticas, normas y procedimientos para la implementación de redes de computadoras y trata de cubrir todos los aspectos del establecimiento de una red, siempre tomando en cuenta la orientación hacia la calidad, es decir, cada propuesta tiene las características para poder aplicar un enfoque basado en procesos, que en el argot de calidad, es la esencia de la ISO 9001:2000.

El capítulo 1 se encarga de poner en claro conceptos básicos acerca de las políticas, las normas y los procedimientos, que es parte fundamental del presente trabajo; no es posible hablar de estos términos sin tener plena conciencia de lo que son, a qué se refieren y cómo se aplican en una organización.

El capítulo 2 es un breve repaso acerca de las redes de computadoras, cómo se constituyen, cómo se estructuran, las topologías que se usan y los diferentes tipos que existen. Al final de este capítulo, se cuenta con una descripción de lo que es el modelo OSI y el enfoque TCP/IP y cómo interactúan sus diferentes capas.

En el capítulo 3 se muestra una serie de normas, protocolos y estándares para redes de computadoras, ya que es esencial conocer la manera en que se trabaja internacionalmente y cuáles son los requisitos que hay que cubrir para poder instalar una red en cuanto a comunicación, instalación y seguridad.

El capítulo 4 es la esencia de este trabajo de tesis, este capítulo presenta las propuestas de políticas, normas y procedimientos para la implementación de redes de computadoras; se inicia con la adquisición de los bienes informáticos y de comunicaciones, mobiliario y servicios de telecomunicaciones, así como de la contratación del personal; seguimos con la instalación, desde su planeación, pasando por el diseño de la red, el local de instalación y la instalación eléctrica, hasta la distribución de la red, el cableado estructurado y la conexión de WIRELES (redes inalámbricas). Continuamos con la seguridad, para los equipos de cómputo, en las telecomunicaciones y del uso de los recursos de la red. El mantenimiento es parte importante y se tiene la planeación de éste para el equipo de red y

de comunicaciones, para la información y documentación y por supuesto no pueden faltar cláusulas para el contrato de mantenimiento por terceras personas. Finalmente se cuenta con la observancia por los usuarios y por los administradores, considerando la autorización para el uso de la red, el acceso para los usuarios y la seguridad de la red.

En lo que respecta al capítulo 5, este trabajo cuenta con una introducción a la auditoría informática, explicando lo que es una auditoría, los tipos de auditoría que existen, sus lineamientos generales, y lo que es una auditoría informática.

Hacemos uso de apéndices que tienen como tarea crear mayor énfasis en algunos aspectos mencionados durante el trabajo de tesis, y que muestran de manera sencilla la elaboración de documentos para la administración y la auditoría de las redes de computadoras.

Finalmente, sabemos que cada empresa u organización es diferente, por tal motivo, la intención de este trabajo no es imponer un estilo o una regla en cuanto a la instalación de redes de computadoras; sino crear un precedente que ayude e incluso sirva de guía para las diferentes empresas, organizaciones o particulares que deseen instalar una red, y que tengan como expectativa obtener una o varias certificaciones en los diversos procedimientos que se llevan a cabo.

Atte. Los autores

Conceptos básicos sobre políticas, normas y procedimientos

Capítulo 1

CAPÍTULO 1

CONCEPTOS BÁSICOS SOBRE POLÍTICAS, NORMAS Y PROCEDIMIENTOS

1. Introducción

Toda empresa tiene sistemas de gestión, los cuales rigen la manera en que se realizan las actividades dentro de la organización, también, cuenta con políticas que regulan las actividades a que se han de enfocar. Sin embargo:

- rara vez están claramente definidas.
- generalmente, no son comunicadas ni entendidas por los integrantes de la empresa.
- con frecuencia no están alineadas con la visión de la empresa.
- no siempre se generan a partir de ellas objetivos claros.
- en la mayoría de los casos, no son revisadas periódicamente.

En general se oyen frases como: “la empresa debe mejorar su rentabilidad”; “la empresa debe ser más competitiva”. Pero qué son estas frases sin un elemento clave llamado “compromiso”.

Si reescribimos la primera frase de la siguiente manera: “La empresa mejorará continuamente su rentabilidad”. Ahora, contiene el compromiso de mejorar la rentabilidad, la palabra que define el compromiso es: “mejorará”. Ahora sí la podemos llamar una política.

Podemos ampliar y orientar aun más esta frase de la siguiente manera:

“La empresa mejorará continuamente su rentabilidad para asegurar su competitividad en el negocio y aumentar la satisfacción de sus accionistas.”

No es tan difícil definir las políticas, el problema es llevarlas a cabo, como bien lo dice la premisa de la norma ISO[(1)] 9001:2000, “escribe lo que haces y haz lo que dices”. De nada sirven las políticas en la empresa si éstas no son comunicadas y comprendidas por todos los integrantes que laboran ahí, es decir, cada empleado debe ser capaz de analizar y de describir, con sus propias palabras, de qué manera su trabajo contribuye al cumplimiento de las políticas de la empresa.

Para ello es necesario “documentar” las políticas de la empresa, ya que sólo se alcanzarán los objetivos si el personal incorpora las políticas a su manera de pensar y lo refleja en sus actitudes. La alta dirección debe ser plenamente consciente de su papel en

[1] ISO: Organización Internacional de Estandarización.

este proceso, bajo la premisa de que no hay posibilidades de éxito si no se "predica con el ejemplo".

1.1. Conceptos básicos sobre políticas, normas y procedimientos y su relación con la Calidad

1.1.1. Conceptos elementales

Como punto de inicio, es indispensable establecer una serie de conceptos que serán la base del buen entendimiento de esta propuesta y en el desarrollo integral de las empresas, así pues, es necesario que todo el personal conozca y sepa interpretarlos de la manera más adecuada y que su transición hacia el ambiente laboral sea lo más naturalmente posible.

Políticas

A diferencia de lo que muchas personas conocen, las políticas van a ayudar a la organización a establecer un orden, van ayudarla a crecer. Una primera aproximación hacia este término nos la da el diccionario de la real academia de la lengua, el cual dice de manera textual:

"Política: Arte o traza con que se conduce un asunto o se emplean los medios para alcanzar un fin determinado. Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado[(2)]"

No es para menos que puesta así la definición, sea poco o casi incomprensible, primero nos habla acerca de un arte o traza, entonces las políticas por sí solas son un arte, pero se sabe que éste es sumamente subjetivo, lo que nos conduce hacia las personas, las políticas entonces son propias de un grupo de sujetos que las hacen y las llevan a cabo para alcanzar un fin determinado.

Lo más curioso hasta aquí es que aún no tenemos una definición clara de lo que es una política, pero quizás la segunda parte de la definición nos aclare más el panorama, reinterpretándola nos dice que las políticas "son en esencia leyes y reglamentos que gobiernan las operaciones"

Por lo tanto las políticas son:

1. Un arte.
2. Un modo de actuar que acatan las personas.
3. Directrices.
4. Pertenecientes a cada organización.

[2] Diccionario de la Real Academia Española en línea [www.rae.es]

Las políticas no son:

5. Un instructivo.
6. Una recomendación.
7. Un castigo.
8. Una sanción, aunque pueden contenerlas.

Normas

Es notorio que siempre que uno oye esta palabra, no duda en referirla hacia cosas tales como leyes o algo relacionado con preceptos jurídicos, ya que aunque si bien es cierto que su verdadera magnitud e importancia se mide en dicho campo; en el presente trabajo se abordará más desde la perspectiva humanística, hacia las personas y los grupos de trabajo que de ella se van a desprender. Así pues, la primera definición viene del diccionario de la real academia de la lengua española:

"Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc. Mandato u orden que el superior hace observar y guardar al inferior o súbdito[(3)]".

Podemos establecer en primer término que las normas son las reglas de nuestro trabajo, así por ejemplo, una norma de salud, podría ser cuando se prohíbe fumar en edificio gubernamentales.

Generalmente son una referencia específica hacia algo, no son tan genéricas como para ser consideradas un arte como las políticas, pero sí van a tener un papel importante dentro de la organización, ya que van a ser los patrones que se deben seguir durante el desarrollo de alguna tarea, no al grado de mencionar los pasos a seguir, pero sí de marcar el cómo se debe hacer.

Por lo tanto las normas son:

1. Reglamentos.
2. Patrones estándar de las actividades.

Las normas no son:

3. Instructivos por pasos.
4. Planes de contingencia.

Procedimientos

Todas las personas deben saber cómo hacer las cosas, si no, que caso tendría el definir políticas y normas suntuosas, cuando no se sabe como actuar. Es aquí donde la organización debe contar con una metodología especializada, una serie de pasos que nos

[3] Idem 2

digan exactamente cómo se hace alguna actividad o tarea. Nos estamos refiriendo a los llamados procedimientos, el diccionario de la real academia de la lengua española los define como:

"Acción de proceder. Método de ejecutar algunas cosas, actuación por trámites judiciales o administrativos[4]"

Veamos ahora como lo define la norma ISO 9000:2000, concerniente a vocabulario:

"Forma especificada para llevar a cabo una actividad o un proceso[5]"

Claramente podemos ver que ambas definiciones hacen referencia hacia una forma de proceder, solo que en la segunda, aparece una palabra fundamental que la hace tener otro enfoque: "especificada". Día a día las actividades que realizamos parecen ser iguales, desde el momento en que nos levantamos hasta el momento de ir a la oficina y regresar a casa, pero esto no es así, ya que no seguimos un procedimiento especificado y alguna de esas actividades pueden ser omitidas ya sea por olvido o por negligencia por parte de nosotros. Si nuestro trabajo consiste en instalar redes de computadoras, es obvio que cualquier omisión que podamos tener puede afectar el servicio que preste la red que instalamos, para ello, se hace necesario el contar con procedimientos documentados y sistematizados, que nos permitan anular por completo las posibles variaciones que puedan mermar nuestro trabajo, a modo de obtener una mayor eficiencia y seguridad en su realización.

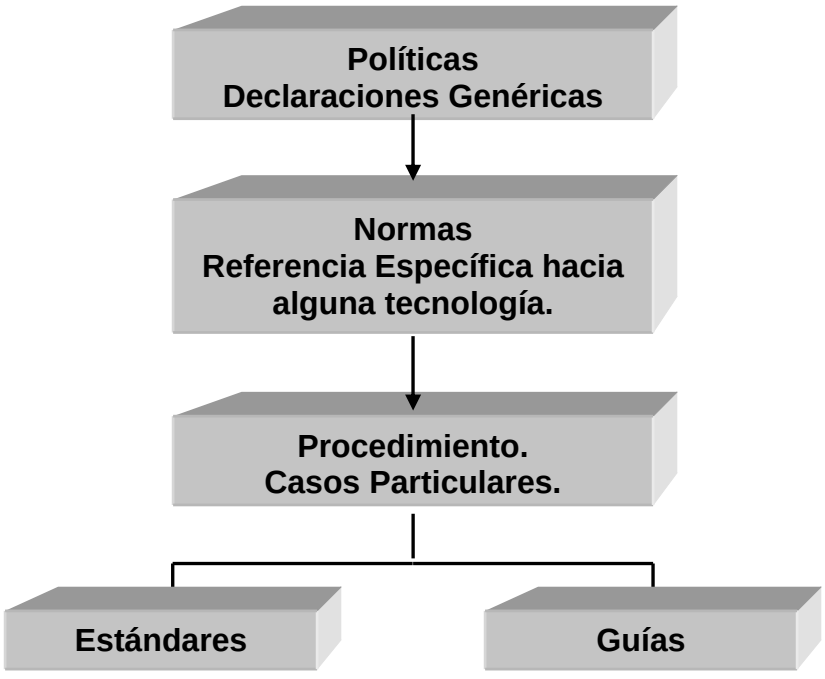


Figura 1.1 Jerarquización de los conceptos.

[4] Idem 2
[5] Norma Oficial Mexicana NMX-CC-9000-IMNC-2000, concerniente a vocabulario

Calidad

Muchas veces uno ha oido la frase, “haz las cosas bien” o cosas tales como “este aparato no es de muy buena calidad”. Y bueno, no es para menos, en un mundo tan competido por el mercado, el consumidor siempre va a preferir irse con la empresa que le deje una mayor satisfacción por su dinero, es aquí cuando términos tales como calidad toman su verdadero significado, pero, ¿en verdad sabemos que significa la palabra calidad?. Veamos, un primer acercamiento nos lo dá el real diccionario de la lengua española:

“Propiedad o conjunto de propiedades inherentes a algo, que permiten apreciarla como igual, mejor o peor que las restantes de su especie[6]”

De lo anterior podemos mencionar que la calidad es una forma de comparar nuestros productos contra otros. Es una especie de calificación que se dá por parte del cliente una vez que ya lo ha aprobado o reprobado, según sea el caso. La norma ISO 9000:2000, correspondiente a vocabulario, la define como:

“Grado en el que un conjunto de características inherentes cumple con la necesidad o expectativa establecida generalmente implícita u obligatoria[7]”

Hay que ver a la calidad como la satisfacción de las exigencias del cliente. En cierto modo la calidad debe formar parte de los objetivos de todos y cada uno de los negocios, ninguna empresa puede considerar la calidad como algo que no sea una preocupación central, ya que todas pueden y deben esforzarse por alcanzarla, mantenerla y mejorarla constantemente.

1.2. Políticas

Al ser las políticas parte esencial en la estructura normativa de las diferentes organizaciones, resulta importante el conocer y comprender sus principios básicos, así como estar conscientes del reto que plantea el escribirlas y más aún el compromiso que surge para llevarlas a cabo y mantenerlas vigentes.

No es ninguna novedad que un término como política tenga tantas acepciones como organizaciones hay en el mundo, y no es para menos, ya que cada quien hace lo que cree conveniente con este término.

Así por ejemplo, en la administración el término “política” hace referencia a distintas ideas con un carácter sumamente amplio y hasta en ocasiones incompatibles, desde verlas meramente como aspiraciones, hasta como una serie de principios éticos que el personal debe respetar. Políticas son la expresión de acuerdos que sirven de guía y canalización de los razonamientos, decisiones y acciones de la gestión hacia la búsqueda de los objetivos de la empresa.

[6] Idem 2
[7] Idem 5

Las políticas se reflejan en una serie de normas, reglamentos y protocolos a seguir, donde se deben definir las distintas medidas que se han de tomar para proteger la integridad de las instalaciones, así como las funciones y responsabilidades de las personas involucradas en la organización para controlar su funcionamiento.

Debe ser la alta dirección, junto con los expertos en la tecnología, en este caso redes de computadoras, quienes deben definir los requisitos de la instalación y su posterior uso, identificando y dando la debida importancia a las distintas actividades que de esto se desprendan, con lo que los procedimientos más importantes recibirán una mayor atención en caso de surgir algún contratiempo.

Dichas políticas deben ser acordes con las prácticas de la organización, es decir, se deben desprender de las intenciones y objetivos globales de la empresa, de nada nos serviría el contar con políticas ostentosas y con nombres estrafalarios si realmente las personas no las cumplen ni les prestan atención alguna. Por el contrario, una política debe ser una guía para la realización de diferentes acciones, que deben permitir mas no obstaculizar la consecución de los objetivos. De hecho, es gracias al establecimiento de políticas dentro de la empresa el que los empleados sentirán la influencia de las actitudes de la alta dirección para con toda la organización; y que le van a permitir al personal directivo la toma de decisiones en el tiempo y forma adecuados ante una posible contingencia en algún departamento, por ejemplo, algún ataque con robo de información, compra de equipo nuevo, entre otros.

1.2.1. Tipos de políticas

Cada vez que hablamos de un documento que contiene políticas de cualquier índole, estaremos hablando de un documento, que por definición, debe responder a las necesidades y características de la organización que las generó; se trata sin duda alguna de un documento dinámico, que se debe adaptar conforme los objetivos de la empresa cambien, conforme la empresa crezca y conforme los clientes lo exijan, de esta forma estaremos garantizando que nuestra capacidad de liderazgo como alta dirección no se vea afectada por el paso del tiempo.

Los documentos con políticas deben ser revisados periodicamente por parte de la alta dirección para mantenerlo vigente, y no como se dice vulgarmente “para molestar al de a lado”, a veces por cuestiones de competividad del mercado, las revisiones a dichos documentos se hacen en un periodo de tiempo muy corto, y en base a los resultados que se obtienen por parte de la empresa.

De todo lo anterior podemos establecer los siguientes puntos:

- Los documentos que contengan políticas de seguridad deben ser objeto de mantenimiento continuo.
- Lo anterior incluye: su revisión para su adecuación a los tiempos actuales y mejora constante.

- Debe ser un compromiso de la alta dirección como un camino hacia lograr el éxito laboral dentro de la empresa.

Dependiendo del grado de amplitud de las situaciones que pretenda abarcar una política, podemos clasificarla en los siguientes niveles jerárquicos:

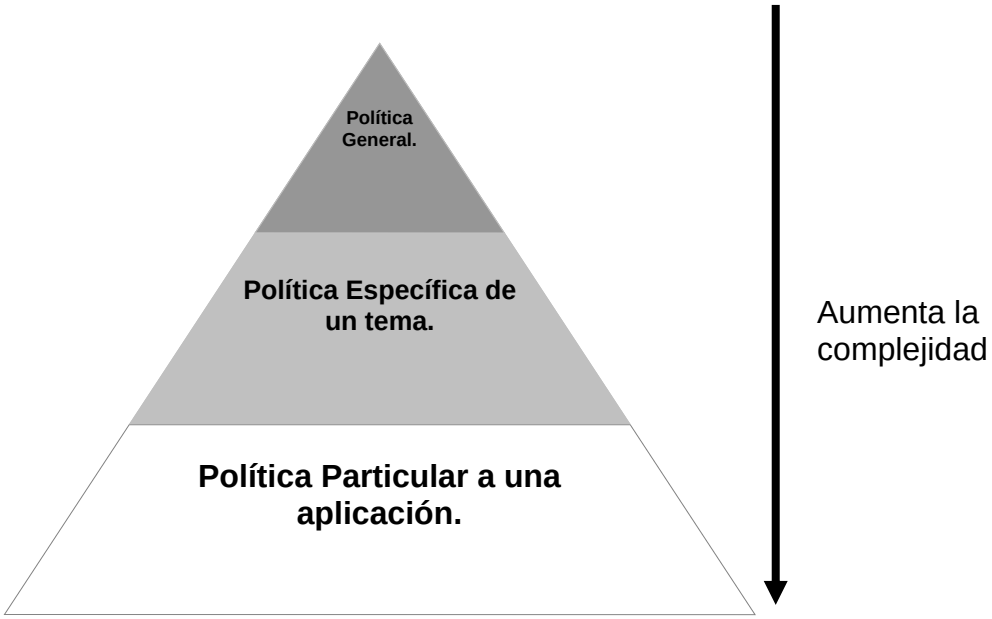


Figura 1.2 Jerarquía en los tipos de políticas.

Política General: Es un estado deseado por la empresa respecto a algún rubro en específico, por ejemplo, una política general podría ser la política de calidad de la organización.

Política Específica de un tema*:* Son aquellas políticas que están orientadas a tópicos con un interés en específico, por ejemplo, política de adquisición de equipo nuevo.

Política Particular a una aplicación*:* Son todas aquellas políticas que se enfocan a la toma de decisiones por parte de la alta dirección para responder ante contingencias en algún área en específica, por ejemplo, políticas de protección de la información ante un incendio.

Como podemos observar, si partimos de las políticas generales, el grado de complejidad aumenta conforme avanzamos hacia las políticas particulares, cosa normal, ya que entre más especializada sea una política, ésta debe considerar detalles que a simple vista no son tan obvios como parecería ser, de la misma manera, su periodo de revisión se verá afectado haciendolo más corto, debido al cambio de tecnologías o métodos en el desarrollo de las actividades, además un gran obstáculo que este tipo de políticas afrontan es el alto grado de dificultad en su implementación, debido a su nivel de especialización.

Por otro lado, las políticas también se pueden clasificar de acuerdo a los recursos a los que está encaminada:

Orientada a los recursos lógicos.
Incluye a todos aquellos recursos tecnológicos con los que cuenta la organización, para generar, explotar o intercomunicar tanto aplicaciones como los datos que transitan entre ellas. Muchas veces este tipo de políticas incluyen aquellas relacionadas con la seguridad de la red y de la preservación de la información, cuando aún se encuentran dentro del disco duro de la computadora.

Orientada a la gestión.
Incluye aquellos recursos que tienen que ver con aspectos administrativos, de personal o bienes que tengan que ver con la estructura organizacional de la empresa. Por ejemplo, políticas laborales de convivencia entre los empleados, políticas enfocadas a la calidad de los productos, etcétera.

Orientada a los recursos físicos.
Abarca aquellos bienes materiales tales como locales con los que cuenta la empresa, mobiliario, infraestructura tecnológica que se tenga, equipos de telecomunicación, computadoras, entre otros.

Orientada a la respuesta ante incidentes.
Incluye los recursos que son empleados durante y después de alguna contingencia. Fondo monetario de contingencia, locales alternativos de funcionamiento de la empresa, y respaldos de la información que se tengan.

Es de notarse el grado de especialización que cada una de las clasificaciones anteriores tiene, ya que se podría pensar que éstas podrían caer fácilmente en el rubro de políticas particulares, aunque esto no es así, porque en ese sentido también podriamos decir que forman parte de las otras dos (específicas y generales), y se estaría hablando entonces de una política general de gestión de la empresa.

Lo verdaderamente importante aquí, es que la organización sepa identificar los diferentes tipos de políticas y adopte aquellas que le sean convenientes y le puedan funcionar. De nada nos sirve contar con una gran cantidad de políticas especializadas si ninguna de ellas logra el objetivo para el cual fueron propuestas. La alta dirección debe definir mediante la experiencia del personal de cada área afectada, aquellas políticas que le pueden ayudar a mejorar el trabajo que se está haciendo día con día. En ningún momento debe imponerlas, y debe estar conciente de la importancia de que el personal las adopte de la mejor manera, ya que ellos son los que, a final de cuentas, hacen mejor que nadie el trabajo que les ha sido encomendado.

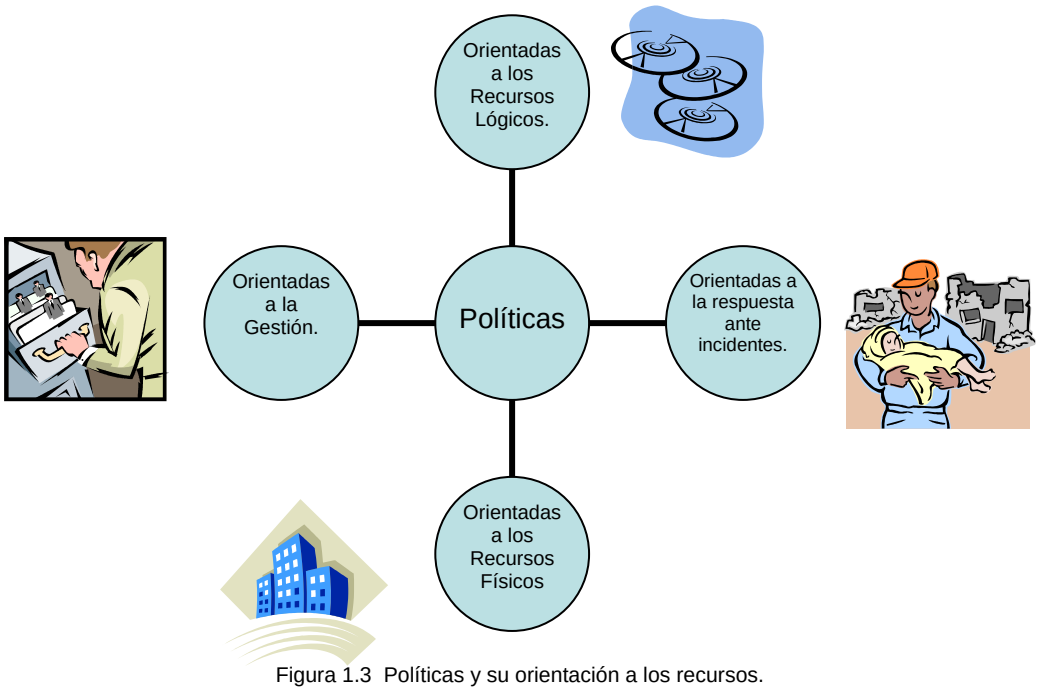


Figura 1.3 Políticas y su orientación a los recursos.

1.2.2. Problemas en la definición de políticas

Muchas veces las políticas sea cual sea su índole de aplicación, son difíciles de aceptar por el personal que labora dentro de la organización, esto se debe generalmente a que en el pasado han existido problemas con su desarrollo. La mayoría de las veces la alta dirección de las empresas, se ha tenido que enfrentar a grandes presiones para poder establecer una política en el ámbito que sea. Además, si el establecimiento de políticas entorpece o hace más lento algún proceso dentro de un departamento, obviamente el personal que labora ahí ejercerá presión para evitar su aplicación.

Desgraciadamente, el personal también asocia a las políticas con burocracia. Y es que el hablar del término “política” trae a la mente pensamientos de textos interminables e inentendibles, así como la asistencia por parte del personal a aburridas reuniones y en general, haciéndole “la vida de cuadritos a la gente que sólo trata de hacer su trabajo”. Este punto de vista es desafortunadamente el que predomina en las empresas hoy en día, olvidando por completo que las políticas son parte del trabajo que realizamos a diario.

En la mayoría de las ocasiones la documentación se elabora y se queda guardada sin que nadie lea su contenido, cuando mejor le va, es publicada, aunque nadie la lleva a cabo. Esta situación tan típica, por llamarla de algún modo, minimiza el gran esfuerzo que lleva a cabo la organización para contar con un marco estandarizado de trabajo, que permita eficientarlo, y que cuente con una normatividad adecuada para su desempeño.

1.2.3. Consideraciones para realizar políticas

No existen fórmulas mágicas para el establecimiento de una serie de políticas, éstas son resultado de reuniones con la alta dirección, en donde se trata de buscar que sean lo más acorde con la misión de la empresa, y que no sean un obstáculo para la consecución de sus objetivos. Sin embargo, el resultado de hacer lo anterior, son políticas hechas en base a la experiencia profesional de los encargados de cada departamento dentro de la organización, es por eso que existe cierta renuencia por parte de los empleados para acatarlas, ya que parecieran una especie de "imposición disfrazada" de las reglas del jefe. Por ello, es importante el contar con medios de comunicación con todo el personal que labora dentro de la empresa, para recoger sus propuestas e inquietudes para la elaboración de las políticas de cada departamento en específico.

El primer requisito para una empresa es definir políticas "medibles y alcanzables", es decir que se puedan cumplir y se pueda cuantificar el grado de su cumplimiento. Para ello, es necesario identificar y analizar los factores internos y externos que afectan a la organización.

El análisis interno puede incluir los siguientes factores:

- la cultura de la empresa.
- los recursos de los que dispone.
- las debilidades y fortalezas de la organización.

Mientras que el análisis externo se debe encargar de lo siguiente:

- las variables del entorno, tanto nacional como internacional entre las que podemos mencionar situaciones tecnológicas, económicas, sociales y políticas entre otras.
- la competencia en el mercado.
- las posibles amenazas y oportunidades de la empresa.

Una vez hecho lo anterior, se puede continuar hacia una segunda etapa, donde se lleven a cabo una serie de actividades encaminadas a la declaración de las políticas en sí, la organización debería considerar los siguientes puntos antes de realizar una declaratoria:

1. Formular una lista de posibles políticas por cada función operacional o departamento interesado en establecerlas (recursos humanos, sistemas, almacén, etc.), aplicable al organismo social que se trate.

2. Discutir con los responsables de cada departamento la posible lista de políticas con el fin de:

- Determinar aquellas que son más deseables con respecto a otras.

- Establecer los límites de cada una de ellas.
- Determinar prioridades e importancia en la redacción de aquellas políticas que puedan afectar notablemente al departamento.
- Presentar un borrador con las propuestas del personal de cada departamento, con el fin de discutirlas con la alta dirección y realizar una sola política que sea incluyente.
- La aprobación de la redacción final de las políticas por parte de la alta dirección y el responsable de cada departamento.

La alta dirección debe asegurarse que las políticas son adecuadas al propósito de la organización, así como, incluir un compromiso de cumplir con los objetivos del departamento donde se quiera aplicar; que son comunicadas y entendidas dentro de la organización y que están sujetas a revisión para su continua adecuación.

Con respecto a la redacción de las políticas, es muy importante el tomar en cuenta que dichos enunciados, deben ser lo suficientemente claros para evitar confusiones y la búsqueda de "atajos" por parte de los empleados para no cumplirlas. Algunas recomendaciones incluyen el establecimiento de un documento controlado donde se establezcan los siguientes puntos:

Propósito de la Política.- Debe describir de manera general y concisa el fin que se pretende lograr con el establecimiento de dicha política.

Definición de conceptos básicos.- Donde se establezcan las nociones básicas involucradas en el enunciado de la política.

Contenido.- El enunciado de la política como tal.

Responsabilidades.- Establecer los niveles de responsabilidad de las personas involucradas en el ámbito de la política.

Finalmente, una buena política debería considerar en primer lugar los objetivos generales de la empresa (ya que son los puntos hacia donde queremos llegar), y contestar a las siguientes preguntas:

¿Qué se hace?

¿Cómo se hace?

¿Para quién se hace?

¿En qué se sustenta?

Un ejemplo de política basado en lo anterior podría ser: *"En nuestra organización, nos comprometemos a ofrecer a nuestros clientes productos que cumplan con sus requisitos, a*

través de la mejora y con personal altamente capacitado, en concordancia con los objetivos de la empresa".

¿Qué se hace? → Productos que cumplan con sus requisitos

¿Cómo se hace? → A través de la mejora y con personal altamente capacitado.

¿Para quién se hace? → Nuestros clientes.

¿En qué se sustenta? → En concordancia con los objetivos de la empresa.

1.3. Normas y procedimientos

El comercio internacional actualmente se rige por diferentes sistemas de normas y principios de carácter general, en específico para los productos y servicios que se ofertan en los mercados globalizados. Con relación a lo anterior, el mundo se ha organizado en bloques económicos que determinan sus propias normas y principios para reglamentar, por un lado, todas las transacciones comerciales entre ellos, así como a las empresas que participan o desean participar en ellas. Un claro ejemplo de dichas normatividades y que han logrado ser aceptadas mundialmente, es el sistema de normas ISO 9000, las cuales abarcan diversos temas que van de acuerdo a la naturaleza u objeto de lo que se normaliza, así tenemos por ejemplo: sistemas administrativos, de capacitación, sistemas de planeación, de productos y servicios, medio ambiente, documentación y aseguramiento de la calidad, entre otros.

México no podría ser la excepción, ya que al suscribir el tratado de libre comercio con Canadá y los Estados Unidos, adquirió el compromiso de respetar y hacer valer todas aquellas normas y reglamentos jurídicos, necesarios para controlar las transacciones comerciales entre países, buscando con ello asegurar la calidad de los productos y servicios que se venden dentro de dicho bloque económico.

Los sistemas de normas y los principios de calidad total, forman parte de un proceso no solamente para proponer esquemas de desarrollo empresarial, sino también para formalizar las estructuras funcionales de las instituciones públicas, con la finalidad de hacerlas más competitivas y confiables.

Lo anterior no aplica exclusivamente para los gobiernos de los países, sino también a sus empresarios, la necesidad de disponer de información sobre el conjunto de normas regulatorias de cada rubro del mercado, que les permita tener el conocimiento necesario acerca de ellas para poder realizar sus relaciones comerciales y estandarizar la calidad de sus procesos de producción de bienes y servicios.

1.3.1. Importancia de las normas

El establecimiento de cualquier tipo de normas, implica el adecuar un conjunto de métodos, técnicas y procedimientos que se llevan a cabo dentro de una organización; además, proveen la estandarización en toda la documentación que se usan dentro de la empresa, garantizando una correcta comunicación entre todos los departamentos.

La correspondencia de un conjunto de normas hacia un mismo parámetro, que puede ser de carácter técnico, o bien de procedimiento, y que sean establecidas dentro del mismo ámbito, ya sea local, regional, nacional o incluso internacional, tienen como objetivo primordial el que sean acatadas, entendidas y respetadas por todo el personal que labora dentro de la empresa. De esta forma, es posible la comunicación y cooperación en el desarrollo de proyectos entre los diferentes departamentos, sin tener que redefinir las técnicas o los procedimientos de los equipos de trabajo, evitándonos *reprocesos*.

Obviamente cuando se establece una normatividad adecuada dentro de la organización, entendiendo adecuada, como algo realista y que se puede alcanzar, éstas van a ayudarnos a evitar la prolongación en los plazos de entrega de productos o servicios, además de que nuestro producto cada vez sea mejor visto por nuestros clientes, símbolo que es de buena calidad y de menor costo.

Por último, el factor comunicación es determinante muchas veces en la consecución de los objetivos de la empresa, bajo una normatividad bien establecida es posible mejorarla, y agilizar los trámites en cuanto al desarrollo de un proyecto, ya que la empresa ha fijado su postura en las normas, y quedan entendidas como el compromiso que la alta dirección ha asumido con respecto a los productos y/o servicios que ofrece. Además, el personal encargado puede tener la capacidad de desarrollar otro proyecto con costos mínimos de adaptación y aprendizaje, ya que se cuenta con el respaldo de dicha normatividad.

1.3.2. ¿Cómo se hace una norma?

Como ya mencionamos anteriormente, las normas son reglas que regulan la conducta de las personas en una determinado ámbito. Son como una horma que da forma a algo, en este caso, la conducta de los individuos. Podemos mencionar varios ejemplos de normas como: cumplir los términos de un contrato; pagar el pasaje de un autobus; respetar los tiempos del trabajo; saludar a una persona, etcétera.

Los seres humanos, en la vida diaria, nos encontramos sujetos a diversas clases de normas que regulan nuestra conducta dentro de un grupo social, dichas normas son: de tipo moral, jurídicas, religiosas y sociales. En el presente trabajo solamente trataremos las de tipo jurídicas, ya que los demás tipos están fuera de nuestro estudio.

Normas Jurídicas.

Las normas jurídicas, tienen como objetivo la regulación de la conducta para con los demás, a fin de organizar la vida social al prevenir conflictos y dar las bases para la solución. Son disposiciones que la alta dirección, por medio de los diferentes departamentos señala como obligatorias, plasmada en los códigos y reglamentos de la institución.

Características.

Bilaterales: esto es, por un lado deben imponer obligaciones y por otro conceder derechos a los individuos. Ejemplos de esto pueden ser, contratos de compraventa con el proveedor, donde el vendedor tiene la obligación de entregar los bienes vendidos y el derecho de exigir el pago correspondiente. Por su parte, el comprador tiene la obligación de pagar el precio de dichos bienes y el derecho de exigir que se le entreguen.

Exteriores: dicho de otra forma, a la empresa solamente le van a importar los actos o conductas humanas que son exteriorizadas y no la causa o pensamiento que se genere en el individuo. Por ejemplo, si una persona piensa en robarse la información de algún producto, mientras sólo lo piense a la empresa no le importará; pero si divulga sus intenciones e incluso invita a participar a más personas, hace preparativos para llevar a cabo el plan y finalmente lo realiza, entonces se hace del interes de la empresa.

Coercibles: que puede exigirse el cumplimiento de la obligación aun en contra de la voluntad de la persona. Por ejemplo, todo el personal está obligado a llegar a su hora de trabajo de acuerdo al contrato que firmaron, si no es así, el jefe inmediato aplicará una sanción administrativa que puede ir desde un descuento en el pago, hasta el despido de la persona.

Heterónomas: los sujetos obligados por ellas, no las dictan para sí, no emanan de sus voluntades, sino de la voluntad de alguien más, que bien puede ser la de alta dirección. Un ejemplo de esto, es cuando el personal de un departamento se ve obligado a cumplir con determinados objetivos, que fueron, establecidos por el jefe o algún superior a él.

Como hemos visto la redacción de una norma adecuada a cada organización, no es una tarea fácil, ya que el hecho de estar enfocadas a los individuos, siempre van a acarrear descontento para unos, y aceptación para otros más. Debe existir una adecuada comunicación entre la alta dirección con todos sus departamentos y en general con todo el personal, para promover un ambiente de trabajo en el que todos sean partícipes, y las disposiciones sean tarea de todos y acatadas por todos, solamente así será posible el éxito de las normas.

1.3.3. ¿Cómo se hace un procedimiento?

Aparentemente, la descripción de las actividades que conforman el trabajo que realizamos a diario debería ser fácil y lo más naturalmente posible, sin embargo, cuando uno se

propone redactar lo que hace a diario, se topa con preguntas tales como ¿será todo lo que hago?, ¿no estaré excluyendo nada?, ¿estará bien redactado?, entre otras más. Por ello, es importante el contar con una metodología que nos permita desarrollar un procedimiento, sin olvidar aspectos fundamentales de forma y funcionalidad.

¿Por qué realizar procedimientos documentados?, simple, porque nos van a permitir garantizar que las actividades organizadas ocurran de la manera en que son planeadas, lo que se conoce como "gestión de la calidad[8]". Contar con un documento donde se establezcan todas las actividades, nos va a permitir tener menos reprocesos, ya que minimizan las posibles desviaciones en el trabajo que realizamos a diario, al evitar eso, los costos se verán reducidos, y las ganancias aumentarán, beneficiando a toda la empresa. Es un circulo virtuoso que sin duda todas las empresas quisieran tener.

Es por eso, que la naturaleza de la norma de calidad internacional ISO 9001:2000, está orientada a realizar el trabajo de una forma ordenada y documentada, como se muestra en el diagrama siguiente:

Figura 1.4 Naturaleza de la norma ISO 9000:2000

En pocas palabras: "Escribe lo que haces y haz lo que escribiste".

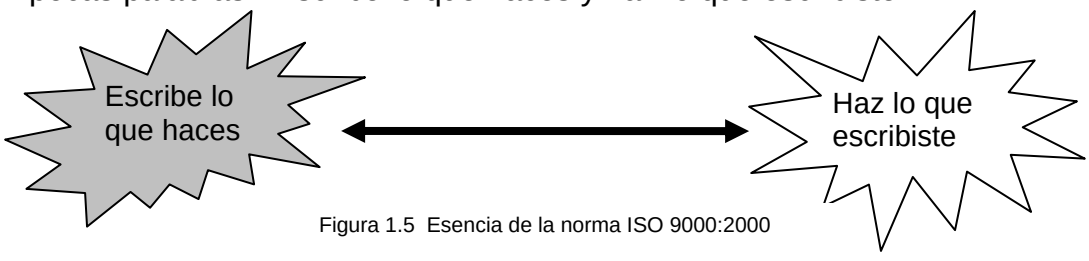


Figura 1.5 Esencia de la norma ISO 9000:2000

[8] Ver glosario de términos.

La redacción de los procedimientos de trabajo es vital para la consecución de los objetivos de la empresa, más aún si se cuenta con empleados concientes de que su trabajo si lo realiza de forma adecuada, beneficia no sólo a él sino a toda la empresa.

Estructura general de los procedimientos

Todo procedimiento deberá contar con cada uno de los apartados que proponen enseguida, y solamente aquellos donde se indique que es opcional y que no se requiere, se indicará con un *(asterisco):

Introducción*: Debe dar un panorama general del procedimiento.

Objetivo: Es el fin que se pretende alcanzar y para el cual están orientadas las actividades de la organización.

Alcance: Delimitación de las fronteras de aplicación del procedimiento al cual se refiere el documento y se describe su campo de acción, es decir a qué procesos, servicios, documentos o área es aplicable.

Documentos de Referencia*: Se debe hacer mención de los documentos, normas, códigos, especificaciones o leyes que respalden dicho procedimiento.

Responsabilidad y Autoridad: Se debe indicar el cargo del responsable de la actividad, sujeta a control e indica la autoridad.

Definiciones y Abreviaturas*: En esta parte se deben definir aquellos términos que aparecen de manera recurrente en el procedimiento, tales como el significado de siglas, palabras usadas dentro de la organización, entre otras palabras que a consideración del autor no son de uso común. Ejemplos:

FI: Facultad de Ingeniería.
Disparo Automático: Significa desconexión automática del sistema.

Lineamientos*: Son un conjunto de directrices a observar para la ejecución de las actividades indicadas en los documentos.

Descripción del Procedimiento: En este apartado se deben describir las actividades secuenciales que se realizan dentro de la organización, es decir, qué se hace. Debe contener la información necesaria para facilitar su entendimiento y aplicación. Si la actividad que describe el procedimiento está en otro procedimiento, se debe hacer referencia a él.

La descripción de las actividades debería responder a preguntas tales como: ¿qué es lo que se va a hacer?; ¿quién lo va a hacer?; ¿cómo lo va a hacer?.

Cabe destacar que lo anterior es sólo una recomendación y no necesariamente se debe contestar a todas las preguntas, pero, aquellas que sí se contesten deben expresar la respuesta de forma sencilla, clara y concisa, de forma que sea entendible la intención del procedimiento que se está redactando. Lo anterior es muy importante, ya que la intención de documentar los procedimientos, es para que lo entienda el personal que cubra los requisitos del perfil del puesto.

Todo procedimiento debe describir las actividades críticas que se deben cumplir para su realización, y estará sujeta su descripción a la complejidad del trabajo, de los métodos usados y de las habilidades y capacitación requerida por el personal que realizará el trabajo.

Diagrama de Flujo*: Son una representación gráfica de la actividad que se está desarrollando, de tal manera que sean fácilmente localizadas las acciones a seguir para la buena ejecución del procedimiento.

Mecanismos de Control: Se les llama así a los registros y controles a través de los cuales se verificarán y controlarán las actividades definidas en los procedimientos.

Anexos: Contienen información adicional al procedimiento, tales como instrucciones de trabajo o de operación de algún equipo.

Generalmente las instrucciones de trabajo se desarrollan en caso de que un procedimiento general requiera de una explicación más detallada o de que varios procedimientos hagan referencia a una misma actividad en específico. Su estructura puede ser igual que la de un procedimiento, pero incluye además en su descripción: dibujos, registros, esquemas, matrices, diagramas.

Para cualquier procedimiento siempre se debe tomar en cuenta al personal, ya que ellos se deben sentir conformes con lo escrito y con las actividades descritas en él. La alta dirección no debe “inventar” actividades que no sean factibles de realizar, por más fastuosas y pretensiosas que éstas puedan ser. Solamente aquello que se pueda realizar será materia de estar documentado y nada más.

1.4. Beneficios de las políticas, normas y procedimientos

La falta de normas políticas y procedimientos, ha sido por mucho tiempo uno de los problemas más graves que han afrontado las empresas modernas. Muchas veces por desconocimiento de los beneficios que pueden traer, o simplemente porque se tiene la creencia que sólo traería más “burocracia” dentro de la organización. Visión errónea sin duda, pero que representa el sentir de la gran mayoría. Ahora bien, no hay que olvidar que todas las empresas sin excepción, crean planes de lo que se va hacer en el año, la dirección que debe tomar , y las acciones correspondientes para alcanzar los objetivos, los cuales, son trasmitidos de alguna u otra manera hacia los diversos departamentos y acatados por el personal que labora ahí. Es decir, está estableciendo una política anual

de planeación, con una serie de actividades controladas por la alta dirección (normas), y acatados por el personal que labora ahí (procedimientos para el personal).

Como podemos ver, la mayoría de las empresas ya lo hacen, el problema es que no se tiene la cultura de la documentación, no se establece por escrito lo que hacemos, y solamente cuando se necesita saber algo concerniente a algún proyecto siempre se recurre con los jefes, los cuales a su vez van con sus jefes y así sucesivamente, hasta llegar con la persona que diseñó dicho plan. Haciendo que en verdad ese mito de que generan más "burocracia" sea cierto, cuántas veces no nos hemos preguntado: ¿cuánto más fácil sería esto si los trámites fueran más sencillos, o al menos que supieramos los pasos necesarios para llevarlo a cabo?. Ahí es donde entra la documentación y el establecimiento de normas, políticas y procedimientos dentro de las empresas.

1.4.1. Dentro de la organización y con el personal

Aunque en general la alta dirección, frecuentemente conoce los problemas que aquejan a los diversos departamentos o a la empresa en su totalidad, no termina por ponerse de acuerdo en cuáles requieren mayor atención o cuáles son prioritarios para la salud de la empresa, ya que paradójicamente "todos son importantes". Sin una estrategia organizada para el mejoramiento, es difícil alcanzar un consenso entre la alta dirección y el personal que labora en los diferentes departamentos. De esta forma se hace necesario el constituir políticas, normas y procedimientos dentro de la empresa, con la finalidad de establecer un proceso inicial para definir las prioridades en la consecución de los objetivos.

Las políticas, normas y procedimientos permiten a las organizaciones contar con una guía para controlar sus proyectos, planes, etcétera, asímismo fomentan la cultura de la documentación y la calidad, al lograr:

- El establecimiento de reglamentos generales dentro de la empresa, los cuales van a permitir controlar y ordenar las actividades que se realizan a diario.
- La organización y monitoreo de los proyectos que se lleven a cabo.
- La recavación de registros generados por la propia empresa.
- La realización de acciones preventivas y/o correctivas.
- La capacitación y entrenamiento del personal invlocurado en actividades claves dentro de la empresa, con el fin de asegurar su competencia.

Otro beneficio muy importante y que no se ha mencionado hasta ahora, es la institucionalización de la empresa; mediante la instauración de políticas, normas y procedimientos en sus estructuras organizacionales. La institucionalización nos va a permitir poner las bases dentro de la empresa de una cultura corporativa que esté basada en métodos, prácticas y procedimientos estandarizados, con el fin de mejorar continuamente en las labores que realiza día con día.

1.4.2. Con los clientes

Para una empresa contar con una serie de políticas, normas y procedimientos, es sinónimo de una imagen seria y confiable frente a sus clientes, asegurandole la fidelidad de los mismos, ya que le va a permitir hacer todo bien a la primera y con garantía hacia el cliente, dicho de otra manera, hacer bien las cosas que debe hacer y conforme a las normas, especificaciones y procedimientos establecidos por la alta dirección; a tiempo, cuando el cliente lo necesita, respetando compromisos de horario y calendario, realizando las actividades de forma ordenada.

Todo lo anterior derivará en la percepción del cliente hacia nuestro producto, haciéndolo rentable para nuestra empresa, evitando reprocesos, menos equivocaciones, menos retrasos y gastos inútiles, elevando la productividad y el márgen de utilidades.

Finalmente, debemos mejorar día con día lo que hacemos, no sería sano el mantener siempre el mismo producto o servicio sin hacerle ninguna adecuación, ya que en un mundo tan cambiante como lo es el nuestro, el cliente siempre va a exigir más de lo que compra, ya sean servicios extra o ese “plus” que le permita tener mayor satisfacción en lo que compra. Por ello, la organización debe ser capaz de seguir satisfaciendo al cliente y a la sociedad, cumpliendo con las nuevas expectativas que surjan, debe mejorar continuamente.

1.4.3. Retos del futuro

Siempre el hablar del futuro no es fácil, las empresas modernas están viviendo tiempos de cambios, donde la globalización y la apertura de fronteras comerciales, están jugando un papel preponderante dentro de la economía de cada país. México no puede ser la excepción, su principal socio comercial, los Estados Unidos de América, con sus enormes trasnacionales, y su enorme influencia dentro de los mercados más importantes a nivel internacional, están provocando que las empresas mexicanas se vuelvan más competitivas si no quieren ser dejadas en el olvido por empresas con marcas reconocidas a nivel mundial.

Sin duda alguna es una competencia desleal, pero, también es un foco de atención que el gobierno mexicano debe atender, el fomentar dentro de su mercado interno, que sus empresas se vuelvan hacia el uso de normas internaciones como ISO y estándares internacionales, que permitan estar en el mismo canal de competencia que sus contrapartes extranjeras.

Es preocupante ver que mientras Estados Unidos se encuentra clasificado dentro del “top ten” de países con mayor número de empresas certificadas con ISO 9001:2000 a nivel mundial (clasificación encabezada por China), México solamente cuenta con algunas empresas certificadas, siendo que somos países vecinos y donde existe un tratado de libre comercio.

Será un reto difícil para México, pero servirá al desarrollo económico y empresarial del país. Podemos confiar que un futuro la competitividad de las empresas mexicanas se encontrará al nivel de cualquier otra, haciendo un compromiso de mejora continua y el esfuerzo de las organizaciones por adoptar estándares internacionales.

Redes de computadoras

Capítulo 2

CAPÍTULO 2

REDES DE COMPUTADORAS

2. Las redes

Durante el pasado siglo XX y lo que va de este siglo XXI, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos visto la invención y la instalación de redes telefónicas en todo el mundo, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedente de la industria de las computadoras, así como el gran desarrollo de las telecomunicaciones.

Organizaciones con grandes cantidades de oficinas, dispersas en una amplia área geográfica, basan su eficiencia en la comunicación que pueda existir entre ellas y contar con la comodidad de hacerlo oprimiendo solamente un botón. A medida que crecen las capacidades para recolectar, procesar y distribuir información, la demanda de los procesamientos de información que requieren dichas empresas, crece con mayor rapidez. Generando, así, la necesidad de crear medios que permitan manejar las enormes cantidades de datos e información de las empresas.

2.1. ¿Qué es una red?

La industria de computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de una organización, se ha reemplazado con rapidez por otro que considera un número grande de computadoras separadas, pero interconectadas y que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadoras.

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos para establecer la comunicación, y se incorporaron moduladores y demoduladores para que fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

2.1.1. Objetivo de las redes

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Así, todos los archivos podrían duplicarse en dos o tres

máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias.

Otro objetivo es el económico. Las computadoras pequeñas tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es considerablemente mayor.

Un objetivo más del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si.

2.1.2. Aplicación de las redes

Consideremos tres casos en particular para entender el campo de aplicación de una red de computadoras: el acceso de programas remotos, el acceso a bases de datos remotas y las facilidades de comunicación de valor añadido.

Para el primer caso, consideremos un banco, el cual ha desarrollado un programa que permite a sus clientes realizar simulaciones sobre la inversión de su dinero, entonces, el banco da las facilidades para que el cliente realice dichas simulaciones, a través de la red; aquí se evita la necesidad de vender los derechos del programa y al mismo tiempo el banco da un valor agregado a los servicios que ofrece a sus clientes.

Siguiendo con el ejemplo del banco, enfoquémonos en la necesidad de los clientes de conocer sus estados de cuenta; entonces, se evita la conglomeración en las distintas sucursales de cualquier banco si se permite el acceso a una base de datos para los clientes, y así, puedan acceder a ella desde cualquier computadora.

Para la tercera aplicación, pensemos en la necesidad de comunicación; los gastos de comunicación vía telefónica para una empresa se elevan considerablemente para mantener las relaciones de ésta con sus clientes o bien con sus empleados, mas aún, cuando la comunicación se lleva a un grado internacional. Aquí, la parte económica se ve beneficiada con el uso de una red, por ejemplo del Internet y del correo electrónico.

2.1.3. Clases de redes

No existe una taxonomía generalmente aceptada dentro de la cuál quepan todas las redes de computadoras, pero sobresalen dos dimensiones: la tecnología de transmisión y la escala. En términos generales existen dos tipos de tecnología de transmisión.

- Redes de Difusión.
- Redes de punto.

Las redes de difusión tienen un sólo canal de comunicación compartido por todas las máquinas de la red. Los paquetes cortos que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir el paquete, la máquina verifica el campo de dirección, si el paquete esta dirigido a ella, lo procesa; si esta dirigido a otra máquina lo ignora.

Los sistemas de difusión generalmente también ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama difusión (broadcasting). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo que se conoce como multidifusión.

Las redes de punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar una ó más máquinas intermedias. A veces con posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de ruteo son muy importantes en estas redes.

2.2. Estructura de una red

En toda red existe un conjunto de máquinas para correr programas de usuario (aplicaciones). Llamaremos “host” a las máquinas antes mencionadas. En algunas ocasiones se utiliza el término sistema terminal o sistema final. Bien, los “host” están conectados mediante una subred de comunicación, o simplemente subred. El trabajo de la subred consiste en enviar mensajes entre “host”, de la misma manera como el sistema telefónico envía palabras entre la persona que habla y la que escucha. El diseño completo de la red se simplifica notablemente cuando se separan los aspectos puros de comunicación de la red (la subred), de los aspectos de aplicación (los hostales).

Una subred en la mayor parte de las redes de área extendida consiste de dos componentes diferentes: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (conocidas como circuitos, canales o troncales), se encargan de mover bits entre máquinas.

Los elementos de conmutación son computadoras especializadas que se utilizan para conectar dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación deberá seleccionar una línea de salida para reexpedirlos.

2.2.1. Componentes físicos

Respecto a la estructura física, los modos de conexión física, los flujos de datos, etc.; podemos decir que una red la constituyen dos o más computadoras que comparten determinados recursos, sea hardware (por ejemplo impresoras, escáner, sistemas de almacenamiento) o bien sea software (por ejemplo aplicaciones, archivos, datos).

Elementos de hardware

Apoyándonos en el modelo OSI, la capa uno (capa física) se encarga de la comunicación a través de un medio físico, esto es, un medio de transmisión y una interfaz.

Dentro de los medios físicos más comunes se encuentran:

Medios terrestres

Par Trenzado (Twister-Pair Cabling).

El medio de transmisión más común es el par trenzado. Este consiste en dos alambres de cobre aislados de 1mm de grosor generalmente, trenzados en forma helicoidal. Con esta característica se busca reducir la interferencia eléctrica de pares similares cercanos, así como la característica de que dos alambres paralelos funcionen como antena. La utilidad más común del par trenzado son las redes LAN.

Existen dos tipos de par trenzado, los cuales son divididos de acuerdo a sus características físicas, teniendo así diferentes características de alcance en distancia.

- **UTP (Unshielded Twister Pair)**. El cable UTP es conocido como el cable de par trenzado típico, en donde únicamente depende de trenzar los cables, sin necesidad de un recubrimiento externo a ellos. La distancia máxima sin necesidad de repetidores es de 100m. El par trenzado UTP es clasificado por el número de "trenzados" que se realizan por la unidad de medición pie.

- **Categoría 3 (Cat 3)**. Cables que son formados por 3 trenzados por pie. Pueden transmitir a 16MHz y por tal motivo, es ampliamente utilizado en redes Ethernet a 10Mbps y Token Ring a 4Mbps.

- **Categoría 4 (Cat 4)**. Cables que son formados por 4 trenzados por pie. Pueden transmitir a 20MHz, por tal motivo es utilizado en redes Token Ring a 16Mbps.

- **Categoría 5 (Cat 5)**. Cables que son formados por 5 trenzados por pie. Pueden transmitir a 100MHz, lo cual lo hace un cable utilizado en redes Fast Ethernet.

• **Categoría 6 (Cat 6)**. Cables que son formados por 6 trenzados por pie. Pueden transmitir a 1 Gbps y las características de transmisión del medio están especificadas hasta una frecuencia superior de 250 MHz.

• **Categoría 7 (cat 7).** Es una mejora a la categoría anterior, puede transmitir datos hasta 1 Gbps, y las características de transmisión del medio están especificadas hasta una frecuencia superior de 600 MHz.

• **STP (Shielded Twister Pair)**. STP es el tipo de cable de par trenzado en donde existe un recubrimiento de aluminio alrededor de los cables, de tal manera de impedir interferencias eléctricas sobre los cables, teniendo así, una mejor respuesta al ruido y logrando una distancia sin necesidad de repetidores de 200m. STP fue desarrollado por IBM, por lo cual, es utilizado para redes Token Ring, aunque no existen estándares para redes Ethernet.

Tipo	Uso
Categoría1	Voz (Cable de teléfono)
Categoría 2	Datos a 4 Mbps (LocalTalk)
Categoría 3	Datos a10 Mbps (Ethernet)
Categoría 4	Datos a 20 Mbps/16 Mbps Token Ring
Categoría 5	Datos a 100 Mbps (Fast Ethernet)
Categoría 6	Datos a 1 Gbps (Fast Ethernet)
Categoría 7	Datos a 1 Gbps (Fast ethernet)

Tabla 2.1 Categorías de par trenzado

Conectores de cable par trenzado

Así como existen conectores de contacto para la luz eléctrica, de la misma forma, existen conectores para el cable par trenzado. Dentro de este apartado veremos dos de ellos que son los más utilizados.

RJ45

Es un conector modular que puede contener hasta cuatro pares de cables. Este conector es el más común para cableado de par trenzado sin blindaje (UTP) que se utiliza para la instalación de redes LAN. Los conectores RJ45 típicamente soportan “transmisión de datos”, “recepción de datos”, “terminal de datos”, “conjunto de datos”, “datos por defecto”, “peticiones de envío” y “señal de tierra”.

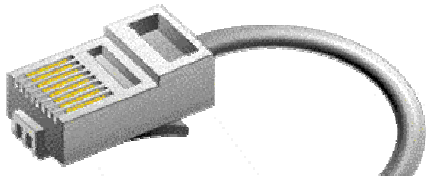


Figura 2.1 Conector RJ45

RJ11

Es un conector modular que puede contener hasta tres pares de cables. Este conector es típico en enlaces telefónicos. Este cable es comúnmente utilizado en casas y oficinas por la misma razón. El conector RJ11 es también utilizado para líneas privadas de cuatro cables. Aunque el RJ11 es conectado a un cable que contiene dos o tres pares de cables, sólo un par es utilizado para las aplicaciones de switcheo de la red. Cuando se conecta a líneas de dos pares, los cuatro conductores que lo forran son utilizados. Los plugs utilizados tienen un punto común denominado “tip”, el cual, es de color rojo, mientras el adyacente conocido como “ring” es de color verde. En los cables de teléfono de dos pares tiene colores amarillo, verde, rojo y negro. El verde es el tip del circuito y el rojo es el ring. El amarillo y negro son utilizados para proporcionar energía o para controlar un segundo teléfono

Cable coaxial (Coaxial Cable)

El cable coaxial está formado por un alambre de cobre rígido como núcleo, rodeado por un material aislante. El aislante está forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado. El conductor externo se cubre de una envoltura protectora de plástico.

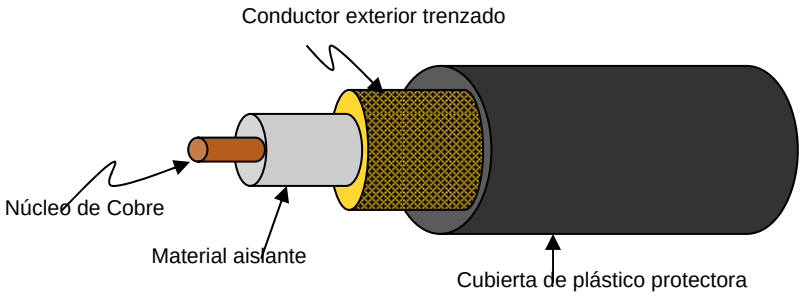


Figura 2.2 Diagrama de cable coaxial

El cable coaxial puede abarcar tramos más grandes sin necesidad de repetidores a velocidades mayores. Existen dos tipos de cable coaxial.

• **Cable de 50 ohms (RG-58/U))** para comunicación banda-base (transmisión digital). Generalmente para redes Lan.

• **Cable de 75 ohms (RG-59/U))** para comunicación de banda ancha (transmisión analógica), utilizado comúnmente en sistemas de televisión por cable.

El cable coaxial, sea cual sea el tipo, no puede ser utilizado para redes Token Ring, FDDI, teléfono o ISDN. Sin embargo, el cable coaxial puede ser utilizado para redes Ethernet, siendo en este caso, de dos modelos diferentes:

• **ThinLAN**.- Cable coaxial con un diámetro de 0.2 pulgadas de 50 ohms que pueden abarcar una distancia de 185m. Este tipo de cable coaxial es denominado comúnmente "*cheapernet*" debido al bajo costo en su instalación. Las redes ethernet con ThinLAN requieren contener el transceiver dentro de las tarjetas de red. Los nodos accesan a la red por medio de conectores T.

• **ThickLAN.-** Cable coaxial con un diámetro de 0.4 pulgadas de 50 ohms que pueden abarcar una distancia de 500m.

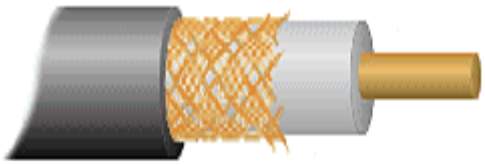


Figura 2.3 Cable coaxial

Conectores de cable coaxial

El conector para cable coaxial más utilizado es el BNC. Para redes LAN que utilizan cable coaxial es común utilizar conectores BNC[9] tipo T.

Ethernet por medio de un cable Thin Ethernet para realizar las conexiones entre las estaciones de trabajo y el cableado. Existen conectores adaptadores tipo hembra/hembra, los cuales conectan o prolongan dos longitudes de cables Thin-Ethernet.

Conectores T. Es un conector BNC en forma de T; se conecta a la tarjeta de red y permite conectar entre sí las diferentes estaciones de trabajo. En ambos extremos del segmento se conectarán a la T los terminadores

[9] BNC: British Naval Connector, conector utilizado típicamente en redes.

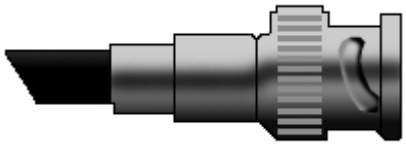


Figura 2.4 Conector BNC

Fibra óptica

Los circuitos de fibra óptica son filamentos de vidrio flexibles, del espesor de un cabello, llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

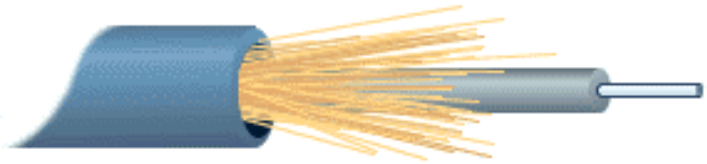


Figura 2.5 Fibra óptica

Este cable está constituido por uno o más hilos de fibra de vidrio. Cada fibra de vidrio consta de:

- Un núcleo central de fibra con un alto índice de refracción.
- Una cubierta que rodea al núcleo, de material similar, con un índice de refracción ligeramente menor.
- Una envoltura que aísla las fibras y evita que se produzcan interferencias entre fibras adyacentes, a la vez que proporciona protección al núcleo. Cada una de ellas está rodeada por un revestimiento y reforzada para proteger la fibra.

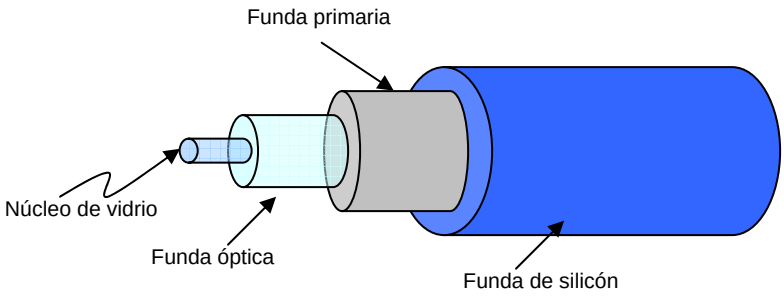


Figura 2.6 Diagrama de fibra óptica

La luz producida por diodos o por láser, viaja a través del núcleo debido a la reflexión que se produce en la cubierta y es convertida en señal eléctrica en el extremo superior.

Figura 2.7 Medio de transmisión

La fibra óptica es un medio excelente para la transmisión de información debido a sus excelentes características: gran ancho de banda, baja atenuación de la señal, integridad, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración. Su mayor desventaja es su costo de producción superior al resto de los tipos de cable, debido a necesitarse el empleo de vidrio de alta calidad y la fragilidad de su manejo en producción. La terminación de los cables de fibra óptica requiere un tratamiento especial que ocasiona un aumento en los costos de instalación.

Uno de los parámetros más característicos de las fibras es su relación entre los índices de refracción del núcleo y de la cubierta que depende también del radio del núcleo y que se denomina frecuencia fundamental o normalizada; también se conoce como apertura numérica y es adimensional. Según el valor de este parámetro se pueden clasificar los cables de fibra óptica en dos clases:

Modo Monomodo.

Cuando el valor de la apertura numérica es inferior a 2405 (frecuencia fundamental), un único modo electromagnético viaja a través de la línea; es decir, una sola vía y por tanto ésta se denomina modo simple o monomodo. Este tipo de fibra necesita el empleo de emisores láser para la inyección de luz, los que proporcionan un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa. Resultan más caras de producir y el equipamiento es más sofisticado.

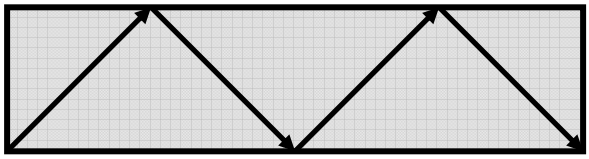


Figura 2.8 Diagrama de transmisión monomodo

Modo Multimodo.
Cuando el valor de la apertura numérica es superior a 2405 (frecuencia fundamental), se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo. Las fibras multimodo son las más utilizadas en las redes locales por su bajo costo. Las distancias de transmisión de este tipo de fibras están alrededor de los 2.4Km y se utilizan a diferentes velocidades: 10Mbps, 16Mbps y 100Mbps.

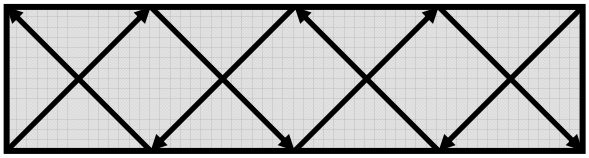


Figura 2.9 Diagrama de transmisión multimodo

Las características generales de la fibra óptica son:

- **Ancho de banda.-**La fibra óptica proporciona un ancho de banda significativamente mayor que los cables de pares (blindado/no blindado) y el coaxial. Aunque en la actualidad se están utilizando velocidades de 1.7Gbps en las redes públicas, la utilización de frecuencias más altas (luz visible) permitirá alcanzar los 39 Gbps. El ancho de banda de la fibra óptica permite transmitir datos, voz, video, etcétera.
- **Distancia.-** La baja atenuación de la señal óptica permite realizar tendidos de fibra óptica sin necesidad de repetidores.
- **Integridad de datos.**- En condiciones normales, una transmisión de datos por fibra óptica tiene una frecuencia de errores menor a $10E^{-11}$.
- **Duración.**- La fibra óptica es resistente a la corrosión y a las altas temperaturas. Gracias a la protección de la envoltura es capaz de soportar esfuerzos elevados de tensión en la instalación.
- **Seguridad.**- Debido a que la fibra óptica no produce radiación electromagnética, es resistente a las acciones intrusitas de escucha. Para acceder a la señal que circula en la fibra es necesario partirla, con lo cual no hay transmisión durante este proceso, y puede por tanto detectarse.

Conectores para fibra óptica

Los conectores para fibra óptica más comunes son el ST, FC y el SC.

• **ST (Straight Tip).-** Se sujeta a la fibra por medio de una aguja y un cilindro que son cerámicos, aunque los hay de metal o plástico.

• **FC (Fiber Connector).-** Conector cilíndrico que se enrosca fácilmente. Es comúnmente utilizado en conexiones con fibra óptica.

• **SC (Subscriber Connector).-** Conector utilizado en enlaces más delicados, es un conector muy confiable pero costoso. Conector de forma cuadrada.

Medios aéreos

Microondas (Microwaves)

Por encima de los 100 MHz, las ondas viajan en línea recta, y por tanto, enfocan en un haz estrecho. Es así como se requiere que tanto los transmisores como los receptores se encuentren bien alineados. Debido a la curvatura de la tierra, la distancia entre transmisor-receptor no debe ser muy grande, utilizándose repetidores a ciertas distancias.

Cuanto más altas sean las torres, más separadas pueden estar, es por ello que se desarrollaron los satélites, aumentando así la altura de las “antenas”. Comúnmente se utiliza una frecuencia entre los 890MHz y los 20GHz, y son generalmente utilizadas para la transmisión telefónica, fax, video y datos.

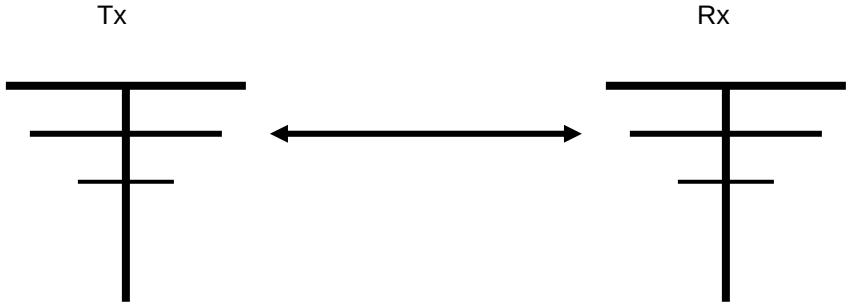


Figura 2.10 Medio de transmisión

Rayo infrarrojo

Este medio de transmisión es comúnmente usado en comunicaciones de corto alcance, tales como los controles remotos de televisores y estéreos. Son relativamente baratos y fáciles de construir. Usan una sola frecuencia, este tipo de comunicación tiene una característica importante, no atraviesan cuerpos sólidos. Esto tiene la desventaja de no poder existir una comunicación entre paredes, pero tiene la ventaja de que no interfiere con otras comunicaciones. En 1994 se desarrollaron las primeras PC´s con un puerto denominado IRDA (Infrared Serial Data Link), el cual puede funcionar para la comunicación como cualquier otra interfaz.

Rayo láser (Laser o Light Amplification by Stimulated Emission of Radiation)

El rayo láser es capaz de la transmisión de luz a una sola frecuencia. El rayo láser es totalmente inmune a interferencias electromagnéticas de cualquier tipo, lo cual permite la eliminación de muchos repetidores que únicamente hacen la instalación muy costosa. Es utilizado para la comunicación entre edificios cercanos ya que no puede transmitir a

grandes distancias. Se necesita un transmisor y un receptor, al igual que para el rayo infrarrojo. Una desventaja es que el rayo láser no puede penetrar la lluvia ni la niebla densa.

Interfaz

La interfaz es el enlace mecánico y eléctrico que conecta dos o más dispositivos o equipos. La interfaz es formada por el punto físico donde las señales eléctricas, conectores, timers y aperturas de llamada son definidos, así como procedimientos, códigos y protocolos para el intercambio de información. Las interfaces más comunes son:

- RS-232
- RS-449
- V-35

2.3. Tipos de redes de computadoras

Para poder visualizar el sistema de comunicación en una red es conveniente utilizar el concepto de topología, o estructura física de la red. Las topologías describen la red físicamente y también nos dan información acerca del método de acceso que se usa (ethernet, token ring, por ejemplo).

2.3.1. Topología de anillo

Una de sus características importantes es que está formado por un conjunto de enlaces punto a punto, lo cual es una topología bien entendida y probada, en donde la información es pasada a través de los nodos uno a uno en una comunicación punto a punto. La ventaja que tiene esta topología es que no se requiere un cuarto de control central, aunque la desventaja es que si uno de los enlaces punto a punto que la forman se rompe (o se desconecta debido a errores en la transmisión), la red deja de funcionar.

El control de transmisión que usa esta topología es distribuido y su modo de transferencia es de conmutación. La tecnología común que utiliza dicha topología se conoce con el nombre de token ring.

Token ring es una tecnología desarrollada por IBM, correspondiente al estándar IEEE 802.5. El diseño básico es un anillo de nodos que no superan 256, operando a 4 ó 16 Mbps. En token ring se utiliza un código de autorización llamado “token” que actúa como método de acceso al medio denominado “token passing”. El método de acceso al medio “token passing” trabaja de la siguiente forma. Si no hay mensaje, el token (tres bytes) es enviado a través del anillo. Cuando un nodo A con un mensaje a enviar recibe el token, retiene éste y envía el mensaje, el cual incluye un código de identificación del destinatario. Los nodos ignoran el mensaje si no es para sí mismo, en caso contrario, obtienen la

información. La información sigue viajando hasta que completa su trayectoria alrededor del anillo y llega al nodo A. Dicho nodo suelta el token para que pase nuevamente alrededor del anillo para futuros envíos de información.

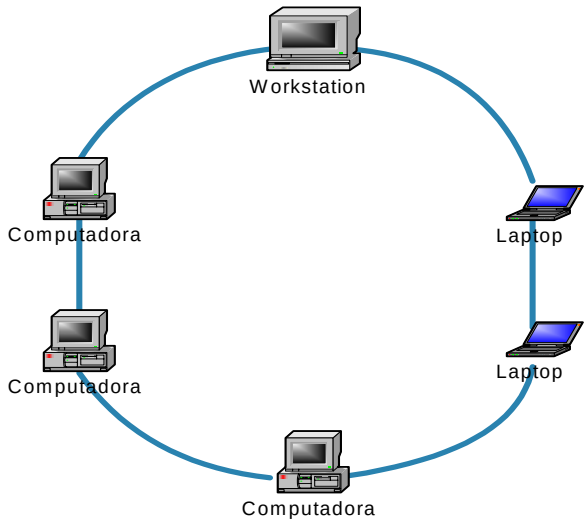


Figura 2.11 Diagrama de topología de anillo

2.3.2. Topología de bus

En esta topología no existe un CPU o similar que controle la comunicación entre los nodos. Cada nodo está conectado a un bus, donde cada uno actúa como si fuera parte de una red anillo, pero ninguno depende del nodo siguiente para que el flujo de información continúe, ni tampoco depende del nodo anterior para que la información llegue a él. La tecnología común que trabaja bajo una topología Bus es denominada Ethernet.

Ethernet fue desarrollada por Digital, Intel y Xerox, normalizada con IEEE 802.3. Ethernet distribuye paquetes de datos de longitud variable con una velocidad de 10 Mbps a los diferentes nodos dispersos a lo largo de un bus que comúnmente es cable coaxial. Los nodos separados hasta unos 50m de largo pueden ser también unidos por cable de par trenzado. Una red Ethernet puede estar formada hasta por 1024 nodos. Y no puede estar separado más de 2500 metros entre puntos finales.

Así como Token Ring utiliza un Token como acceso al medio, Ethernet se basa en el acceso al medio denominado CSMA/CD (Carrier Sense Multiple Access with Collision Detect). Es denominada Carrier Sense porque cada nodo es capaz de saber si la información que viaja en el bus es para si mismo o no. Multiple Access porque como se ha mencionado, un bus es compartido por todos los nodos que forman la red. Collision Detect porque cada nodo sabe si existe información que viaja en la red y es posible detectar y eliminar colisiones. Si choca la señal se pierde (collision).

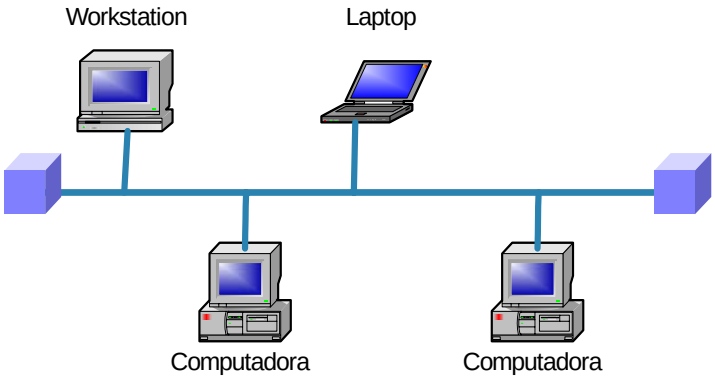


Figura 2.12 Diagrama de topología de bus

2.3.3. Topología de estrella

La topología de estrella consta de una unidad central que controla el flujo de información a través de la red. La topología estrella tiene limitaciones en cuanto a rendimiento y confiabilidad, ya que el tamaño de la red depende directamente de la capacidad del controlador central (número de conexiones que puede soportar) y en caso de fallar éste, todo el sistema deja de funcionar. Por otro lado, tiene la ventaja de poderse administrar únicamente administrando el dispositivo central.

En la topología estrella se tiene un control de transmisión centralizado y una forma de transferencia de conmutación.

2.3.4. Topología de árbol

La topología de árbol combina las características de la topología de estrella con la de bus. Consiste en un conjunto de redes estrella conectadas a un bus. Esta topología facilita la expansión de la red.

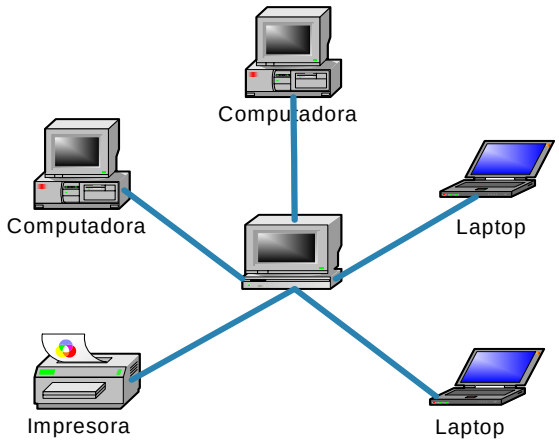


Figura 2.13 Diagrama de topología de estrella

2.3.5. Topología híbrida

Son las más comunes y se derivan de la combinación de topologías puras como lo son: estrella-estrella, bus-estrella, por ejemplo.

2.4. Ejemplos de redes de computadoras

Un número muy grande de redes se encuentran funcionando actualmente en todo el mundo, algunas de ellas son redes públicas operadas por proveedores de servicios portadores comunes o PTT, otras están dedicadas a la investigación, también hay redes en cooperativas operadas por los mismos usuarios y redes de tipo comercial o corporativo.

Las redes, por lo general, difieren en cuanto a su historia, administración, servicios que ofrecen, diseño técnico y usuarios. La historia y la administración pueden variar desde una red cuidadosamente elaborada por una sola organización, hasta una colección específica de máquinas, cuya conexión se fue realizando con el paso del tiempo, sin ningún plan maestro o administración central que la supervisara. Los servicios ofrecidos van desde una comunicación arbitraria de proceso a proceso, hasta llegar al correo electrónico, la transferencia de archivos, y el acceso y ejecución remota. Los diseños técnicos se diferencian en el medio de transmisión empleado, los algoritmos de encaminamiento y de denominación utilizados, el número y contenido de las capas presentes y los protocolos usados. Por último, las comunidades de usuarios pueden variar desde una sola corporación, hasta aquella que incluye todos las computadoras científicas que se encuentren en el mundo industrializado.

La posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios. La generalización de la computadora personal (PC) y de la red de área local (LAN) durante la década de los ochenta ha dado lugar a la posibilidad de acceder a información en bases de datos remotas; cargar aplicaciones desde puntos de ultramar; enviar mensajes a otros países y compartir ficheros, todo ello desde una computadora personal.

Las redes que permiten todo esto son equipos avanzados y complejos. Su eficacia se basa en la confluencia de muy diversos componentes. El diseño e implantación de una red mundial de computadoras es uno de los grandes milagros tecnológicos de las últimas décadas.

2.4.1. Redes de área local (LAN)

Es un sistema de comunicación entre computadoras, que permite compartir información y recursos, con la característica de que la distancia entre las computadoras debe ser pequeña.

La topología o la forma de conexión de la red, depende de algunos aspectos como la distancia entre las computadoras y el medio de comunicación entre ellas, ya que este determina la velocidad del sistema.

Las LAN se distinguen de otro tipo de redes por tres características: su tamaño, su tecnología de transmisión y su topología.

2.4.2. Redes de área extensa (WAN)

Es un sistema de comunicación entre computadoras, que permite compartir información y recursos, con la característica de que la distancia entre las computadoras es amplia (de una ciudad a otra, de un país a otro, de un continente a otro).

Son comúnmente dos o más redes de área local interconectadas, generalmente a través de una amplia zona geográfica.

Algunas redes de área extendida están conectadas mediante líneas rentadas a la compañía telefónica (destinadas para este propósito), soportes de fibra óptica y, otras por medio de sus propios enlaces terrestres y aéreos de satélite. Las redes de las grandes universidades pueden incluso contar con sus propios departamentos de telecomunicaciones que administran los enlaces entre las instalaciones y los satélites.

2.4.3. Redes de área metropolitana (MAN)

Una red de área metropolitana es básicamente una versión más grande de las redes LAN y normalmente se basan en tecnologías similares. Podría abarcar un grupo de oficinas o una ciudad, o bien ser sólo una red privada o pública.

El aspecto que distingue a esta red es el estándar utilizado para la implantación de ellas, este estándar ya se encuentra implementado y lleva las siglas de DQDB (Distributed Queue Dual Bus o bus dual de cola distribuida) o IEEE 802.6 DQDB.

Un aspecto importante de las redes MAN es que hay un medio de difusión, al cual se conectan todas las computadoras y esto simplifica mucho el diseño de la red a comparación de otras redes de computadoras.

2.4.4. Redes inalámbricas

Las redes inalámbricas se basan en el principio de conectar una antena a un circuito eléctrico en donde las ondas electromagnéticas se difunden para captarse por un receptor a una cierta distancia, cuentan con la ventaja de su instalación ya que es algo más sencilla que cualquier otra red.

Las redes inalámbricas tienen muchas formas. Una de ellas hace que las computadoras se comuniquen directamente con la red LAN inalámbrica de modo digital. Otra manera es usar un teléfono celular con un modem analógico común.

2.4.5. Redes privadas virtuales (VPN)

Una red privada virtual es una red donde todos los usuarios parecen estar en el mismo segmento de LAN, pero en realidad están a varias redes (generalmente públicas) de distancia. Para lograr esta funcionalidad, la tecnología de redes seguras, privadas y virtuales debe completar tres tareas.

Primero.- Deben poder pasar paquetes IP a través de un túnel en la red pública, de manera que dos segmentos de LAN remotos no parezcan estar separados por una red pública.

Segundo.- La solución debe agregar encriptación, tal que el tráfico que cruce por la red pública no pueda ser espiado, interceptado, leído o modificado.

Tercero.- Finalmente la solución tiene que ser capaz de autenticar positivamente cualquier extremo del enlace de comunicación de manera que un adversario no pueda acceder a los recursos del sistema.

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro, un firewall o los sitios permiten la conexión segura a través de internet. Las VPN's son una alternativa de costo útil para usar líneas alquiladas que conecten sucursales o para hacer negocios con clientes habituales. Los datos se encriptan y se envían a través de la conexión, protegiendo la información y el password.

2.4.6. Redes públicas y redes privadas

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción.

Estas operadoras incluyen a:

- Compañías de servicios de comunicación local.
- Compañías de servicios de comunicación a larga distancia. Una compañía de comunicación a larga distancia (IXC: Interexchange carriers) es un operador de telecomunicaciones que suministra servicios de larga distancia como AT&T, MCI, por mencionar algunos.
- Proveedores de servicios de valor añadido. Los proveedores de servicio de valor añadido (VACs: Value-added carriers) ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

Una red privada es una red de comunicaciones construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones.

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio. Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

2.4.7. Internet

El término "Internet" se deriva del término “internetworking” (trabajo en interred) que quiere decir redes conectándose con otras redes.

También llamada Telaraña de Area Mundial (World Wide Web).

Es una enorme red de redes que se enlaza a muchas de las redes científicas, de investigación y educacionales alrededor del mundo así como a un número creciente de redes comerciales.

2.5. Modelo OSI

El sistema de comunicaciones del modelo “OSI” estructura el proceso en varias capas que interaccionan entre sí. Una capa proporciona servicios a la capa superior siguiente y toma los servicios que le presta la siguiente capa inferior. De esta manera, el problema se divide en subproblemas más pequeños y por tanto más manejables.

Para que dos sistemas se comuniquen ambos deben tener el mismo modelo de capas. La capa más alta del sistema emisor se comunica con la capa más alta del sistema receptor, pero esta comunicación se realiza vía capas inferiores de cada sistema. La única comunicación directa entre capas de ambos sistemas es en la capa inferior (capa física). Los datos parten del emisor y cada capa le adjunta datos de control hasta que llegan a la capa física. En esta capa son pasados a la red y recibidos por la capa física del receptor. Luego irán siendo captados los datos de control de cada capa y pasados a una capa superior. Al final, los datos llegan limpios a la capa superior.

Cada capa tiene la facultad de poder segmentar los datos que le llegan en paquetes más pequeños para su propio manejo. Luego serán reensamblados en la capa paralela de la estación de destino.

El proceso de descomposición del problema de comunicaciones en capas hace posible la normalización de cada capa independiente y la posible modificación de una capa sin

afectar a las demás. Es preciso el empleo de normas y estándares para que dos sistemas puedan conocerse y comunicarse con plena exactitud, sin ambigüedades. Para que dos capas de dos sistemas se puedan comunicar es necesario que estén definidas las mismas funciones en ambos, aunque el cómo se implementen en la capa inferior de cada sistema sea diferente.

Las capas inferiores suministran a las superiores una serie de funciones o primitivas y una serie de parámetros. La implementación concreta de estas funciones está oculta para la capa superior, ésta sólo puede utilizar las funciones y los parámetros para comunicarse con la capa inferior (paso de datos y control).

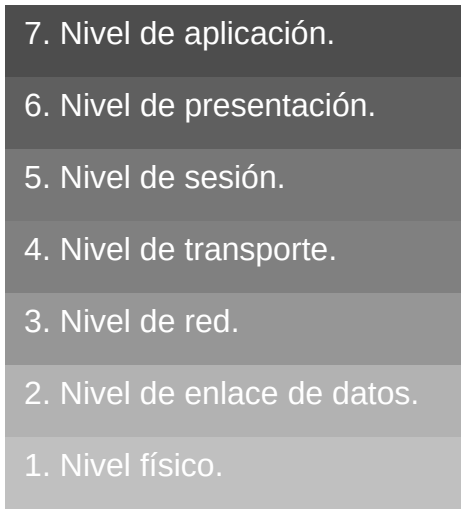


Figura 2.14 Modelo OSI

2.5.1. Las capas de OSI

Capa de aplicación: esta capa acoge a todas las aplicaciones que requieren la red. Permite que varias aplicaciones compartan la red. Algunos ejemplos de servicio son: correo electrónico, acceso a archivos remotos, ejecución de tareas remotas, directorios, administración de la red.

Capa de presentación: esta capa se encarga de definir los formatos de los datos y si es necesario, procesarlos para su envío. Este proceso puede ser el de compresión o el de paso a algún sistema de codificación. En resumen, se encarga de la sintaxis.

Capa de sesión: se encarga de proporcionar diálogo entre aplicaciones finales para el uso eficiente de las comunicaciones. Puede agrupar datos de diversas

aplicaciones para enviarlos juntos o incluso detener la comunicación y restablecer el envío tras realizar algún tipo de actividad.

Capa de transporte: esta capa se encarga de que los datos enviados y recibidos lleguen en orden, sin duplicar y sin errores. Puede ser servicio de transporte orientado a conexión (conmutación de circuitos o circuitos virtuales) o no orientado a conexión (datagramas).

Capa de red: esta capa se encarga de enlazar con la red y encaminar los datos hacia sus lugares o direcciones de destino. Para esto, se produce un diálogo con la red para establecer prioridades y encaminamientos. Esta y las dos capas inferiores son las encargadas de todo el proceso externo al propio sistema y que están tanto en terminales como en enlaces o repetidores.
Capa de enlace de datos: esta capa debe de encargarse de que los datos se envíen con seguridad a su destino y libres de errores. Cuando la conexión no es punto a punto, esta capa no puede asegurar su cometido y es la capa superior quien lo debe hacer.

Capa física: se encarga de pasar bits al medio físico y de suministrar servicios a la siguiente capa. Para ello debe conocer las características mecánicas, eléctricas, funcionales y de procedimiento de las líneas.

2.6. Arquitectura de protocolos TCP/IP

Hay una serie de razones por las que los protocolos TCP/IP han ganado a los OSI: Los TCP/IP estaban ya operativos antes de que OSI se normalizara, por lo que empezaron a utilizarse y luego el costo implicado en cambiar a OSI impidió este trasvase.

2.6.1. El enfoque TPC/IP

La filosofía de descomposición del problema de la comunicación en capas es similar que en OSI. El problema de OSI es que en una capa, todos los protocolos deben de tener un funcionamiento similar además de utilizar las funciones definidas en la capa inferior y de suministrar funciones a la capa superior. De esta forma, en OSI, dos sistemas deben tener en la misma capa los mismos protocolos. TCP/IP permite que en una misma capa pueda haber protocolos diferentes en funcionamiento siempre que utilicen las funciones suministradas por la capa inferior y provean a la superior de otras funciones.

En OSI, es imprescindible el paso de una capa a otra pasando por todas las intermedias. En TCP/IP esto no se hace imprescindible y es posible que una capa superior utilice directamente a cualquier capa inferior y no siempre pasando por las intermedias. Por ejemplo, en TCP/IP, una capa de aplicación puede utilizar servicios de una capa IP.

2.6.2. Arquitectura de protocolos TCP/IP

Aunque no hay un TCP/IP oficial, se pueden establecer 5 capas:

1. Capa de aplicación: proporciona comunicación entre procesos o aplicaciones en computadoras distintas.

2. Capa de transporte o computador-a-computador: encargada de transferir datos entre computadoras sin detalles de red pero con mecanismos de seguridad.

3. Capa de internet: se encarga de direccionar y guiar los datos desde el origen al destino a través de la red o redes intermedias.

4. Capa de acceso a la red: interfaz entre sistema final y la subred a la que está conectado.

5. Capa física: define las características del medio, señalización y codificación de las señales.

Normatividad para redes de computadoras

Capítulo 3

CAPÍTULO 3

NORMATIVIDAD PARA REDES DE COMPUTADORAS

3. Importancia de contar con una normatividad

La industria de la computación ha llegado a tener miles de formatos de datos y lenguajes, pero muy pocos estándares y normas que se empleen universalmente. Este tema es recurrente entre los proveedores de hardware y software y los planificadores industriales.

Sin importar lo mucho que se hable en el mercado acerca de compatibilidad de equipos, software o hardware, aparecen rutinariamente nuevos formatos y lenguajes. Los creadores de estándares están siempre tratando de moldear nuevos estándares en comunicaciones, en almacenamiento de datos, para realizar encriptación de datos, etcétera, mientras que los innovadores intentan crear un formato nuevo. Incluso una vez creados los estándares, se necesita cambiarlos o modificarlos tan pronto como el proveedor agregue una nueva característica a su producto.

Es evidente la necesidad de contar con herramientas que ayuden a manejar de la manera adecuada el intercambio de archivos, es decir, contar con la portabilidad necesaria para intercambiar datos, software y hardware entre distintos equipos de cómputo. Y de esto se desprende el inevitable uso de redes de computadoras.

El objetivo principal de una red de computadoras es conectar máquinas entre sí permitiendo su intercomunicación, además de poder compartir recursos entre sí. Las redes tienen características importantes:

1. El campo de acción en el que se desarrollan.
2. La velocidad de trasmisión de los datos que trasmiten.
3. Y las organizaciones a las que pertenecen.

Para que exista la comunicación entre distintas redes es necesario contar con estándares de redes y protocolos de comunicación, es decir que exista una normatividad para las redes de computadoras.

Se le llama protocolo de red o protocolo de comunicación, a los diversos conjuntos de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red. En este contexto, las entidades de las cuales se habla son programas de computadora o dispositivos electrónicos capaces de interactuar en una red.

Los protocolos de red establecen aspectos tales como:

- Las secuencias posibles de mensaje que pueden arribar durante el proceso de la comunicación.

- La sintaxis de los mensajes intercambiados.
- Estrategias para corregir los casos de error.
- Estrategias para asegurar la seguridad (autenticación, encriptación).

Los protocolos que son implementados en sistemas de comunicación que tienen un amplio impacto, suelen convertirse en estándares, debido a que la comunicación e intercambio de información (datos) es un factor fundamental en numerosos sistemas, y para asegurar tal comunicación se vuelve necesario copiar el diseño y funcionamiento a partir del ejemplo pre-existente.

Ejemplos de lo anterior son la IEEE que propone varios estándares para redes físicas, y la W3C (World Wide Web Consortium) que gestiona la definición aceptada sobre http[10]

3.1. Organismos internacionales

Si un formato o lenguaje se usa extensamente y otros lo copian, se convierte en un estándar y puede pasar a ser usado tan ampliamente como los estándares oficiales creados por organizaciones tales como:

ISO International Organization for Standardization

Define una estructura para la implementación de protocolos en siete estratos o capas. El control es transferido de un estrato al siguiente, comenzando en una estación por el estrato de aplicación, llegando hasta el estrato más bajo, luego por el canal hasta la otra estación y subiendo nuevamente la jerarquía.

Existe una funcionalidad similar en todas las redes de comunicaciones; sin embargo, algunos sistemas no-OSI existentes integran a menudo dos o tres capas funcionales en una sola. La mayoría de los fabricantes han accedido a apoyar el modelo OSI en una forma u otra.

IEEE (Instituto de ingenieros electrónicos y eléctricos).

Es la encargada de fijar los estándares de los elementos físicos de una red, cables, conectores, por mencionar algunos.

Los estándares se dividen en dos partes, cada una publicada como libro independiente. El estándar 802.1 es una introducción al grupo de estándares y define las primitivas de la interfaz. El estándar 802.2 describe la parte superior de la capa de enlace de datos, que usa el protocolo LLC (*Logical Link Control,* control de enlace lógico). Las partes 802.3 a 802.5 describen los tres estándares para la LAN, CSMA/CD, *token bus y token ring,* respectivamente. Cada estándar cubre la capa física y el protocolo de la subcapa MAC.

[10] Protocolo de transferencia de hipertexto (*HTTP, HyperText Transfer Protocol*)

Los comités 802 del IEEE se concentran principalmente en la interfaz física relacionada con los niveles físicos y de enlace de datos del modelo de referencia OSI. Los productos que siguen las normas 802 incluyen tarjetas de la *interfaz de red, bridges (puentes), routers (ruteadores)* y otros componentes utilizados para crear LAN's de par trenzado y cable coaxial. El nivel de enlace se divide en 2 subniveles MAC y LLC. Son diferentes en la capa física y en la subcapa MAC, pero son compatibles en la subcapa de enlace.

ARPANET (Advanced Research Projects Agency NETwork)

Red Avanzada de Agencias para Proyectos de Investigación. Red de Investigación fundada por DARPA[11] (originalmente ARPA) y construida por BBN[12], Inc., en 1969. Fue pionera en tecnología de conmutación de paquetes y fue la piedra angular original y la base de la ahora gigantesca Internet. En 1983, la parte militar de comunicaciones se dividió como MILNET[13].

Muchos países tienen organizaciones nacionales de estándares donde expertos de la industria y las universidades desarrollan estándares de todo tipo. Entre ellas se encuentran por ejemplo las que aparecen en la siguiente tabla :

País	Abreviatura	Nombre completo
Alemania	DIN	Deutsches Institut fuer Normung
Australia	SAA	Standards Australia
Dinamarca	DS	Dansk Standard
España	AENOR	Asociación Española de Normalización
Estados Unidos	ANSI	American National Standards Institute
Francia	AFNOR	Association Francaise de Normalisation
Italia	UNI	Ente Nazionale Italiano de Unificatione
Noruega	NSF	Norges Standardiseringsforbund
Nueva Zelanda	SANZ	Standards Association of New Zealand
Países Bajos	NNI	Nederlands Normalisatie-Instituut
Reino Unido	BSI	British Standards Institution

Tabla 3.1 Organizaciones de estandarización/normalización de algunos países del mundo

[11] DARPA: Defense Advanced Research Projects Agency – agencia de proyectos de investigación avanzada de defensa
[12] BBN: BBN Technologies (originalmente Bolt, Beranek and Newman)
[13] MILNET: red precursora de lo que actualmente conocemos como Internet

ANSI

Es la organización de estándares de los Estados Unidos. Debido a que muchos fabricantes de equipos de comunicaciones diseñan o desarrollan sus productos en Estados Unidos muchos estándares ANSI son de interés también en otros países. Además muchos estándares ANSI son adoptados posteriormente por ISO como estándares internacionales.

NIST (National Institute of Standards and Technology)

Es una agencia del Departamento de Comercio de los Estados Unidos, antes conocido como el NBS (National Bureau of Standards). Define estándares para la administración de los Estados Unidos.

ETSI (European Telecommunications Standards Institute)

Es una organización internacional dedicada principalmente a la estandarización de las telecomunicaciones europeas. Es miembro de la ITU-T. Entre sus misiones está elaborar especificaciones detalladas de los estándares internacionales adaptadas a la situación de Europa en los aspectos históricos, técnicos y regulatorios.

EIA (Electrical Industries Association)

Es una organización internacional que agrupa a la industria informática y que también participa en aspectos de la elaboración de estándares.

ECMA (European Computer Manufacturers Association)

Creada en 1961, es un foro de ámbito europeo donde expertos en proceso de datos se ponen de acuerdo y elevan propuestas para estandarización a ISO, ITU-T y otras organizaciones.

CEPT (Conference European of Post and Telecommunications)

Es una organización de las PTTs[14] europeas que participa en la implantación de estándares de telecomunicaciones en Europa. Sus documentos se denominan Norme Europeene de Telecommunication (NET). La CEPT está avalada por la Comunidad Europea.

[14] PTT: método para hablar en líneas half-duplex de comunicación

3.2. Normas, protocolos y estándares para redes de computadoras

TCP/IP

El Protocolo de Control de Transmisiones/Protocolo Internet (Transmision Control Protocol/Internet Protocol) es un conjunto de protocolos de comunicaciones desarrollado por la DARPA (Defense Advanced Research Projects Agency – agencia de proyectos de investigación avanzada de defensa) para intercomunicar sistemas diferentes. Se ejecuta en un gran número de computadoras VAX[15] y basadas en UNIX, además es utilizado por muchos fabricantes de hardware, desde los de computadoras personales hasta los de supercomputadoras. Es empleado por numerosas corporaciones y por casi todas las universidades y organizaciones federales de los Estados Unidos.

TELNET

Es un protocolo de comunicaciones que permite al usuario de una computadora con conexión a Internet, establecer una sesión como terminal remota de otro sistema de la Red. Si el usuario no dispone de una cuenta en la computadora remota, puede conectarse como usuario *anonymous* (anónimo) y acceder a los ficheros de libre distribución. Muchas máquinas ofrecen servicios de búsqueda en bases de datos usando este protocolo. En la actualidad se puede acceder a través de World Wide Web (WWW) a numerosos recursos que antes sólo estaban disponibles usando TELNET.

FTP

(File Transfer Protocol) Protocolo de Transferencia de Archivos
Un protocolo TCP/IP que es usado para conectarse a la red, listar directorios y copiar archivos. También puede traducir entre ASCII y EBCDIC[16].

FTP es el servicio de transferencia de archivos de Internet. Le permite mover archivos de una computadora a otra. No importa dónde se localicen estas dos computadoras, cómo están conectadas o si tienen o no el mismo sistema operativo. Al igual que TELNET, FTP ha provocado la proliferación de una amplia gama de datos y servicios. De hecho se puede encontrar cualquier cosa, desde opiniones legales hasta un software gratuito en una gran cantidad de bases de datos en línea, disponibles a las que se puede tener acceso mediante FTP.

[15] VAX: primera máquina comercial de arquitectura de 32 bits
[16] EBCDIC: Extended Binary Coded Decimal Interchange Code, código binario que representa caracteres alfanuméricos, controles y signos de puntuación.

SMTP (Simple Message Transfer Protocol)

Se usa para transmitir correo electrónico. Es transparente por completo para el usuario, pues estos así nunca se dan cuenta del trabajo del SMTP debido a que es un protocolo libre de problemas.

Kerberos

Es un protocolo de seguridad soportado en forma muy amplia. Este utiliza una aplicación especial llamada servidor de autenticidad para validar las contraseñas y esquemas de encriptado. Este protocolo es uno de los más seguros.

DNS (Domain Name Service)

Permite a una computadora con un nombre común convertirse en una dirección especial.

SNMP (Simple Network Manager Protocol)

Proporciona mensajes de cola y reporta problemas a través de una red hacia el administrador, usa el UDP[17] como mecanismo de transporte.

RPC (Remote Procedure Call)

Es un conjunto de funciones que permiten a una aplicación comunicarse con otra máquina (servidor). Atiende funciones de programas, códigos de retorno.

NFS (Network File System)

Conjunto de protocolos desarrollados por Sun MicroSystems para permitir a múltiples maquinas tener acceso a las direcciones de cada una de las tras de manera transparente.

TFTP (Trivial FTP)

Es un protocolo de transferencia de archivos muy sencillo que carece de seguridad. Ejecuta las mismas tareas que FTP pero usando un UDP como protocolo de transporte.

[17] UDP: protocolo del nivel de transporte basado en el intercambio de datagramas.

TCP

Es un protocolo de comunicación que proporciona transferencia confiable de datos. Es responsable de ensamblar los datos pasados de aplicaciones de capas superiores hacia paquetes estándar y asegurar que los datos se transfieran en forma segura.

Local talk

El protocolo LocalTalk fue desarrollado por Apple Computer, Inc. Para máquinas Macintosh. El método de acceso al medio es el CSMA/CA. (Carrier Sense Multiple Access with Collision Avoidance) Este método se diferencia en que la computadora anuncia su transmisión antes de realizarla. Mediante el uso de adaptadores LocalTalk y cables UTP especiales se puede crear una red de computadoras a través del puerto serie. El sistema operativo de estos establece relaciones punto a punto sin necesidad de software adicional aunque se puede crear una red cliente servidor con el software AppleShare. Con el protocolo LocalTalk se pueden utilizar topologías BUS, estrella o árbol usando cable UTP pero la velocidad de transmisión es muy inferior a la de Ethernet.

Token ring

El protocolo Token Ring fue desarrollado por IBM a mediados de los 80. El modo de acceso al medio está basado en el traspaso del testigo o token passing. En una red Token Ring las computadoras se conectan formando un anillo. Un testigo o token electrónico de una computadora a otra. Cuando se recibe este testigo se está en disposición de emitir datos. Estos viajan por el anillo hasta llegar a la estación receptora. Las redes Token Ring se montan sobre topologías estrella cableada o “star-wired” con par trenzado o fibra óptica. Se puede transmitir información a 4 o 16 Mbps.

El comité que se ocupa de los estándares de computadoras a nivel mundial es la IEEE en su división 802, los cuales se dedican a lo referente de sistema de red; están especificados los siguientes:

NORMA 802, características generales

La norma 802 creada por el IEEE está compuesta de las siguientes normas:

- 802.1 da una introducción al conjunto de normas y define las primitivas de interfaz, para interconexión de redes.
- 802.2 describe la parte superior de la capa de enlace que utiliza el protocolo LLC.
- 802.3 describe la norma CSMA/CD.
- 802.4 describe la norma token bus.
- 802.5 describe la norma token ring.
- 802.6 red de área metropolitana MAN.

- 802.7 grupo asesor para técnicas de banda ancha.
- 802.8 grupo asesor para técnicas de fibra óptica.
- 802.9 redes integradas para voz y datos.
- 802.10 seguridad de red.
- 802.11 redes inalámbricas.
- 802.12 LAN de acceso de prioridad bajo demanda (100VG-Any LAN).

Definición de interconexión de red 802.1 y control de enlaces lógicos 802.2

El IEEE 802.1 define la relación entre las normas 802 del IEEE y el modelo de referencia de la OSI. Este comité establece que las direcciones de las estaciones de la LAN sean de 48 bits para todas las normas 802, para que cada adaptador tenga una única dirección.

El control de enlaces lógicos 802.2 define el protocolo que asegura que los datos se transmiten de forma confiable a través del enlace de comunicaciones LLC *(Logical Link Control, Control de Enlaces Lógicos)*. En los bridges (puentes) estos dos subniveles se utilizan como un mecanismo modular de conmutación.

Un marco o “frame” que llega a una red ethernet y se destina a una red token ring, se le desmonta su cabecera o “header” de frame ethernet y se empaqueta con un “header” de token ring.

El LLC suministra los siguientes servicios:

- Servicio orientado a la conexión en el cual se establece una sesión con un destino y se libera cuando se completa la transferencia de datos.
- Servicios orientados a la conexión con reconocimiento parecido al anterior, en el cual se confirma la recepción de los paquetes.
- Servicio sin reconocimiento no orientado a la conexión en el cual no se establece una conexión ni se confirma su recepción.

Ethernet / IEEE 802.3

Ethernet fue inventada en el Xerox Palo Alto Research Center en los 70s por el Dr. Robert M. Metcalfe. Fue diseñada para soportar búsqueda en la "oficina del futuro," que incluía una de las primeras estaciones de trabajo personal del mundo, la Xerox Alto. El primer sistema Ethernet funcionaba aproximadamente a 3-Mbps y era conocido como "Ethernet experimental." Las especificaciones formales para Ethernet fueron publicadas en 1980 por un consorcio de fabricantes que crearon el estándar DEC-Intel-Xerox (DIX). Este impulso convirtió el Ethernet experimental en un sistema abierto y de calidad que opera a 10 Mbps. La tecnología Ethernet fue adoptada después como estándar por el comité de estándares LAN del Instituto de Ingenieros Eléctricos y Electrónicos (*Institute of Electrical and Electronics Engineers*) con la norma IEEE 802.

El estándar IEEE fue publicado por primera vez en 1985, bajo el título "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications." (IEEE 802.3 Portadora de Acceso Múltiple con Detección de Colisiones (CSMA/CD) Método de Acceso y Especificaciones Físicas). El estándar IEEE ha sido adoptado desde entonces por el *International Organization for Standardization* (ISO), lo que lo convierte en un estándar a escala mundial.

El estándar IEEE proporciona un sistema "tipo Ethernet" basado en el estándar original DIX. Todos los equipos Ethernet desde 1985 se construyen de acuerdo al estándar IEEE 802.3 Para ser exactos, deberíamos referirnos a Ethernet como "IEEE 802.3 CSMA/CD".

El estándar 802.3 es periódicamente puesto al día para incluir la nueva tecnología. Desde 1985 el estándar ha crecido para incluir los nuevos medios para el sistema Ethernet de 10 Mbps (par trenzado), así como las últimas especificaciones para el 100 Mbps Fast Ethernet.

El sistema Ethernet consta de tres elementos básicos:

1. El medio físico usado para transportar las señales Ethernet entre computadoras.
2. Una serie de reglas de control de acceso al medio incluidas en la interface que permite a múltiples computadores regular su acceso al medio de forma equitativa.
3. Una trama Ethernet que consiste en una serie estandarizada de bits usados para transportar los datos en el sistema.

Y los distintos estándares que de ésta se conforman, se muestran en la siguiente tabla:

Estándar Ethernet	Fecha	Descripción
Ethernet experimental	1972 (patentado en 1978)	2.94 Mbit/s sobre cable coaxial en topología de bus.
Ethernet II (DIX v2.0)	1982	10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
IEEE 802.3	1983	10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
802.3a	1985	10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 metros
802.3b	1985	10BROAD36
802.3c	1985	Especificación de repetidores de 10 Mbit/s
802.3d	1987	FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.

Estándar Ethernet	Fecha	Descripción
802.3e	1987	1BASE5 o StarLAN
802.3i	1990	10BASE-T 10 Mbit/s sobre par trenzado (UTP). Longitud máxima del segmento 100 metros.
802.3j	1993	10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
802.3u	1995	100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
802.3x	1997	Full Duplex (Transmision y recepción simultáneos) y control de flujo.
802.3y	1998	100BASE-T2 100 Mbit/s sobre par trenzado (UTP). Longitud máxima del segmento 100 metros
802.3z	1998	1000BASE-X Ethernet de 1 Gbit/s sobre coaxial.
802.3ab	1999	1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado
802.3aq	en proceso	10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.
802.3ar	en proceso	Gestión de Congestión
802.3as	en proceso	Extensión de la trama

Tabla 3.2 Estándares Ethernet

El protocolo CSMA/CD

El protocolo CSMA/CD funciona de algún modo como una conversación en una habitación oscura. Todo el mundo escucha hasta que se produce un periodo de silencio, antes de hablar (sin portadora). Una vez que hay silencio, todo el mundo tiene las mismas oportunidades de decir algo (acceso múltiple). Si dos personas empiezan a hablar al mismo tiempo, se dan cuenta de ello y dejan de hablar (detección de colisiones).

En términos de ethernet, cada interface debe esperar hasta que no haya ninguna señal en el canal, entonces puede empezar a transmitir. Si alguna otra interface esta transmitiendo habrá una señal en el canal, a la cual se llama portadora. Todos las demás interfaces deben esperar hasta que la portadora cese antes de intentar transmitir, este proceso es llamado sin portadora.

Todas las interfaces ethernet tienen las mismas posibilidades de mandar tramas a la red. Ninguna tiene una prioridad mayor que las demás, y reina la democracia. Esto es lo que significa Acceso Múltiple. Como la señal tarda un tiempo finito en viajar de un extremo al otro de un segmento ethernet, los primeros bits de una trama no llegan simultáneamente a todas las partes de la red. Así pues, es posible que dos interfaces escuchen que el canal

esta vacío y comiencen a transmitir sus tramas simultáneamente. Cuando esto ocurre, El sistema Ethernet tiene un modo de detectar la "colisión" de las señales e interrumpir la transmisión y reenviar las tramas. A esto se le llama detección de colisiones.

El protocolo CSMA/CD esta diseñado para permitir un fácil acceso al medio compartido, con lo que todas las estaciones tienen oportunidad de usar la red. Después de cada transmisión todas las estaciones usan el protocolo CSMA/CD para determinar cuál es la siguiente en usar el canal.

Colisiones

Si más de una estación comienza a transmitir en el canal ethernet al mismo tiempo las señales colisionan. Esto es notificado a las estaciones, que inmediatamente reestructuran sus transmisiones usando un algoritmo especialmente diseñado. Como parte de este algoritmo, cada una de las estaciones involucradas elige un intervalo de tiempo aleatorio para volver a intentar retransmitir la trama, lo que impide que todas vuelvan a intentarlo al mismo tiempo.

La palabra colisión no debe interpretarse como algo malo, no es un fallo de la red, se trata de algo absolutamente normal y esperado en una red ethernet, e indica simplemente que el protocolo CSMA/CD funciona como es debido. Cuantas más estaciones se añaden a una red ethernet, y cuanto mas se incrementa el trafico en la red, ocurrirán mas colisiones como parte del funcionamiento normal de ethernet.

El diseño del sistema asegura que la mayoría de las colisiones en una red ethernet que no esté sobrecargada, serán resueltas en microsegundos, (millonésimas de segundo). Una colisión normal no supone perdida de datos. En caso de colisión la interface ethernet espera durante un número de microsegundos, y después retransmite los datos.

En redes con tráfico denso pueden darse múltiples colisiones para los intentos de transmisión de una trama dada. Esto también es normal. Si se da esta situación, las estaciones involucradas eligen aleatoriamente tiempos cada vez mayores para intentar la retransmisión.

Sólo tras 16 colisiones consecutivas para los intentos de transmisión de una misma trama, esta será descartada por la interface. Esto únicamente puede ocurrir si el canal esta sobrecargado por un periodo muy largo, o si está dañado en alguna parte.

Protocolos de alto nivel y direcciones Ethernet

Las computadoras conectadas mediante ethernet pueden enviar datos de aplicaciones a otras utilizando software de protocolos de alto nivel, como el protocolo TCP/IP utilizado en Internet. Los paquetes del protocolo de alto nivel son transportados entre las computadoras en el campo de datos de las tramas ethernet.

El sistema de transporte de datos en los protocolos de alto nivel y el sistema Ethernet son entidades independientes que colaboran para el reparto de los datos entre las computadoras. Los protocolos de alto nivel tienen su propio sistema de direccionamiento, como las direcciones de 32 bits utilizadas en la versión actual de IP.

IEEE 802.4 Token bus (paso de testigo en bus)

Físicamente es un cable lineal, al cual se conectan las estaciones. Estas, lógicamente están organizadas en un anillo, en el que cada una de las estaciones conoce la dirección de la estación ubicada a su "izquierda" y "derecha".

El orden físico en el que se encuentran conectadas las estaciones al cable no es importante. Cada estación recibe todas las tramas descartando las que no le están dirigidas. El paso de testigo es enviar la trama de testigo al vecino lógico en el anillo, independientemente del lugar físico donde se encuentre la estación en el cable.

Protocolo de subcapa MAC para 802.4 token bus

Al iniciar el anillo, las estaciones se le introducen en forma ordenada, de acuerdo con la dirección de la estación, desde la más alta a la más baja. El testigo se pasa también desde la más alta a la más baja. Para transmitir, la estación debe adquirir el testigo, el cual es usado durante un cierto tiempo, para después pasar el testigo en el orden adquirido. Si una estación no tiene información para transmitir, entregará el testigo inmediatamente después de recibirlo.

IEEE 802.5 o Token ring

La red token ring fue desarrollada originalmente por IBM en los años 70 y continúa siendo la red de área local primaria de dicha empresa y la segunda en importancia después de la especificación IEEE 802.3. La especificación IEEE 802.5 es casi idéntica y completamente compatible con la red token ring IBM. El término token ring es generalmente utilizado tanto para referirse a las redes token ring IBM como a las redes IEEE 802.5.

Las redes token ring IBM especifican una estrella con todas las estaciones conectadas a un dispositivo denominado *multistation access unit* (MSAU), en tanto que IEEE 802.5 no especifica una topología. Otra diferencia es que IEEE 802.5 no especifica un medio de transmisión, mientras que IBM especifica el uso de par trenzado.

Token Ring e IEEE 802.5 son ejemplos primarios de las redes token passing. Las redes token passing mueven una pequeña trama, denominada “token”, alrededor de la red. Posesionándose de este token se gana el derecho a transmitir. Si un nodo recibe el token y no tiene información que transmitir, simplemente pasa el token a la estación siguiente. Cada estación puede retener el token por un período de tiempo determinado. Si una

estación tiene el token y tiene información que transmitir, se posesiona del token, altera un bit del token, anexa la información que desea transmitir y finalmente envía la información a la siguiente estación del anillo. Mientras la información circula por el anillo, no hay token en la red, así que otra estación que desee transmitir debe esperar. A raíz de esto no existen colisiones en este tipo de red. Un nuevo token debe ser liberado cuando la transmisión se ha completado.

La información circula por el anillo hasta que es encontrada por la estación de destino, la cual copia la información para su posterior procesamiento. La información continúa circulando por el anillo hasta que finalmente es removida cuando se encuentra con la estación que la envió. La estación que envía revisa la trama retornada para verificar que fue recibida y copiada por la estación de destino.

A diferencia de las redes CSMA/CD, las redes token ring son deterministas. En otras palabras, es posible calcular el tiempo máximo que debería transcurrir antes de que cualquier estación pueda transmitir, esto hace ideal a las redes token ring para aplicaciones donde el retardo debe ser predecible y la operación robusta.

IEEE 802.6 Red de área metropolitana (MAN)

Define un protocolo de alta velocidad en el cual las estaciones enlazadas comparten un bus doble de fibra óptica que utiliza un método de acceso llamado bus dual de cola distribuida o *DQDB Distributed Queue Dual Bus*.
DQDB es una red de transmisión de celdas que conmuta celdas con una longitud fija de 53 bytes, por lo tanto, es compatible con la ISDN de banda ancha ISDN-B y ATM. La conmutación de celdas tiene lugar en el nivel de control de enlaces lógicos 802.2.

IEEE 802.7 Grupo asesor para técnicas de banda ancha

Proporciona asesoría técnica a otros subcomités en técnicas de conexión de red de banda ancha.

IEEE 802.8 Grupo asesor para técnicas de fibra óptica

Proporciona asesoría técnica a otros subcomités en redes de fibra óptica como alternativa a las redes actuales basadas en cobre.

IEEE 802.9 Redes integradas para voz, datos y vídeo

Tanto para LANs 802 como para ISDNs. La especificación se denomina *IVD Integrated Voice and Data*. El servicio proporciona un flujo multiplexado que puede llevar información de datos y voz por los canales que conectan las dos estaciones sobre cables de par trenzado de cobre.

IEEE 802.10 Seguridad de red

Grupo que trabaja en la definición de un modelo normalizado de seguridad que opera sobre distintas redes e incorpora métodos de autentificación y de cifrado.

IEEE 802.11 Redes inalámbricas

Comité que trabaja en la normalización de medios como la radio de amplio espectro, radio de banda angosta, infrarrojos y transmisiones sobre líneas de potencia.

IEEE 802.12 LAN de acceso de prioridad bajo demanda (100VG-AnyLAN)

Comité que define la norma ethernet a 100 Mbps con el método de acceso de prioridad bajo demanda propuesto por la Hewlett Packard y otros fabricantes. El cable especificado es un par trenzado de 4 hilos de cobre utilizándose un concentrador central para controlar el acceso al cable. Las prioridades están disponibles para soportar la distribución en tiempo real de aplicaciones multimedia.

Los concentradores 100VG-AnyLAN controlan el acceso a la red con lo cual eliminan la necesidad de que las estaciones de trabajo detecten una señal portadora, como sucede en el CSMA/CD de la norma ethernet. Cuando una estación necesita transmitir, envía una petición al concentrador. Todas las transmisiones se dirigen a través del concentrador, que ofrece una conmutación rápida hacia el nodo destino. Emisor y receptor son los únicos involucrados en las transmisiones, a diferencia del CSMA/CD donde la transmisión es difundida por toda la red. Si múltiples peticiones de transmisión llegan al concentrador, primero se sirve la de mayor prioridad. Si dos estaciones de trabajo hacen la solicitud con la misma prioridad y al mismo tiempo, se van alternando para darles servicio. Este método de trabajo es mejor que CSMA/CD.

IEEE 802.14

Define los estándares de módem por cable.

IEEE 802.15 (WPAN, *Wireless Personal Area Networks*)

Define las redes de área personal sin cables.

IEEE 802.16

Define los estándares sin cable de banda ancha.

Estándares de estructuras de red

10 base 5: describe una red tipo bus con cable coaxial grueso o RG48, banda base, que puede transmitir a 10 Mbps a una distancia máxima de 500m.

10 base 2: describe una red tipo bus con cable coaxial delgado RG58, banda base y que puede transmitir a 10 Mbps a una distancia de 200m, a esta se le conoce como cheaper-ethernet.

10 base T: tipo de red que hoy en día es una de las más usadas por su fácil estructuración y control central, en ésta se utiliza cable UTP y se puede transmitir de 10 Mbps a 1Gbps.

El desarrollo tecnológico moderno ha hecho que la velocidad de las redes sea cada vez más alta, tecnologías de red como fast ethernet la cual trabaja a 100 Mbps puede manejar cables como el UTP categoría 5 o la recién liberada Gigaethernet la cual mantiene velocidades de Gbps.

Protocolos de transporte

Los protocolos de transporte operan en los niveles de transporte y de red del modelo OSI. Son los responsables de agregar información de la dirección software a los datos y de garantizar la fiabilidad de la transmisión. Los protocolos de transporte se vinculan con la tarjeta de red (NIC) para ofrecer comunicación. Durante la instalación y la configuración de Windows NT, siempre se deben enlazar estos protocolos a una tarjeta de red específica.

Estándares de seguridad

NIVEL D1

El nivel D1 es la forma más elemental de seguridad disponible. Este estándar parte de la base que asegura, que todo el sistema no es confiable. No hay protección disponible para el hardware, el sistema operativo se compromete con facilidad, y no hay autenticidad con respecto a los usuarios y sus derechos, para tener acceso a la información que se encuentra en la computadora. Este nivel de seguridad, se refiere por lo general a los sistemas operativos como MS-DOS, MS-Windows y System 7.x de Apple Macintosh.

NIVEL C1

El nivel C1 tiene dos subniveles de seguridad C1 y C2. El nivel C1, o sistema de protección de seguridad discrecional, describe la seguridad disponible en un sistema típico UNIX. Existe algún nivel de protección para el hardware, puesto que no puede comprometerse tan fácil, aunque todavía es posible. Los usuarios deberán identificarse así mismos con el sistema por medio de un nombre de usuario y una contraseña. Esta combinación se utiliza para determinar que derechos de acceso a los programas e

información tiene cada usuario. Estos derechos de acceso son permisos para archivos y directorios. Estos controles de acceso discrecional, habilitan al dueño del archivo o directorios, o al administrador del sistema, a evitar que algunas personas tengan acceso a los programas e información de otras personas. Sin embargo, la cuenta de administración del sistema no está restringida a realizar cualquier actividad. En consecuencia, un administrador del sistema sin escrúpulos, puede comprometer con facilidad la seguridad del sistema sin que nadie se entere.

NIVEL C2

El nivel C2, fue diseñado para ayudar a solucionar tales hechos. Junto con las características de C1, el nivel C2 incluye características de seguridad adicional, que crean un medio de acceso controlado. Este medio tiene la capacidad de reforzar las restricciones a los usuarios en la ejecución de algunos comandos o el acceso a algunos archivos, basados no sólo en permisos sino en niveles de autorización. Además la seguridad de este nivel requiere auditorias del sistema. Esto incluye la creación de un registro de auditoria para cada evento que ocurre en el sistema. La auditoria se utiliza para mantener los registros de todos los eventos relacionados con la seguridad, como aquellas actividades practicadas por el administrador del sistema. La auditoria requiere de autenticación adicional. La desventaja es que requiere un procesador adicional y recursos de discos del subsistema.

NIVEL B1

En nivel B de seguridad tiene tres niveles. El B1, o protección de seguridad etiquetada, es el primer nivel que soporta seguridad multinivel, como la secreta y la ultrasecreta. Este nivel parte del principio de que un objeto bajo control de acceso obligatorio, no puede aceptar cambios en los permisos hechos por el dueño del archivo.

NIVEL B2

El nivel B2, conocido como protección estructurada, requiere que se etiquete cada objeto, los dispositivos como discos duros, cintas, terminales, etc. podrán tener asignado un nivel sencillo o múltiple de seguridad. Este es el primer nivel que empieza a referirse al problema de un objeto a un nivel más elevado de seguridad en comunicación con otro objeto a un nivel interior.

NIVEL B3

El nivel B3, o el nivel de demonios de seguridad, refuerza a los demonios con la instalación de hardware. Por ejemplo, el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado, o la modificación de

objetos en diferentes dominios de seguridad. Este nivel requiere que la terminal del usuario conecte al sistema, por medio de una ruta de acceso segura.

NIVEL A

El nivel A, o nivel de diseño verificado, es hasta el momento el nivel más elevado de seguridad. Incluye un proceso exhaustivo de diseño, control y verificación. Para lograr este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse, el diseño requiere ser verificado en forma matemática, además es necesario realizar un análisis de los canales encubiertos y de la distribución confiable.

Políticas, normas y procedimientos para la implementación de redes de computadoras

Capítulo 4

CAPÍTULO 4

POLÍTICAS, NORMAS Y PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE REDES DE COMPUTADORAS

4. Introducción

Las políticas en la empresa son necesarias para poner en rumbo a todos los integrantes de una organización; con las políticas se sabe hacia donde deberán converger los esfuerzos conjuntos de trabajadores y directivos.

Sin políticas, una empresa no controla su futuro, es un barco a punto de naufragar, lo único que puede hacer es tratar de evitar el colapso, lidiando cada tormenta que se presenta con una tripulación pobremente coordinada, que desperdicia gran cantidad de recursos y esfuerzo individual, y de lo que podemos visualizar un final previsible: el agotamiento y el desastre.

La política es la luz del faro que guía a la embarcación hacia el puerto próximo, ahora todos saben hacia donde deben ir para llegar a salvo, y salen de nuevo con la sapiencia de encontrar una nueva luz, otro faro que los orientará a buen camino.

Una política de calidad es el enunciado que marca la dirección hacia donde se dirigirá la organización, por eso es necesario que tenga términos que sean fáciles de medir, sus puntos clave son:

- Satisfacción al “cliente”
- Cumplimiento de los “requisitos “
- “Mejora continua”

Ahora, debemos tener en cuenta, que para que una organización funcione de manera eficaz, tiene que identificar y gestionar todas las actividades relacionadas entre sí, una actividad que utiliza recursos y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados, se le llama proceso.

La aplicación de un sistema de procesos dentro de una empresa y la adecuada identificación de interacciones entre éstos, se conoce como “enfoque basado en procesos”, es decir, la identificación y gestión sistemática de los procesos empleados en la organización y en particular las interacciones que existen entre tales procesos.

La ventaja de este modo de trabajo es el control continuo que se da sobre los vínculos entre los procesos individuales dentro del sistema de procesos, así como, la combinación entre ellos.

Establecidos los lineamientos sobre lo que se ha de trabajar, este capitulo se encargará de establecer las políticas, las normas y los procedimientos asociados a éstas. Se cubrirán todos los requerimientos para la instalación de una red de computadoras usando un enfoque basado en procesos de calidad.

Veremos entonces las políticas que han de guiar a la empresa para realizar la adquisición de los equipos, su instalación, los locales de instalación, la seguridad en la red, el mantenimiento que requieren las distintas redes de computadoras; además, se convendrá y se darán recomendaciones para los usuarios y administradores de la red, que permitan obtener el máximo rendimiento y en consecuencia el máximo beneficio de la misma.

4.1. Adquisiciones

4.1.1. Política de adquisición

Realizar la compra de todos los bienes e insumos necesarios para la instalación de los servicios de red requeridos, incluyendo el software para la instalación, funcionamiento y mantenimiento de la red; refrendando el compromiso de eficiencia y competitividad cumpliendo con los requisitos de: tiempo, costo y calidad, a través de la mejora continua de los procedimientos de la empresa.

4.1.2. Norma de Adquisición

La adquisición de cualquier equipo necesario para la instalación de una red de computadoras debe asegurar que se cumplen los requisitos de compra especificados. Asimismo, debe establecer mecanismos adecuados de evaluación y selección de los proveedores, en función de la capacidad de estos para suministrar en tiempo y forma el equipo requerido. En el caso de la adquisición o contratación de servicios, estos deben ser sujetos de una evaluación continua con el fin de dar cumplimento a las políticas de la empresa.

4.1.3. Procedimiento para la adquisición de servicios, equipo nuevo de red y software

Introducción

Sin duda alguna, la adquisición de equipo nuevo puede resultar un verdadero dolor de cabeza ya que involucra muchos factores que afectan directamente la calidad de la instalación de la red, por un lado se tiene el factor económico, causa primordial en la decisión de la contratación de un servicio, muchas veces preferimos lo barato sobre lo caro, aunque no siempre es lo mejor. Y por otro, se tiene el factor tiempo, donde la capacidad de respuesta de nuestro proveedor juega un papel muy importante, ya que de

esto dependerá que los plazos de instalación sean cumplidos. Por ello, se hace necesario implantar un procedimiento documentado, donde se justifiquen los pasos a seguir para la adquisición de equipo nuevo de red, sin hacer de lado las exigencias del cliente, así como la durabilidad de la instalación y retribución económica de la inversión hecha en un mediano plazo.

Por el lado de la adquisición o contratación de servicios externos, es necesario contar con controles adecuados donde se establezcan parámetros de calidad claros, en base a la eficiencia de la empresa contratada para prestar el servicio, así como su costo y valores agregados de servicios al cliente.

El siguiente procedimiento, tiene como fin, proporcionar una base sólida en cuanto a la toma de decisiones en la adquisición de equipo y/o servicios en la instalación de redes de computadoras.

Objetivos

- Definir las actividades necesarias para la adquisición de equipo nuevo de red, que cumplan con los estándares de calidad requeridos por la organización.
- Establecer los mecanismos adecuados de control para el caso de la contratación de servicios externos.
- Definir los lineamientos necesarios para el control del proceso de adquisición, así como el establecimiento de indicadores a la salida del proceso.

Alcance

El presente procedimiento es aplicable al área de compras o adquisiciones en la instalación de una red de computadoras.

Procedimiento

Referente a los equipos de cómputo

a) De acuerdo a la planeación estratégica de la empresa, se deberá hacer un análisis de crecimiento para el mediano plazo, esto con el fin de estimar la cantidad de equipo ha adquirir por cada departamento.
b) Programar reuniones con el encargado del presupuesto para establecer las posibilidades reales de adquisición del equipo de cómputo.
c) Determinar las características idóneas del equipo de cómputo, tomando como parámetros de discriminación las áreas a las que se va a estar dedicado. Así pues, podemos dedicar un equipo más robusto a las áreas donde, el tiempo de

procesamiento de datos sea clave, la capacidad de almacenamiento masivo indispensable, y el accionar ante las peticiones de los usuarios deba ser lo más eficiente posible. Por otro lado, un equipo menos robustos suele ser suficiente en áreas donde la demanda de recursos no sea tan grande, tal es el caso de accesos a Internet, procesadores de texto, hojas de cálculo entre otros.

d) Si la cantidad de equipos a adquirir excede un número suficientemente grande de unidades, será necesario hacer al menos 3 cotizaciones distintas con 3 diferentes proveedores de equipo de cómputo, esto con el fin de garantizar que el derroche de recursos sea el más eficiente posible.
e) El proveedor deberá tener las siguientes características: reconocido prestigio a nivel nacional; soporte de mantenimiento adecuado (personal especializado, stock de repuestos); local apropiado; canales de comunicación con el cliente eficientes; cartera de clientes con equipos equivalentes adquiridos; y tiempo de entrega oportunos.
f) Con respecto a los precios se debe considerar lo siguiente: condiciones de pago; desglose de componentes de configuración de cada equipo adquirido; descuentos por volumen; costos de mantenimiento.
g) Si la cantidad de equipos de cómputo es de pequeña a mediana, bastará con solicitar entrevistas con el personal de ventas del proveedor deseado, con el fin de negociar el precio de cada equipo.
h) De conformidad con el proveedor se establecen los tiempos y lugar de entrega del equipo adquirido, garantía, y formas de devolución del equipo defectuoso si es que procediese.

Referente a los equipos de comunicaciones

a) De acuerdo a la planeación estratégica de la empresa, se deberá hacer un análisis de crecimiento para el mediano plazo, esto con el fin de estimar la cantidad de equipo ha adquirir por cada departamento.
b) Programar reuniones con el encargado del presupuesto para establecer las posibilidades reales de adquisición del equipo de cómputo.
c) Determinar las características idóneas del equipo de red necesario para la implantación de esta. La organización debe realizar un estudio de factibilidad basándose en los incisos siguientes.

    a. Determinar las características del entorno físico, puesto que se desea implantar una red de computadoras, necesitamos encontrar la manera de establecer contacto entre los diferentes dispositivos, lo cual permitirá decidir la forma en que se pueden establecer las conexiones necesarias y con qué tipo de equipo es posible realizarlas.
    b. Número y tipo de usuarios, gran parte del diseño de la red de computadoras es debido a esto, ya que el número de usuarios de la red además de darle su diseño esencial, nos obliga a considerar el uso de cierto tipo de equipo (servidores, switchs, routers entre otros), permitiendo una conexión y administración adecuada de la red.

c. Prestaciones técnicas, la adquisición de todo equipo de red debe satisfacer las necesidades de la misma a un mediano plazo, la organización debe preferir aquel equipo que le permita expandirla.
d. Seguridad, ante todo la organización debe contar con equipo de red que le permita salvaguardar la integridad de la información de sus usuarios, equipos tales como firewalls son recomendados.
e. Integración e interoperabilidad con otras redes, la organización debe considerar que el proyecto puede interactuar con otros sistemas de distinta naturaleza, ya sea a nivel físico o lógico; por lo tanto se debe tener especial cuidado en la adquisición de equipo que posibilite la integración e interacción con otras redes.

d) Si la cantidad de equipos a adquirir excede un número suficientemente grande de unidades, será necesario hacer al menos 3 cotizaciones distintas con 3 diferente proveedores de equipo de cómputo, esto con el fin de garantizar que el derroche de recursos sea el más eficiente posible.
e) Si la cantidad de equipos de red es de pequeña a mediana, bastará con solicitar entrevistas con el personal de ventas del proveedor deseado con el fin de negociar el precio de cada equipo.
f) De conformidad con el proveedor se establecen los tiempos y lugar de entrega del equipo adquirido, garantía, y formas de devolución del equipo defectuoso si es que procediese.

Referente a los servicios de telecomunicaciones

a) De acuerdo a la planeación estratégica de la empresa, se deberá hacer un análisis de crecimiento para el mediano plazo, esto con el fin de estimar el tipo de servicio de comunicaciones a adquirir.
b) Programar reuniones con el encargado del presupuesto para establecer las posibilidades reales de adquisición del equipo de cómputo.
c) La organización debe realizar un estudio de factibilidad en base a los siguientes incisos.

a. Determinar la relación costo-beneficio de cada uno de los proveedores de servicios de telecomunicaciones existentes en el mercado.
b. La organización debe preferir aquellos que cuentan con certificaciones de calidad por ejemplo ISO 9001:2000, en el área de servicios al cliente.
c. La organización debe preferir aquellos prestadores de servicio que cuenten con planes de contingencia en caso de que algún siniestro, llegue a afectar la prestación del servicio.

d) Finalmente, si es posible, solicitar reuniones con las personas encargadas de la empresa a contratar, para conocer de primera mano la forma en que el servicio se va a prestar.

e) De conformidad con el proveedor se establecen los tiempos y lugar de la prestación del servicio, garantía, y formas de comunicación con la empresa, en caso de fallo o caída del servicio.

Referente al software

a) La selección del software requerido por cada organización, debe ir de acuerdo con el plan estratégico de sistemas y sustentado por un estudio elaborado por el departamento de sistemas, en el cual se deben enfatizar las características y volumen de información que ameritan sistematización, así como una evaluación del costo aproximado de la inversión.
b) Para realizar cualquier adquisición de software se deberán considerar los siguientes incisos:

    a. Solicitud de propuesta, los parámetros sobre los cuales debe medirse dicha solicitud son los objetivos y las políticas de la empresa, así como las metas que se pretende cumplir con dicha adquisición.
    b. Evaluación de la propuesta, previamente debe llevarse a cabo una investigación con el propósito de establecer con seguridad el tipo de software requerido. Posteriormente se debe integrar toda la información obtenida de dicha investigación y así poder establecer la operatividad del software a adquirir.
    c. Financiamiento, las fuentes de financiamiento son principalmente instituciones bancarias a través de créditos. Verificar si el proveedor acepta este tipo de pago.
    d. Negociación de contrato, la negociación de contrato debe incluir todos los aspectos de operación de software y del hardware a implementarse, entre los que se incluyen: actualizaciones, innovaciones, capacitación, asesoría técnica, etcétera.

c) Alguna de las características que debe reunir el proveedor de software son:

    a. Reconocido prestigio a nivel nacional (y mundial si se considerase necesario)
    b. Soporte técnico en instalación
    c. Ayuda en problemas
    d. Personal especializado en la atención al cliente
    e. Tiempo de atención
    f. Servicios de capacitación tales como cursos, materiales, expositores, (si se considerase necesario) etcétera
    g. Cartera de clientes de software iguales a los adquiridos
    h. Documentación y facilidad de uso

d) Con respecto a los costos se debe considerar lo siguiente:

    a. Condiciones de pago
    b. Local de distribución

   c. Posibilidad de inclusión de entrenamiento en el uso del software (si es necesario)
   d. Costos de mantenimiento

e) Programar reuniones con el encargado del presupuesto para establecer las posibilidades reales de adquisición del software solicitado.
f) De conformidad con el proveedor se establecen los tiempos y lugar de entrega del software, servicio, garantía, y formas de comunicación con la empresa, en caso de cualquier fallo.

Referente al mobiliario

a) De acuerdo a la planeación estratégica de la empresa, se deberá hacer un análisis de crecimiento para el mediano plazo, esto con el fin de estimar la cantidad de mobiliario ha adquirir por cada departamento.
b) Programar reuniones con el encargado del presupuesto para establecer las posibilidades reales de adquisición del equipo de cómputo.
c) Determinar las características idóneas del mobiliario a usar por el personal. La organización debe realizar un estudio de factibilidad con ayuda de los incisos siguientes.

   a. Determinar los requisitos de los usuarios en base a su lugar de trabajo, esto es, adquirir mobiliario que incite a la labor diaria, y no a la pereza.
   b. Determinar la cantidad de espacio disponible para la asignación de los cubículos de trabajo, evitar en lo posible las aglomeraciones en los pasillos y la cercanía con las ventanas.

d) Lo anterior no significa que el lugar de trabajo sea reducido y con poca luz, por el contrario, la organización debe asegurar que el ambiente de trabajo sea idóneo para el correcto desempeño de las labores diarias.
e) Tomar en cuenta que el mobiliario va a ser parte importante en la organización, y que más que un gasto es una inversión, ya que los empleados son los que pasaran gran parte del tiempo en ellos.
f) De conformidad con el proveedor se establecen los tiempos y lugar de entrega del mobiliario adquirido, garantía, y formas de devolución del mobiliario defectuoso si es que procediese.

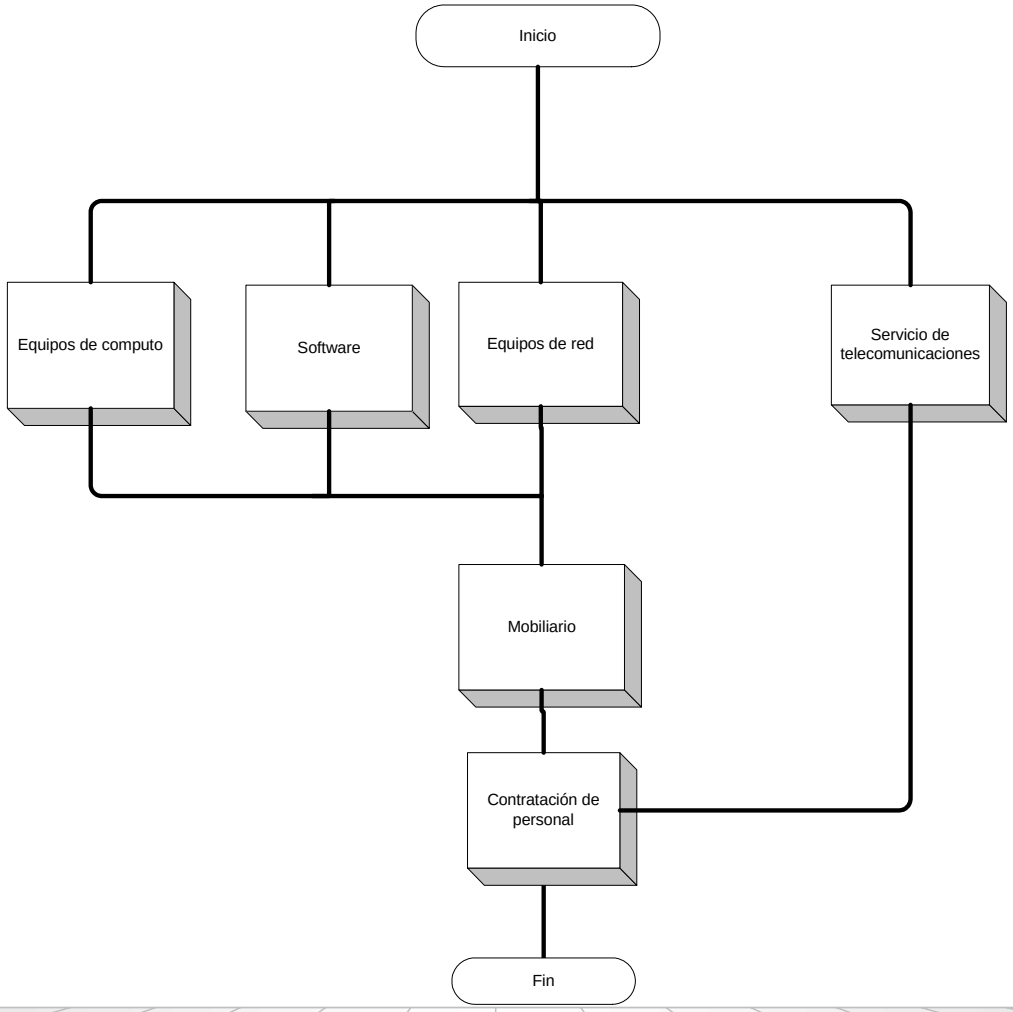
Referente a la contratación de personal

a) De acuerdo a la planeación estratégica de la empresa, se deberá hacer un análisis para la contratación de personal, en el que se deben seguir las siguientes recomendaciones:

a. El personal que realice los trabajos que afectan la instalación de la red, debe ser competente con base en la educación, formación, habilidades y experiencia apropiadas.
b. Se debe determinar la competencia necesaria para el personal que realiza trabajos en la instalación de la red, mediante la aplicación de exámenes evaluatorios.
c. La organización debe asegurarse que el personal es consciente de la pertinencia e importancia de sus actividades y de cómo contribuyen al logro de los objetivos de la empresa.
d. La organización debe proporcionar la formación o tomar otras acciones para satisfacer aquellas necesidades vitales para la instalación de la red.

b) Todo el personal debe estar comprometido con la "política de calidad" de la empresa, así como en la consecución de los objetivos de calidad.

Adquisición



4.2. Instalación

4.2.1. Política de Instalación

Reflejar el compromiso de mantener la eficacia, la eficiencia y la competitividad necesarias, para ofrecer a los clientes un excelente servicio, asegurando cumplir con los requisitos de control de calidad, costo y tiempo planeados, y buscando la mejora continua de los servicios brindados.

4.2.2. Norma de Instalación

La instalación de redes de computadoras debe asegurar un adecuado uso de los recursos humanos y los recursos económicos con los que se disponga. Siempre respetando los tiempos y los diseños hechos para su implantación, ambos aprobados por las partes interesadas.

4.2.3. Procedimiento para la instalación de redes de computadoras

Introducción

El siguiente procedimiento, tiene como fin dar una base adecuada para la instalación de redes de computadoras. Siempre considerando las necesidades del cliente y los requerimientos para la adecuada instalación de dichas redes.

Objetivos

- Establecer los lineamientos para controlar las actividades que se han de realizar durante la instalación de redes de computadoras.
- Asegurar que los análisis realizados para la instalación se lleven a buen término.

Alcance

Este procedimiento es aplicable para toda instalación de redes de computadoras, utilizando los mecanismos necesarios para la comunicación entre distintas redes.

Procedimiento

Referente a la planeación de tiempos

a) Primero se enlistan todas y cada una de las actividades a realizar durante la instalación de la red.
b) Estimar la duración de cada actividad en días, semanas o meses, considerando un tiempo determinado, que servirá de holgura para resolver cualquier imprevisto en la instalación de la red.
c) Realizar la descripción de cada actividad a realizar, dicha descripción debe ser corta pero específica.
d) Crear un diagrama de tiempos (diagrama de Gant) con los datos recabados.
e) Llevar el registro de las actividades realizadas, las actividades por concluir, las actividades por comenzar y las actividades faltantes.
f) Hacer una comparación de los tiempos reales de terminación de cada actividad, con los tiempos estimados para las mismas actividades y hacer los ajustes necesarios.

Referente al diseño de la red de computadoras

a) Se realiza un análisis para determinar la mejor opción en la elección de una topología. Considerando el equipo de computo y la tecnología de conectividad que se va a utilizar.
b) Se estila manejar por lo menos dos opciones para la topología. A partir de estas opciones, se analizan los beneficios y las desventajas de cada topología.
c) Analizar los costos y los beneficios que brinda cada opción.
d) Considerar siempre el factor económico y elegir la configuración que permita obtener el máximo desempeño de los recursos de la red y del sistema en general.
e) Debe considerarse el mantener las bases de datos actualizadas instantáneamente y de acceso desde distintos puntos.
f) Debe existir facilidad para la trasmisión de archivos entre miembros de un grupo de trabajo.
g) Considerar siempre el compartir periféricos caros (impresoras láser, plotters, por ejemplo).
h) Tener en cuenta que se necesita bajar el costo del software comprando licencias de uso múltiple en vez de muchas individuales, para cada equipo.
i) Mantener versiones actualizadas y coherentes del software.
j) Debe existir la facilidad para la comunicación con otras redes.
k) Mantener usuarios remotos.

Referente al local de instalación

a) Analizar la facilidad de acceso al local en cuestión, así como la comunicación con otros servicios o departamentos, como son: fotocopiadora, almacén, cuarto de telecomunicaciones y la gerencia.
b) Estimar la capacidad de carga de piso (loza o piso firme)
c) Verificar que cuente con el espacio suficiente para el mobiliario (mesas, sillas, racks, servidores).
d) Observar los requerimientos y la disponibilidad de la energía eléctrica necesaria para el equipo en general.
e) Debe de tomarse en cuenta el espacio para el equipo de aire acondicionado.
f) Considerar las normas de seguridad del edificio y de la institución en general.
g) Contemplar los peligros de incendio y de inundación en el edificio.
h) Prever futuras ampliaciones para el local, debido a la adquisición de nuevo equipo o bien al cambio de mobiliario.
i) Evitar la luz solar directa, para poder observar la consola y las señales.
j) Debe mantenerse un promedio de 450 luxes a 70cm del suelo para la iluminación del local.
k) Del 100% de iluminación, deberá distribuirse el 25% para iluminación de emergencia y se conectará a un sistema de fuerza ininterrumpible (no-brake).
l) Mantener un rango de temperatura de 18 a 22 grados centígrados y una humedad relativa (HR) de 50% $\pm$ 5%.
m) Es necesario contar con una salida de emergencia.
n) Si hay vibraciones superiores a las normales, es necesario estudiarlas antes de colocar cualquier equipo y se utilizarán los dispositivos antivibratorios necesarios (juntas de neopreno).
o) Los cubículos de computadoras, no deberán instalarse encima, debajo o adyacente a un área donde se almacenen, procesen o fabriquen materiales inflamables o explosivos.
p) Debe preverse un sistema de drenaje en el piso firme.
q) Habrá un sistema de detección de humo, para aviso anticipado, el cual deberá sonar una alarma e indicar la situación del detector activado.

Referente a la instalación eléctrica

a) Se comprobará, con el proveedor del equipo de cómputo, los voltajes de trabajo del equipo instalado.
b) La tolerancia en tensión no deberá ser mayor de 10% ni menor al 8% de la tensión nominal que especifique el fabricante del equipo de cómputo.
c) La tolerancia de frecuencia será de ½ Hz.
d) La acometida de energía eléctrica que alimente al equipo de cómputo deberá ser completamente independiente y a ella no se conectará ninguna otra carga, a fin de evitar interferencias.
e) La sección de los conductores eléctricos de la acometida deberá calcularse para la potencia consumida por el equipo de cómputo, señalada en las hojas de

especificaciones, y deberá considerarse un 75% adicional como margen de seguridad y de crecimiento a futuro. Esto tiene la finalidad de evitar caídas de tensión debido al crecimiento del equipo de cómputo.

f) La toma de tierra física, será independiente, con una resistencia total de 3 ohms.
g) La sección de conductor a tierra física será igual a una de las fases e irá aislado en todo su recorrido.
h) Las terminales (computadoras e impresoras remotas) que se localizarán dentro del edificio de la sala de cómputo, o fuera de él, estarán alimentadas por energía eléctrica regulada.
i) Se debe asegurar utilizar un sistema de energía ininterrumpible (equipos no-brake), respaldados por una planta de generación de energía eléctrica para emergencias (PGEEE), es de alto costo pero proporciona continuidad de servicio.
j) Se debe contar con un regulador de voltaje que elimine las armónicas perjudiciales al equipo de cómputo.

Referente a la instalación del software para red

a) Verificar que el hardware que se esta utilizando es apto para el software que se va a manejar.
b) Antes de comenzar la instalación es recomendable efectuar una copia de seguridad del software que se va a utilizar.
c) Realizar la partición necesaria (cuando aplique), para instalar el software en el disco duro, el proveedor del software deberá indicar cual es el tamaño recomendado para su software.
d) Iniciar la instalación siguiendo al pie de la letra las indicaciones de los ejecutables del software utilizado.
e) Se realiza la instalación del software en el servidor y cada una de las terminales de la red.
f) Finalizada la instalación, puede probarse la conexión al servidor desde alguna terminal para verificar que todo esté correcto.
g) Para finalizar, salir del programa de instalación. Desconectar el servidor y reiniciarlo.

Referente a la distribución del equipo de cómputo

a) Se deberá realizar un análisis del espacio con que cuenta el local de instalación, las dimensiones de los equipos de cómputo (considerando los muebles que utilizarán cada uno de los equipos de cómputo) y la cantidad de equipos que se instalarán, esto con el fin de determinar la cantidad de equipos que se podrán colocar o bien las dimensiones de los muebles que se deberán utilizar para el acomodo de los equipos de cómputo que se requieran.
b) Se recomienda tener una separación entre equipos de cómputo (considerando las dimensiones de los muebles donde se encuentran instalados)

de 75cm a 80cm. Para el espacio de pasillo se recomienda dejar un espacio de 1.5m para el libre transito del personal y el transporte de equipo y material.

c) Se tendrá en cuenta el espacio destinado para los equipos de impresión, estos pueden permanecer en las partes traseras o delanteras de la sala de cómputo, contando con un espacio similar al de cualquier equipo de cómputo. También se puede tener el equipo de impresión en cada modulo de trabajo, pero se recomienda que cuenten con su propio espacio de trabajo.
d) Se debe considerar tener un equipo de impresión por cada diez equipos de cómputo, para facilitar el tiempo de impresión.

Referente al equipo de interconexión de la red

a) Se deberá realizar un análisis previo para saber qué tan pesado será el tráfico de información del centro de cómputo.
b) De acuerdo a la envergadura de la red, se estimará cuál será la seguridad necesaria en dicha red.
c) Se deberán conocer las distancias que se recorrerán con el cableado, a través de los distintos cubículos de computadoras.
d) Se recomienda tener varias opciones de cableado a considerar.
e) Realizar el análisis correspondiente, para determinar el tipo de conectividad que se usará, considerando repetidores (hub's), switch's y puentes.
f) A nivel industria, no se recomienda el uso de hub's.
g) Se debe tener en cuenta que los dominios de colisión son independientes y corresponden a cada conexión del puerto de un switch.
h) Por cada switch o puente se pueden poner hasta 4 hub's.
i) El número máximo de switch's es de 7 por cada red.
j) La distancia máxima de un switch a un nodo será de 100m.
k) Para la comunicación de la red se utilizará el protocolo de acceso al medio CSMA/CD (Carrier Sense Multiple Access / Collition detection)
l) En la ruta de comunicación entre dos nodos no debe existir más de dos repetidores. Después de pasar un switch o un puente la cuenta vuelve a cero.
m) En la ruta de comunicación entre dos nodos no debe existir más de siete puentes, después de pasar por un ruteador la cuenta vuelve a cero.
n) Para la conexión a alta velocidad de redes LAN se deberá tomar en cuenta la siguiente tabla de conectividad:

Nombre	Medio	Distancia máxima
1000 Base Sx	Fibra óptica multimodo 62.5/125 micras	220 m
1000 Base Lx	Fibra óptica multimodo 62.5/125 micras	550 m
	Fibra óptica Monomodo	5 km
1000 Base Cx	Twinax o Quad (STP/ Coax)	25 m
1000 Base T	UTP Cat 5e o 6	100m

Tabla 4.1 Conectividad de redes LAN

o) Para la conexión Crossover con el estándar 1000 Base T debe considerarse la siguiente tabla:

Blanco-naranja	Blanco-verde
Naranja	Verde
Blanco-verde	Blanco-naranja
Verde	Naranja
Azul	Blanco-café
Blanco-azul	Café
Blanco-café	Azul
Café	Blanco-azul

Tabla 4.2 Conexión crossover para cable UTP

NOTA: Véase el apéndice A que contiene un diagrama del cable UTP utilizado y su fabricación.

p) El apilamiento de los dispositivos de interconexión (interconexión en forma de pila de hub's, puentes, switch's) será con la misma marca y mismas velocidades de transmisión.
q) Se recomienda utilizar apilamientos de dispositivos en vez de conexiones en cascada.

Referente al cableado estructurado

a) El cableado estructurado se debe realizar de acuerdo a los siguientes estándares:

    a. ANSI/TIA/EIA 568.- Estándar de cableado de telecomunicaciones en edificios comerciales.
    b. ANSI/TIA/EIA 569.- Estándar para ductos y espacios de telecomunicaciones en edificios comerciales.
    c. ANSI/TIA/EIA 570.- Estándar de alambrado de telecomunicaciones residencial y comercial pequeño.
    d. ANSI/TIA/EIA 606.- Estándar de Administración de Infraestructura.
    e. ANSI/TIA/EIA 607.- Requerimientos de puesta a tierra para telecomunicaciones.

b) Para el estándar 568 se requiere tener los siguientes subsistemas de cableado estructurado

    a. Subsistema de entrada al edificio
    b. Subsistema de cuarto de equipos
    c. Subsistema de cableado horizontal
    d. Subsistema de cuarto de telecomunicaciones
    e. Subsistema de cableado horizontal o BackBone
    f. Subsistema de área de trabajo

c) Para el subsistema de entrada al edificio, se deberá tener la ruta del BackBone que interconecte con otros edificios, o bien una antena para la comunicación.
d) Para el subsistema de cuarto de equipos se requiere un espacio centralizado para los equipos de telecomunicaciones (hub's, switch, equipo de cómputo). Este cuarto sólo debe contar con los equipos directamente relacionados con el sistema de telecomunicaciones y sus sistemas de soporte.
e) Para el subsistema del cuarto de telecomunicaciones, el espacio no debe ser compartido con instalaciones eléctricas a no ser que sean del mismo equipo. También debe ser capaz de albergar equipo de telecomunicaciones y terminaciones del cableado.
f) El cuarto de telecomunicaciones debe existir por cada sala o piso de equipo de cómputo. Y cada cuarto deberá atender los servicios de su sala o piso correspondiente.
g) Para el subsistema de cableado horizontal deberá salir de un closet de telecomunicaciones (Rack) hacia cada terminal (roseta). La distancia máxima deberá ser de 90 m para cableado con UTP.
h) Las distancias horizontales se deberán considerar de acuerdo a la siguiente tabla y la formula que se muestran a continuación:

Longitud de cable horizontal (H)	Longitud máxima para área de trabajo (W)	Longitud máxima del Patch Cord de los equipos (C)
90 m	3 m	10 m
85 m	7 m	14 m
80 m	11 m	18 m
75 m	15 m	22 m
70 m	20 m	27 m

Tabla 4.3 Distancias máximas horizontales

La longitud se determina por la siguiente fórmula:

$$C = \frac{(102 - H)}{1.2}$$
$$W = (C - 7) < 20m$$

i) Si la distancia es menor a 70m en el cableado horizontal, la distancia de la roseta al nodo nunca deberá ser mayor de 20m. Y la distancia máxima total no será mayor a 100m.
j) Para las distancias recorridas con fibra óptica, todas las combinaciones de distancias con cables horizontales son permitidas, siempre considerando que la distancia máxima no será mayor a 100 m.
k) El subsistema de cableado vertical o de BackBone, deberá proveer la interconexión entre el cuarto de telecomunicaciones, el cuarto de equipos y la entrada al edificio.
l) Para el subsistema del área de trabajo se deberá contar con todos los diversos equipos activos del usuario final, como son: teléfonos, computadoras, impresora y terminales.
m) Los ductos o canaletas (conduit) dentro de la pared deberán cumplir con los requerimientos de estándar eléctrico.
n) En estos ductos ninguna sección deberá contener más de dos dobleces a 90º.
o) Para la instalación dentro de las paredes el radio de giro interior deberá ser mínimo 6 veces el diámetro exterior.
p) En ductos perimetrales la capacidad de llenado práctica será del 30% al 60% del tamaño del ducto o canaleta.
q) En los ductos perimetrales no se debe tener un radio de doblaje interior menor a 6 veces el diámetro exterior.
r) La capacidad de llenado para canaletas rectangulares se determina con ayuda de la siguiente fórmula:

$$\#\,dealambres = \frac{(Anchodelducto \times Altodelducto)}{[1.75(diámetrodelalambre)^2]}$$

Nota: Si la instalación es eléctrica el factor de 1.75 cambia a 2

s) Los cables deberán estar cubiertos, en absolutamente todos sus recorridos, por cablecanal. No debe quedar ni siquiera un centímetro de cable descubierto.
t) Los cables de red no podrán estar en contacto con cables de electricidad. Para prevenir que esto ocurra en el futuro, cada cablecanal deberá incluir una leyenda que diga: “Solo para cables de red de computación. Prohibido introducir cables de electricidad”. Estas leyendas deberán estar adheridas cada 2 metros en todos los cablecanales y cubiertas por cinta adhesiva "ancha"

Referente a la instalación de WIRELES (redes inalámbricas)

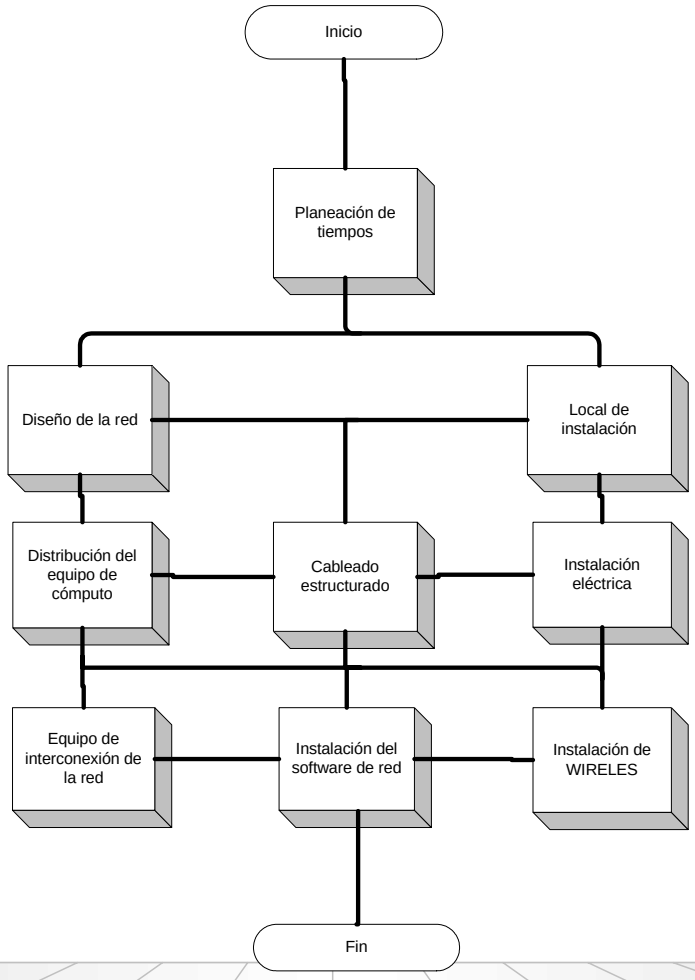
a) Se analizará la adquisición del access point de acuerdo a las necesidades del área donde se colocará la sala de cómputo. Es decir, se tomará en cuenta la distancia que habrá entre el access point y cada Terminal de acuerdo a la siguiente tabla:

Estándar	802.11a	802.11b	802.11g
Ratificación	2002	1999	2003
Frecuencia	5.8 GHz	2.4 GHz	2.4 GHz
Velocidad de transmisión	54 Mbps	11 Mbps	54 Mbps
Precio	Alto	Económico	Accesible
Cobertura	50 – 80 m	50 – 100 m	50 – 125 m

Tabla 4.4 Redes inalámbricas

b) La velocidad de trasmisión del access point deberá ser igual o mayor a las tarjetas de red inalámbricas instaladas en cada equipo de cómputo.
c) Todos los equipos de cómputo que necesiten del uso de red, deberán contar con una tarjeta de red inalámbrica, se recomienda utilizar tarjetas con velocidades iguales a la del access point utilizado.
d) La colocación del access point deberá ser estratégica, para cubrir un radio de alcance suficiente para todos los equipos de cómputo que necesiten del uso de red.
e) El access point deberá estar conectado al backbone.
f) Se deberá realizar la configuración de las IP’s para la asignación de cada equipo utilizado, considerando el uso de IP’s públicas y de IP’s privadas. Se recomienda realizar un análisis de ventajas y desventajas de cada asignación.

Instalación



4.3. Seguridad

4.3.1 Política de seguridad

Garantizar la integridad de los activos de información y los equipos informáticos de la compañía, a través de la vigilancia continua de los datos que se encuentren transitando por la red. La seguridad de la red es punto primordial para el desarrollo de la compañía, comprometiéndonos a mantener un programa actualizado de seguridad informática, basado en los objetivos estratégicos de la compañía.

4.3.2. Norma de seguridad de la red

La compañía debe cuidar la integridad de la información de los usuarios mientras estos se encuentren usando la red local. La compañía debe poder identificar, verificar, proteger y salvaguardar en lo posible la información de los usuarios. Cualquier pérdida o alteración de la información, debe ser registrada y notificada de forma inmediata al usuario afectado.

4.3.3 Procedimiento para la seguridad de la información y el equipo de cómputo

Introducción

La información y los equipos de cómputo son activos importantes y vitales de cualquier empresa moderna. Sin ellos, quedaríamos rápidamente fuera del negocio, es por eso que todas las empresas tienen el deber de preservarlos, utilizarlos y repararlos. Lo anterior significa que se debe contar con un plan estratégico, en dónde se definan las acciones apropiadas para asegurar que la información y los sistemas de cómputo están protegidos apropiadamente de amenazas y riesgos tales como: fraude, espionaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción del servicio, accidentes e incluso desastres naturales.

Objetivos

- Salvaguardar la información de los usuarios dentro de la red local de la compañía.
- Proteger la información usada dentro de la compañía de acuerdo a su valor e importancia.
- Establecer las directrices para asegurar la protección apropiada de la compañía dentro de un ambiente de red.

Alcance

Este procedimiento aplicará a todos los usuarios de la red de datos, empleados, contratistas, consultores y personal temporal de la compañía.

Es política de la compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de cualquier tipo de información propiedad de la compañía. Así como salvaguardar bajo los lineamientos del presente procedimiento, la información perteneciente a empresas o personas que requieran los servicios del centro de cómputo.

Procedimiento

Concerniente al manejo de los equipos de cómputo

a) Todo el equipo de cómputo de la organización sólo puede ser usado en un ambiente seguro. Un ambiente seguro será aquel en el que se han implantado acciones adecuadas para salvaguardar el software, el hardware y los datos (la organización debe establecer un procedimiento por escrito en el que se describan dichas actividades).
b) El equipo de cómputo solamente puede ser usado para actividades de trabajo, y no para fines de esparcimiento tales como juegos, Chat, intercambio de archivos o mensajeros. Periódicamente se llevarán a cabo auditorias al equipo de cómputo para conocer su estado actual.
c) Cada jefatura es la responsable de hacer respetar la configuración designada por el departamento encargado de los sistemas de cómputo.
d) Cada servidor deberá contar con una fuente de poder ininterrumpible o no-break.
e) No se permite la reubicación de los equipos si no se cuenta con un permiso por escrito del área de sistemas.
f) Cuando se detecte la falla de algún equipo o software, deberá ser notificado al jefe inmediato, el cual avisará al área de sistemas de los equipos y/o partes faltantes.
g) Si alguna de las computadoras tiene acceso a datos confidenciales, deberá contar con un cubículo apropiado en el que se garantice solamente el acceso del personal autorizado. Asimismo, la computadora deberá contar con dispositivos de seguridad por hardware para su acceso.
h) Se debe establecer un procedimiento para el control del acceso, esto con el fin de restringir los privilegios de los usuarios en el manejo del equipo de cómputo.
i) Se prohíbe la introducción de computadoras portátiles al área de trabajo, solamente se permitirá la entrada de éstas con el permiso del jefe de la sala de cómputo.
j) Cada departamento deberá hacer especial énfasis a todos sus empleados, de que la copia a un medio removible de almacenamiento, de la información concerniente a la organización, está tajantemente prohibido.

k) Todas las computadoras deberán contar con programas antivirus instalados, y deberán mantenerse actualizados en todo el equipo de cómputo. Se registrarán las fechas de descargas de las actualizaciones, así como la información concerniente al estado que guarda el equipo en ese momento.
l) La instalación de software solamente se realizará de común acuerdo con el área de sistemas y bajo su aprobación explícita.
m) Periódicamente se harán respaldos de la información de los usuarios y de los servidores, salvo en el caso de información importante, la cual será respaldada en un lapso de tiempo determinado por el jefe de cada área y de común acuerdo con el área de sistemas.
n) Toda la información confidencial o de mayor importancia, solamente podrá ser enviada por la red si ésta es cifrada antes de su envío.
o) El acceso a dicha información solamente será otorgado al personal autorizado.

Concerniente a la seguridad en las telecomunicaciones

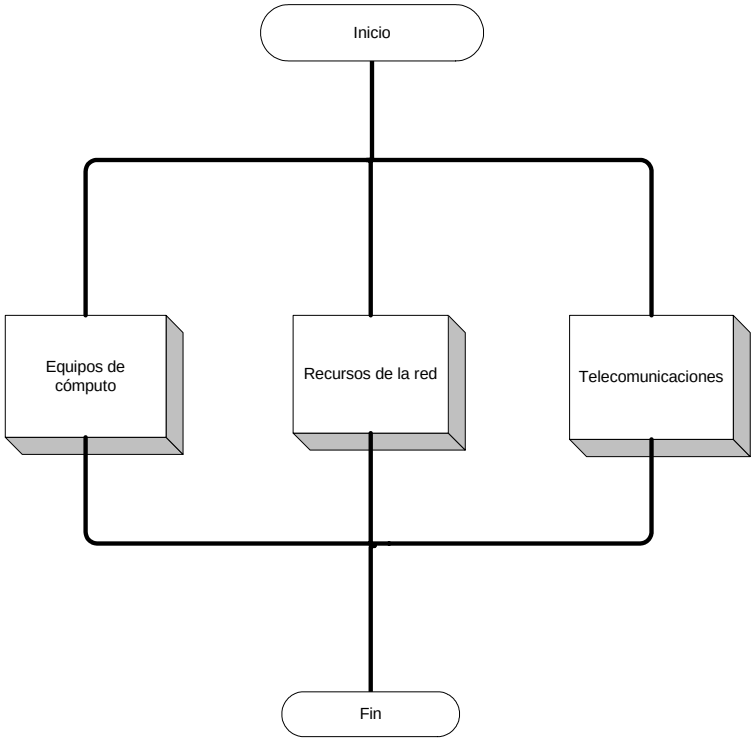
a) Se debe llevar a cabo un monitoreo semanal para verificar el uso que se le ha dado al equipo de telecomunicaciones, con el fin de asegurar que se está usando para actividades de trabajo y no para esparcimiento personal. Dicho monitoreo tomará como punto de partida el hecho de que, los recursos, servicios y conectividad disponibles vía red abren nuevas oportunidades, aunque también le abren la puerta a nuevos riesgos de seguridad.
b) Se verificará periódicamente la instalación física de la red, de tal manera que se pueda comprobar el estado que guarda, así como el detectar posibles intercepciones de información en la comunicación entre computadoras.
c) Se mantendrá un monitoreo aleatorio diario de las operaciones de la red, con el fin de detectar posibles fallas en la seguridad de la misma.
d) Se mantendrán registros de los acontecimientos importantes que sucedan en la red, tales como una carga excesiva en el uso de la misma, así como los errores que se puedan registrar.
e) Todos los puntos anteriores conformarán un plan de auditoria, el cual deberá ser revisado y aprobado por la alta dirección, para su implantación y mantenimiento.

Concerniente al uso de los recursos de red

a) Todos los usuarios serán divididos en grupos o áreas de trabajo. Además existirá un apartado especial para usuarios conocidos como “externos”. Los cuales contarán con un nivel de jerarquía en el uso de la red, en el cual estarán definidos aspectos tales como privilegios, y uso de recursos.
b) Se entregarán cuentas de usuario mediante el procedimiento de asignación de cuentas de usuario. Toda cuenta de usuario, es personal e intransferible y no deberá haber duplicidad de sesiones.
c) Todos los usuarios podrán acceder a la red corporativa de la empresa, usando el programa definido por el área de sistemas.

d) Ningún usuario podrá acceder al sistema con la cuenta de otro.
e) En caso de que algún usuario deseé conectarse a la red de la compañía, y se encuentre fuera de su área de trabajo, lo podrá hacer solamente en las computadoras de acceso público instaladas en cada departamento.
f) Al momento de acceder a la red corporativa, recibirá un mensaje donde se le informará la fecha, hora y dirección desde que se conectó la última vez, esto permitirá al usuario conocer el estado de su cuenta, así como el uso que se le ha dado a ésta. En caso de cualquier irregularidad, deberá notificarla inmediatamente al departamento de sistemas.
g) Como parte del programa de auditorias informática, se llevarán a cabo revisiones periódicas a los sistemas de cómputo, para verificar que no tengan instalado software que pueda vulnerar la seguridad de la red corporativa (spyware).

Seguridad


Inicio
Equipos de cómputo
Recursos de la red
Telecomunicaciones
Fin

4.4. Mantenimiento

4.4.1. Política de mantenimiento

Mantener el compromiso de contar con redes que sean de completa funcionalidad a pesar del paso del tiempo, siempre cumpliendo con los requisitos del cliente y mejorando continuamente los recursos con que se cuenta, para obtener el mayor rendimiento de la red.

4.4.2. Norma de mantenimiento

El mantenimiento de la red de computadoras, ha de contemplar los tiempos de mantenimiento físico y del sistema, la planificación de estos mantenimientos y de ser el caso, la contratación a terceras personas para realizar dicha tarea.

Los mantenimientos pueden ser preventivos o correctivos, a efecto de conservar el equipo en óptimas condiciones de funcionamiento y de conformidad con los requerimientos establecidos por las partes involucradas.

4.4.3. Procedimiento para el mantenimiento de redes de computadoras

Introducción

El siguiente procedimiento, busca inducir una cultura de aprovechamiento máximo en los recursos que nos brinda una red de computadoras.

La eficiencia de los recursos humanos y económicos de una empresa que utiliza redes de computadoras, se ven afectados seriamente por equipos dañados o bien por la mala planificación del mantenimiento de los equipos.

Por tal motivo, es clara la necesidad de contar con un documento que permita ser la base para realizar las distintas actividades que requiere el mantenimiento. A continuación se describe el procedimiento sugerido para llevar el mantenimiento de la red de computadoras.

Objetivos

- Designar las actividades necesarias para realizar el mantenimiento de la red.
- Planificar y determinar los tiempos sugeridos para el mantenimiento de la red de computadoras.

- Establecer algunos términos y condiciones necesarios para la realización de un contrato de mantenimiento.

Alcance

Este procedimiento sirve para realizar la planificación y la resolución de las actividades que requiera el mantenimiento de las redes de computadoras, de igual forma, abarca puntos clave que se deben tomar en cuenta para la contratación de los servicios a terceros de mantenimiento.

Procedimiento

Referente a la planeación del mantenimiento

a) En primer lugar, se debe establecer el periodo de garantía que ofrece el equipo adquirido, con el conocimiento que durante este periodo toda reparación o mantenimiento del equipo corre por cuenta del distribuidor.
b) Una vez terminado el periodo de garantía del equipo de cómputo o de red, se debe establecer el tiempo en que se realizará el mantenimiento; debe tomarse en cuenta el uso del equipo, su desgaste y la antigüedad del mismo.
c) Se debe realizar un inventario de todo el equipo utilizado, y ponderar cual tiene mayor desgaste debido al uso diario.
d) Los factores climáticos y las condiciones del lugar donde se encuentra situada la red, son agentes importantes para la periodicidad del mantenimiento del equipo. Las temperaturas altas y el exceso de polvo implican un monitoreo continuo de la red y sus componentes. Así pues, reducen el tiempo entre revisiones y mantenimiento.
e) El mantenimiento no debe afectar el desempeño las actividades propias de la empresa, por lo cual se recomienda tener los equipos suficientes para cubrir las necesidades de trabajo, y se deberá hacer con la mayor brevedad posible. En el caso de mantenimiento de la información, las actividades relacionadas con este ramo deberán realizarse en horas no pico para la empresa.
f) Se hará constar que los servicios que se han de recibir incluirán los siguientes aspectos: actualización de ingeniería, mano de obra, así como también todos los ajustes, reemplazos de partes y refacciones que sean necesarias, y finalmente la instalación de todo lo anterior en el equipo que recibirá el mantenimiento.

Referente al mantenimiento de los componentes físicos de la red

a) Se verifica el estado del servidor, se realiza la limpieza de las partes físicas y se comprueba el correcto funcionamiento del sistema operativo de red que se esté utilizando.

b) De ser el caso se realiza la misma operación con los diferentes servidores que compongan la red de computadoras (servidor de copias de seguridad, servidor de impresoras, servidor de base de datos, servidor de dominio, por ejemplo).
c) Se procede al mantenimiento de las estaciones de trabajo, que implica la limpieza de los dispositivos y del software necesario para la comunicación con el servidor.
d) Se efectúa la limpieza de la parte física del componente, se recomienda el uso de espumas limpiadoras para las partes externas de los componentes y de aire comprimido o liquido a prueba de cortos eléctricos para la limpieza de los circuitos que componen dichos equipos.
e) Se realiza al mantenimiento de los dispositivos de conexión de red.
f) Se verifica que los transceivers, salidas a Ethernet y cable telefónico se encuentren en buen estado.

Referente a la información y documentación

a) Se explorarán los discos duros para descartar errores y en caso de existir alguno, reparar los sectores alterados.
b) Eliminar los archivos temporales y la información obsoleta.
c) Realizar un respaldo de la información privada y financiera.
d) Hacer copias de los respaldos periódicamente, y guardarlos debidamente.
e) Actualizar las versiones de software que se están utilizando.
f) Explorar en busca de virus, actualizar firewall's y ejecutar herramientas de diagnostico para la seguridad de los equipos de red.

Referente a las cláusulas para contratos de mantenimiento

a) El objeto del contrato es que el proveedor proporcionará en beneficio del cliente los servicios de mantenimiento preventivo y correctivo al equipo que así lo requiera, y asegurando que el equipo se conservará en óptimas condiciones de funcionamiento. El proveedor deberá trabajar de acuerdo a las especificaciones técnicas del fabricante, para lo cual realizará los ajustes y reemplazos necesarios para este fin.
b) Se especificará el importe de los servicios de mantenimiento ofrecidos, podría ser de la siguiente manera:

   El precio convenido para el pago de los servicios de mantenimiento para el equipo objeto de este contrato, en moneda nacional, incluyendo descuentos, importa la cantidad de $_____ (cantidad con letra) y la cantidad adicional $_____ (cantidad con letra) correspondiente al impuesto al valor agregado, lo que importa un costo total por los servicios de mantenimiento de $_____ (cantidad con letra).

c) La forma de pago se hará de manera que el cliente se encuentre amparado por los servicios de mantenimiento que contrata, los cargos por mantenimiento emergente y extraordinarios, se cuantificarán por lapsos previamente definidos, desglosando los importes correspondientes.
d) Las contribuciones fiscales serán cubiertas por ambas partes según corresponda.
e) El contrato deberá ser por lo menos de 12 meses, con el beneficio para el cliente de poder rescindirlo en cualquier momento notificando por escrito a su proveedor con 30 días de anticipación.
f) El cliente tendrá la facultad de ceder los derechos y obligaciones derivados del contrato, siempre y cuando notifique de tal suceso a su proveedor con un mínimo de 30 días de anticipación.
g) El proveedor cubrirá al cliente de cualquier demanda en la que se encuentre inmerso, debido al uso de bienes o cualesquiera de las partes que tengan sus equipos que violen cualquier patente, marca, derecho de autor, secreto industrial o propiedad intelectual registrada. En tales casos el proveedor deberá optar por las siguientes soluciones:

    - Procurar para el cliente el derecho de continuar usando los bienes o las partes que se encuentren en disputa y sean causa de infracción.
    - Reemplazar las partes o bienes en conflicto por unidades que no tengan problemas de esta índole.
    - Modificar los bienes o partes con problemas, de manera que no causen infracción.

h) El cliente tendrá absoluta propiedad de las patentes o derechos de autor sobre procedimientos o programas inventados o desarrollados por cuenta propia o como resultado de la utilización de los bienes comprados al proveedor. Así pues, el proveedor no podrá utilizar programas de mantenimiento desarrollados por el cliente o a costa de este, sin su consentimiento por escrito.
i) Ninguna de las partes será responsable de cualquier atraso o incumplimiento de contrato que resulte directamente o indirectamente del caso fortuito o de fuerza mayor.
j) Al finalizar el servicio de mantenimiento por parte del proveedor, se expedirá un certificado escrito que garantice que los bienes objeto del mantenimiento califican para los servicios futuros que puedan ser proporcionados por el proveedor mismo u otro proveedor, anexando una bitácora de los equipos, donde se indique los servicios y refacciones que fueron sustituidas durante el último mantenimiento realizado.
k) El cliente tendrá las siguientes obligaciones hacia el proveedor de servicios de mantenimiento.

    - Notificar de inmediato al proveedor de cualquier falla de los bienes objetos del contrato.

- Operar los equipos conforme a las especificaciones y manuales del proveedor.
- Mantener las condiciones ambientales y eléctricas conforme lo indique el proveedor.
- No dar mantenimiento a los bienes amparados durante la vigencia del contrato con su proveedor de servicio de mantenimiento.
- Proporcionar el acceso necesario al proveedor para realizar sus tareas de mantenimiento, sin llegar a afectar las funciones de operación normal del mismo cliente.

l) El proveedor deberá comprometerse a que durante 5 años como mínimo a partir de la fecha del contrato, contará con las partes y refacciones necesarias para el mantenimiento del equipo del cliente.

m) El proveedor proporcionará oportunamente un instructivo que establezca la manera en que deberán ser reportados los fallos de los equipos objetos del contrato.

n) Cuando una falla afecte notablemente el desempeño de trabajo del cliente se deberá hacer lo siguiente:

- Si después de dos horas de haber iniciado el mantenimiento y los problemas aún existen, se avisará al gerente de la sucursal correspondiente para que se tomen las medidas necesarias.
- Si después de cuatro horas continúan los fallos y no se ha podido reparar la falla, el proveedor deberá proporcionar al cliente un equipo de soporte sin cargo para el cliente, hasta que se haya reparado la falla.

o) Para el mantenimiento correctivo, el proveedor entregará un reporte escrito al completar cada servicio, y que deberá contener lo siguiente:

- Fecha y hora en que se notifico la falla.
- Fecha y hora en que llegó el personal de mantenimiento.
- Fecha y hora de inicio de corrección de la falla.
- Tipo y modelo del equipo reparado.
- Tiempo invertido en la reparación.
- Descripción de la falla.
- Partes y refacciones utilizadas en el equipo reparado.

p) El proveedor se compromete a proporcionar las partes, refacciones y documentación necesarias para instalar los cambios de ingeniería producidos por el fabricante, con la premisa de mejorar el funcionamiento de los equipos objeto del contrato. Sin embargo, el cliente no deberá aceptar ningún cambio de ingeniería que implique modificaciones sustanciales en sus sistemas o programas.

q) El proveedor debe garantizar que contará con partes, refacciones, componentes y equipos de prueba durante un mínimo de 5 años, para mantener en óptimas condiciones a los equipos objeto del contrato.

r) El proveedor será responsable de los daños y perjuicios que cause al cliente, en sus personas, bienes o a terceros con motivo de la ejecución de los trabajos.

s) En caso de incumplimiento, la parte afectada podrá rescindir administrativamente el contrato, o bien su cumplimiento forzoso, y en cualquier caso puede reclamar el pago de los daños y perjuicios correspondientes, considerando los siguientes pasos:

   1. Las partes convienen que el cliente podrá ejercitar los derechos otorgados en el párrafo anterior por los siguientes motivos.

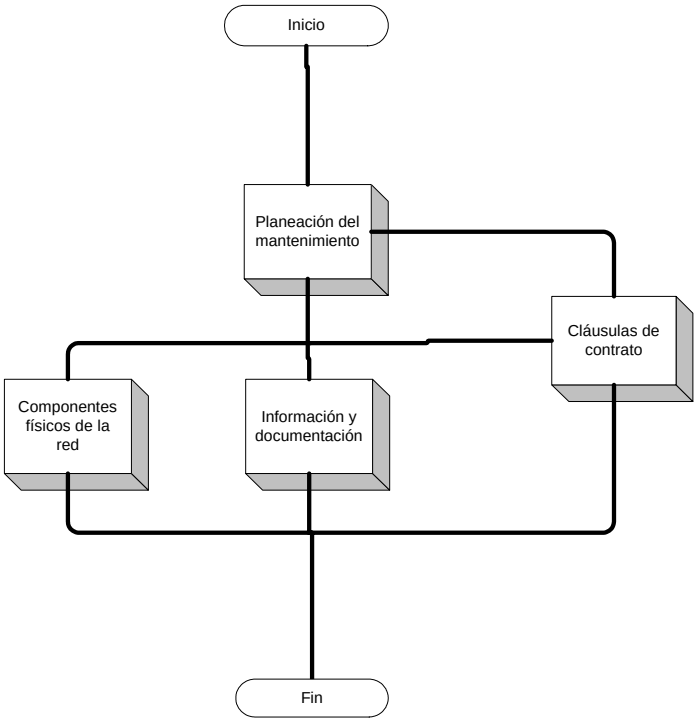
      - Por incumplimiento del proveedor en los servicios de mantenimiento en las condiciones y los términos pactados en el contrato.
      - Si el proveedor suspende injustificadamente los servicios de mantenimiento, o si no los realizase por medio del personal competente.
      - Si la calidad de los servicios de mantenimiento y de las partes y refacciones no corresponden a lo especificado por el fabricante.
      - Si el proveedor no otorgare las facilidades o datos necesarios para la inspección, vigilancia o supervisión de los servicios de mantenimiento.
      - Si el proveedor no atendiere a las recomendaciones que le sean formuladas por el cliente de manera escrita.
      - Si el proveedor cediese, traspase o en cualquier forma enajene, total o parcialmente los derechos y obligaciones que estipulen el contrato. Sin previo consentimiento por escrito del cliente.
      - Si el proveedor fuese declarado en estado de quiebra o suspensión de pagos por autoridad competente.

   2. Las partes convienen en que el proveedor podrá ejercer los derechos otorgados en el primer párrafo en los siguientes casos:

      - Si el cliente no cubre sus obligaciones económicas conforme lo pactado.
      - Si el cliente no da las facilidades para que el proveedor pueda cumplir con el mantenimiento del equipo objeto del contrato.

t) El proveedor deberá indicar los centros de servicio donde puede ofrecer el mantenimiento al cliente, en caso de ser requeridos los servicios fuera del centro de trabajo del cliente o bien para resolver cualquier eventualidad.

Mantenimiento



4.5. La observancia por los usuarios

Sin duda alguna, los principales actores de la red de datos son los usuarios, las personas que van a ser uso de ella y de sus recursos, por ello, es de especial importancia el establecer lineamientos generales que nos servirán para la definición de una política adecuada para todos los usuarios.

Algunos lineamientos que se deben tomar en cuenta para la declaración de una política adecuada pueden incluir aspectos tales como:

- El establecimiento de lo que constituye un abuso en los términos de uso de la red, que puedan afectar el desempeño de todo el sistema de datos.
- La responsabilidad de las cuentas de usuarios, rubro en el que se pueden responder a las preguntas: ¿podrán los usuarios compartir sus cuentas o permitir a otros utilizarlas?, ¿podrán revelarse las contraseñas de usuarios y en qué casos?
- Estableciendo parámetros que nos permitan definir el tiempo de expiración de contraseñas y/o de cambio de éstas por parte de los usuarios.
- Deslindando las responsabilidades de respaldo de la información de los datos, es decir, respondiendo a la pregunta: ¿son responsables los usuarios de brindar respaldo de sus datos o es responsabilidad del sistema?
- Las sanciones meritorias a los usuarios que revelen información concerniente a la empresa o a sus proyectos.
- Una declaración por escrito de una política de privacidad del correo electrónico de los usuarios.

A grandes rasgos podemos decir que lo mencionado anteriormente son sólo lineamientos generales, y que por lo tanto, cada organización deberá contar con adecuaciones particulares de acuerdo a la actividad que realiza. Debido a que no es objetivo del presente trabajo abordar casos particulares, nos enfocaremos a establecer una política y procedimientos generales que deberán observar todos los usuarios de la red de datos.

4.5.1. Política de observancia por los usuarios

Todos los usuarios de la red corporativa de la empresa, se comprometen a acatar la política de seguridad y acceso a la información de la red corporativa, basándonos en los principios éticos y morales que rigen la empresa. Todas las acciones concernientes al uso de la red corporativa y del equipo de cómputo, se reconocen como expresiones de seguridad que nos comprometen con nuestro trabajo.

4.5.2. Norma de observancia por los usuarios

Todos los usuarios deben estar regidos por la política y reglamentos de seguridad de la información. La organización debe determinar y proporcionar la información concerniente a:

- Los derechos y responsabilidades de los usuarios.
- Las sanciones correspondientes a alguna falta que vulnere la seguridad del sistema de red.

La organización debe planificar y gestionar el ambiente de trabajo adecuado para el acatamiento de las medidas de seguridad necesarias para lograr los objetivos de seguridad planteados.

4.5.3. Procedimiento concerniente a la observancia por los usuarios

Introducción

Cuanto más grande y compleja es una organización, las necesidades de comunicación aumentan, así como el intercambio de información de una sucursal a otra. De la misma manera, la cantidad de personas que tienen acceso a la red corporativa crece, volviendo más factible el hurto o robo de información clasificada de la empresa. Por ello, es de vital importancia el contar con un procedimiento encargado de delimitar las responsabilidades de todos los usuarios de la red, su acceso a ella y su uso responsable.

Hoy en día sería inimaginable el que una empresa no contara con oficinas en diferentes partes de un país o incluso en otros países, por ello, la comunicación se vuelve un aspecto primordial y de suma importancia, en el desarrollo de sus actividades, y para muestra basta un botón: las grandes empresas multinacionales, generalmente concentran los datos de sus ventas en una sola oficina central localizada muchas veces en el lugar de origen de la empresa, o en lugares llamados “bunkers”, los cuales cuentan con medidas sumamente rigoristas de seguridad, y vaya no es para menos si estamos hablando de que la información ahí almacenada vale miles de millones de dólares a las empresas.

Objetivos

- Establecer las actividades de los usuarios de la red de computadoras para el adecuado funcionamiento de la misma.
- Brindar el apoyo necesario para satisfacer las necesidades de procesamiento informático de los usuarios.
- Hacer la red más segura a través del establecimiento de mecanismos de control de acceso a la misma.

Alcance

El siguiente procedimiento será aplicable para todos los usuarios de la red corporativa.

Procedimiento

Referente a la autorización del uso de la red

a) Todo usuario que desee acceder a la red corporativa, deberá completar la hoja de alta de usuario y entregarla al jefe del departamento o a la persona que reporta directamente, para la asignación de nivel de acceso y la autorización correspondiente, **véase apéndice B**.
b) Todas las solicitudes correctamente requisitadas y firmadas de alta de usuario, deberán ser turnadas al departamento de sistemas informáticos.
c) Una vez recibidas las solicitudes en el departamento de sistemas, se realizará el alta correspondiente del servicio y se notificará al usuario que se halla en condiciones de utilizar el servicio.

Referente al acceso de los usuarios a la red

a) El ingreso al sistema debe ser mediante la clave proporcionada por el departamento de sistemas, la cual consta de dos partes: una de conocimiento general (el login o nombre de usuario) y la otra de conocimiento exclusivo (password). La cuenta de usuario es personal e intransferible, por lo que no se permite que se comparta con personal alguna, aún si ambas partes están de acuerdo.
b) El usuario está comprometido a respetar las políticas y normatividad de seguridad de la red de computadoras.
c) Así como a respetar la privacidad de toda la información contenida en la red y en las computadoras que la componen.
d) Debe mantener un lenguaje apropiado y respetuoso en todas las comunicaciones. El usuario no puede usar el sistema para insultar o molestar a otro usuario.
e) El usuario queda comprometido a no usar el sistema para fines comerciales u otros fines que no tengan que ver con las actividades laborales.

Referente al uso de la red

a) La infraestructura de la red se utilizará únicamente para desarrollos de trabajo, de investigación, técnicos y administrativos de la empresa.
b) Ningún recurso de la red será utilizado para transmitir información de la empresa a terceros sin previa autorización de la dirección.

c) No está permitido el uso de la red para fines de transmisión de información de carácter comercial, o cualquier otra forma que represente un beneficio personal ajeno a la empresa.
d) Está estrictamente prohibido ejecutar programas que exploten alguna vulnerabilidad para proporcionar privilegios no otorgados explícitamente por el administrador de la red.
e) Así como programas que intenten adivinar las contraseñas de otros usuarios.
f) El usuario debe abandonar su sesión de trabajo, si ésta no es utilizada por un tiempo considerado.

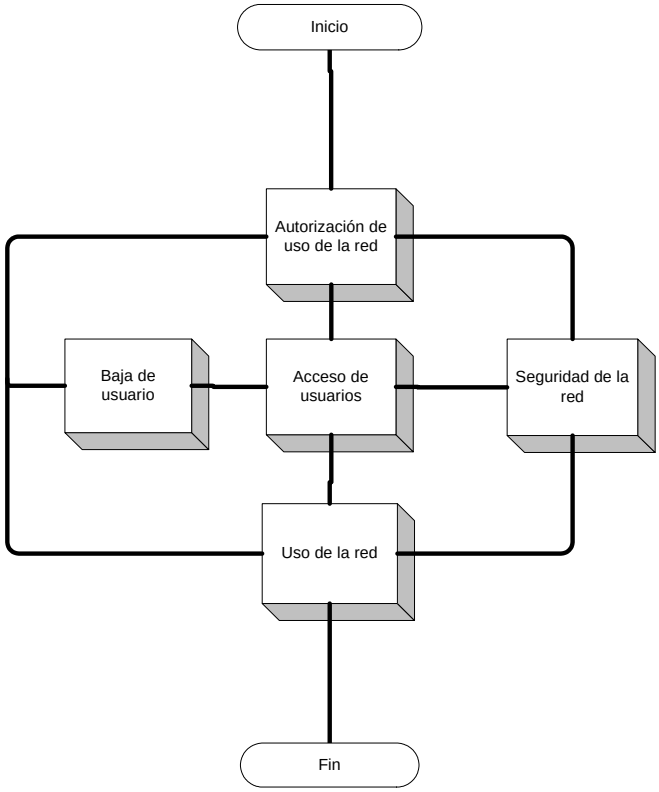
Referente a la seguridad

a) Para reforzar la seguridad de la información de la cuenta, el usuario bajo su criterio deberá hacer respaldos de su información dependiendo de la importancia y frecuencia de cambio de la misma.
b) La contraseña de usuario debe ser cambiada de inmediato si éste detecta o asume que ha sido identificada por descuido o por otro medio.
c) Está estrictamente prohibido crear nombres de archivos que hagan referencia a comandos propios del sistema.
d) Está estrictamente prohibido el otorgamiento de cuentas (si se cuenta con privilegios para hacerlo) sin la autorización por escrito del administrador.
e) El usuario no está autorizado a introducir dispositivos de almacenamiento tales como discos ópticos, memorias USB o agendas electrónicas sin previa autorización del administrador.
f) Queda prohibido el uso de programas de transferencia de datos o archivos, además del uso de mensajeros que puedan vulnerar la seguridad de la red.

Referente a la baja de un usuario

a) El usuario puede perder su condición de tal, si pasado un periodo de tiempo establecido por el administrador, no registra actividad en su cuenta sin justificar debidamente esta situación.
b) Por mantenimiento a los sistemas informáticos, restituyéndole más adelante una nueva cuenta de usuario.
c) El usuario pierde su condición como tal, cuando deje de tener alguna relación oficial con la empresa. Es decir, cuando deje de laborar o formar parte de la empresa por causas ajenas a ésta. Cuando esto suceda es responsabilidad notificar su baja de la institución para evitar el mal uso de su cuenta.
d) Es motivo de baja de un usuario la violación a las normas y políticas de uso de la red de la empresa.
e) Cualquier asunto no considerado en estos puntos quedará a consideración del departamento de sistemas y del jefe del usuario.

Observancia por los usuarios



4.6. La observancia por el administrador

4.6.1. Política para la observancia por el administrador

Asegurar que las actividades realizadas por el administrador de la red, se enfoquen a la obtención del mayor beneficio y aprovechamiento máximo de los recursos del sistema. Buscando siempre la mejora continua de las acciones establecidas a través de la actualización constante en la rama de administración de redes.

4.6.2. Norma para la observancia por el administrador

La observancia por el administrador deberá contemplar la configuración de una red de computadoras, el acceso a dicha red por parte de los usuarios y administradores; así como la seguridad que debe existir en la red y que es menester de los usuarios y administradores respetar.

4.6.3. Procedimiento para la observancia por el administrador

Introducción

Hoy en día es inimaginable contar con una red de computadoras sin una infraestructura informática sólida, de la cual solemos hacer uso de manera tan natural que pocas veces nos detenemos a meditar lo que implica el contar con tal servicio, y lo que sucedería si de repente nos viéramos privados de él.

Bajo esta línea de pensamiento puede suceder (sucede en la vida real) que no sea sino hasta el momento en que algo falla, dentro de toda esa intrincada madeja computacional, que nos detengamos, en el mejor de los casos, a analizar los riesgos y costos involucrados en mantener funcionando una red de servicios de cómputo, aunque es más común que simplemente nos quejemos por la falla o levantemos el teléfono para pedir una explicación y solicitar la pronta reanudación del servicio.

Pueden contraerse problemas tales como: encontrarse que los nodos de uso común se saturen al ser utilizados por personas ajenas a la institución, quienes comparten una misma cuenta de usuario y cuyo uso es más de tipo recreativo que de trabajo, o que estas cuentas sean utilizadas desde sitios remotos por personas diferentes al usuario autorizado, o un consumo excesivo e innecesario de algunos de los insumos o recursos de la red. Así mismo aparecen usuarios intercambiando información como música, películas, archivos de origen dudoso, trasparentado por el uso de los puertos en cuestión.

Así pues se ve reflejada la necesidad de contar con la observancia por parte de un administrador de la red, no con el fin de tener un control de manera arbitraria, sino con la idea de normar algunos aspectos de su utilización, precisamente como una medida que permita continuar ofreciendo el servicio de red de manera constante y eficiente.

Objetivos

- Designar las actividades del administrador de la red, para el adecuado funcionamiento de la red de computadoras.
- Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.
- Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entender la información que circula en ella.

Alcance

El siguiente procedimiento será aplicable para la determinación de las actividades del administrador de red de una empresa.

Procedimiento.

Referente a la administración de la red

a) Realizar un inventario del hardware de los componentes que conforman las estaciones de trabajo (discos, tarjetas, por ejemplo).
b) Anotar los cambios que se producen en el inventario del hardware.
c) Verificar que el hardware asociado (para servidores o terminales) sea apto para trabajar con el software de red que se va a utilizar.
d) Se debe efectuar una copia de seguridad de los discos del software de red.
e) Cuando el equipo es nuevo, es recomendable darle formato en su totalidad y dejar el espacio suficiente para la instalación del software de red que se vaya a utilizar.
f) Se deberán establecer los parámetros de configuración de los archivos de configuración del sistema operativo.
g) Detectar y realizar el seguimiento de las averías de los componentes de las estaciones de trabajo y del servidor de red.
h) Realizar un inventario del software instalado.
i) Se debe especificar el número de copias disponibles de los distintos paquetes de software utilizados en la red.
j) Se debe dar seguimiento de la instalación de software y otros archivos en prevención de la introducción de virus.

k) Dar autorización a los usuarios para la utilización de los paquetes de software disponibles.
l) Únicamente el administrador está autorizado para realizar acciones de conectado/desconectado o inicializar nodos y periféricos, así como realizar modificaciones en los equipos, instalar y modificar elementos de comunicación de la red.
m) La instalación de paquetes de cómputo y programas en los servidores generales de red, se llevará acabo por el administrador o personal de soporte técnico de la empresa.
n) Se deben ejecutar tareas de copias de seguridad y la búsqueda de virus.
o) Se llevará un registro del estado de los procesos que se ejecutan en la red.
p) Se tendrá un registro de entradas y salidas de los usuarios de la red.
q) Registrar el arranque de aplicaciones de la red, así como los errores que existan en el arranque de estas aplicaciones.
r) Se deberán tomar medidas sobre los aspectos de protocolos, colisiones, fallos y paquetes.
s) Realizar el análisis para obtener conclusiones y resolver problemas concretos o bien para optimizar el desempeño de la red.
t) Se debe transformar la información para presentarla en formatos apropiados para el entendimiento del administrador.
u) Realizar el análisis de parámetros para obtener conclusiones que permitan deducir rápidamente lo que pasa en la red.
v) Actuar para generar acciones rápidas y automáticas en respuesta a una falla mayor.

Referente al acceso de la red

a) El ingreso al sistema debe ser mediante una clave, la clave debe constar de dos partes: una de conocimiento general (el login o nombre de usuario) y la otra de conocimiento exclusivo (password).
b) Debe establecer políticas de passwords como su longitud, tiempo de vida, seguridad de la base de datos de los passwords.
c) Si la red tiene varios servidores el login deberá especificar el servidor al que quiere estar conectado.
d) Para designar login y password a un usuario, este deberá presentar una solicitud (**ver apéndice B**).
e) Se asignarán los permisos necesarios para el uso de los recursos de la red, previa solicitud del usuario al administrador.
f) Las cuentas del personal que se encuentre laborando en la empresa, se mantendrán activadas mientras el usuario no pida su cancelación, a no ser que la cuenta se encuentre inactiva durante cierto tiempo (se deja a criterio del administrador establecer este tiempo).
g) Realizará el monitoreo de las actividades de los usuarios.

h) Realizar y establecer las políticas generales y de grupo que faciliten la configuración de los usuarios.

Referente el uso de la red

a) La infraestructura de la red se utilizará únicamente para desarrollos de trabajo, de investigación, técnicos y administrativos de la institución, incluyendo los actos promocionales de la misma.
b) Ningún recurso de la red será utilizado para transmitir información a terceros sin previa autorización de la dirección de la empresa.
c) No se ha de permitir el uso de la red para fines de transmisión de información de carácter comercial, o cualquier otra forma que represente un beneficio personal ajeno a la empresa.
d) Establecer políticas de seguridad para los usuarios durante su uso de la red.

Referente a la seguridad

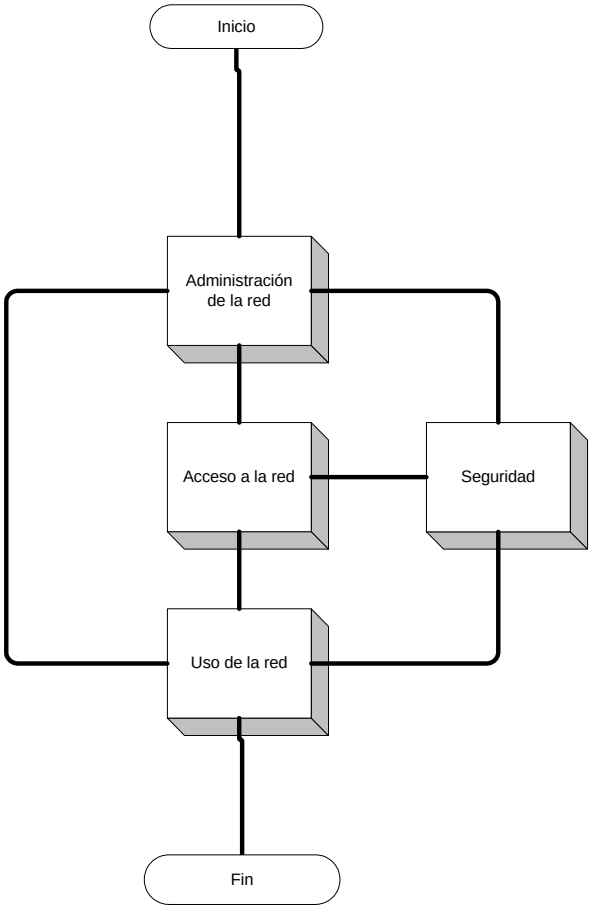
a) Se deberá realizar la identificación de los problemas de seguridad más frecuentes.
b) Desarrollar un plan de seguridad informática y un análisis de seguridad de los equipos de la red, así como su continuo monitoreo.
c) La seguridad debe garantizar:

- La disponibilidad de los sistemas de información.
- La rápida recuperación de los sistemas de información.
- La integridad de la información.
- La confidencialidad de la información.

d) Se realizará el encriptamiento de la información para asegurar su confidencialidad.
e) Deberán existir restricciones de red para controlar el acceso a la red.
f) El administrador otorgará los derechos de acceso de acuerdo al tipo de usuario que requiera hacer uso de la red.
g) Deberá haber un bloqueo de intrusos, es decir, limitar las posibilidades de acceso, si un usuario no autorizado intenta entrar a la red sólo se le permitirá ingresar los datos de “login” y “password” un número determinado de veces. Tras cierto periodo el sistema deberá impedir más intentos de entrada.
h) El administrador debe mantener los programas antivirus actualizados, así como el uso de firewall’s y programas detectores de espías.
i) Es obligación del administrador, proveer las herramientas necesarias para vacunar los discos que utilicen los usuarios antes de introducirlos a las computadoras.
j) Es necesario que los servidores se localicen en salas especiales a las que sólo tenga acceso el administrador, con seguros para evitar que se viole la carcasa del servidor.

k) El administrador debe indicar a los usuarios terminar su sesión en la máquina utilizada cada que terminen su trabajo, esto para evitar el mal uso de su cuenta de usuario.
l) No se permitirá a los usuarios hacer uso de dispositivos de almacenamiento tales como discos, cd's, memorias USB o agendas electrónicas sin previo permiso del administrador.
m) La introducción de computadoras portátiles quedará prohibido, hasta que se den los permisos necesarios por parte del administrador.
n) Quedará prohibido el uso de programas de transferencia de datos o archivos, además de uso de mensajeros que puedan vulnerar la seguridad de la red.

Observancia por el administrador



Introducción a la auditoría informática

Capítulo 5

CAPÍTULO 5

INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA

Aunque pareciera fácil de entender, el concepto de auditoría tiene muchas connotaciones, las cuales han surgido debido al gran campo de aplicación que tienen; por ello, es importante conocer algunas definiciones representativas, mediante las cuales podremos comprender las razones de auditar un centro de cómputo o los sistemas informáticos en general.

5. ¿Qué es una auditoría?

Auditoría es la revisión de cualquier actividad que sea susceptible de ser controlada, es decir, aquellas que puedan ser repetibles. La norma ISO 9000:2000 define a la auditoría como: "El proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente para determinar la extensión en que los criterios se cumplan" [18].

La auditoría entonces, es aquel proceso sistemático que nos va a permitir obtener y evaluar de manera lo suficientemente objetiva, la eficiencia y la eficacia con que realizamos nuestro trabajo, independientemente de la actividad a la que nos dediquemos. Nos va a permitir tomar decisiones que permitan corregir los errores (si se tienen) o mejorar lo que hacemos a diario.

Así pues, podemos decir que la auditoría es un examen crítico basado en normas técnicas establecidas o que puedan establecerse, que no implica necesariamente la preexistencia de fallas en nuestro trabajo, sino de detectar oportunidades de mejora que puedan elevar la calidad de nuestros productos.

Algo muy importante y que todavía no hemos mencionado es que la función auditora debe ser totalmente independiente, no sería nada ético que los que evaluaran nuestro propio trabajo fuéramos nosotros; la auditoría no tiene carácter ejecutivo, y sus conclusiones están sujetas a la voluntad de la entidad auditada, por lo que es responsabilidad de ésta, tomar las decisiones pertinentes sobre su trabajo; contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones, y aunque pueden aparecer sugerencias y planes de acción para corregir dichos inconvenientes, éstas reciben el nombre de recomendaciones.

[18] ISO 9000:2000, Sistemas de Gestión de la Calidad – Fundamentos y vocabulario

5.1. Tipos de auditoría

Podemos clasificar a las auditorías desde diversos puntos de vista, una primera clasificación nos permitiría ubicar el campo de aplicación. De acuerdo con la ISACA(19) las auditorías se pueden clasificar en:

- **Auditoría Financiera.-** Tiene como propósito asegurar la validación de los registros financieros.

- **Auditoría Operacional.-** Tiene como fin evaluar la estructura de control interno de un área o entidad determinada, entre los que se pueden incluir los de aplicación y seguridad lógica de los sistemas.

- **Auditoría Integral.-** Son aquellas que combinan los pasos de la auditoría financiera con los de la operacional.

Las auditorías también pueden clasificarse de acuerdo al periodo de tiempo con que se realizan:

- **Permanente o Continua.-** Cuando se llevan a cabo en periodos cortos de tiempo o en intervalos regulares.

- **Esporádica.-** Cuando se llevan a cabo en cualquier tiempo, mediante pruebas selectivas y llevadas a cabo para examinar a algún área de la organización.

- **Periódica.-** Cuando se llevan a cabo cada cierto tiempo de acuerdo con una planeación.

Ahora bien, considerando la relación que existe entre los auditores y la empresa pueden clasificarse en:

- **Auditoría Interna.-** Cuando ésta se lleva a cabo por empleados pertenecientes a la organización. Los auditores internos deben estar capacitados para revisar trabajos ajenos al suyo, con esto se garantiza la objetividad y veracidad de la auditoría.

- **Auditoría Externa.-** Cuando es llevada a cabo por profesionales independientes, cuyos servicios son contratados por la organización, para analizar sus sistemas de información y presentar un informe de auditoría que exprese su opinión acerca del funcionamiento del sistema.

Finalmente, la última clasificación tiene que ver con el ámbito informático al cual estén enfocadas:

[19] ISACA: Asociación de Auditores de Sistemas Informáticos y Control

- **Regular de Informática.-** Son aquellas en las que se evalúa la calidad de la información existente en las bases de datos de los sistemas informáticos que son utilizados para controlar recursos, su entorno y los riesgos que puedan tener.

- **Especial Informática.-** Consiste primordialmente en el análisis de aspectos específicos relativos a las bases de datos de los sistemas de informáticos, en que haya sido detectado algún tipo de alteración u operación incorrecta de los sistemas.

- **Recurrente Informática.-** Donde se examinan planes concernientes a acciones correctivas, elaborados en auditorías pasadas donde se obtuvo una calificación deficiente o mala.

5.2. Lineamientos generales de auditoría

Debido a la importancia que juegan las auditorías dentro de una empresa, se hace necesario el establecer una serie de lineamientos mínimos de calidad, que deberían seguirse cada vez que se realice una auditoría, a dichos lineamientos se les conocen con el nombre de normas generales de auditoría y se dividen en:

Concernientes al desempeño de las actividades

Planeación
Como primer paso es muy importante que el auditor conozca la entidad sujeta a la auditoría, con el propósito de establecer un plan de trabajo adecuado. Dicho plan debe considerar la delegación de responsabilidades hacia el grupo auditor, así como las pruebas a realizar y el alcance de las mismas.

Estudio del control interno
El equipo auditor debe evaluar y conocer el control interno de los procesos dentro de la entidad a auditar, con la finalidad de llevar a cabo pruebas acordes con los registros que lleva cada organización, en la inteligencia de que cada entidad a ser auditada es diferente.

Obtención de la evidencia suficiente y objetiva
Antes de hacer cualquier dictamen, el equipo auditor debe respaldar sus hallazgos dentro de los procesos auditados con el fin de asegurar la veracidad y credibilidad de la auditoría, es decir, los hallazgos deben ser comprobables y razonables a satisfacción de la entidad auditada.

Concernientes a la personalidad del personal auditor

Competencia del personal
El equipo auditor debe contar con conocimientos suficientes y adecuados, adquiridos ya sea en universidades o instituciones superiores del país. Aunque no es un requisito el

contar con un grado de licenciatura para la auditoría de sistemas de gestión de la calidad, sí es recomendable contar con un título de licenciatura para poder auditar áreas más especializadas ya que se requiere que el personal auditor cuente con experiencia o práctica, que le permita emitir un juicio sólido y veraz.

Diligencia personal
El equipo auditor debe estar conciente de la responsabilidad que implica, haciendo a un lado los juicios de tipo personal y enfocarse a emitir un dictamen profesional y convincente del trabajo realizado.

Independencia mental
La mayoría de las veces es difícil que las organizaciones acepten sus errores, para que la entidad auditada confíe en que su trabajo es realizado correctamente, éste debe ser avalado por un auditor, el cual de manera independiente y objetiva emitirá una opinión acerca del trabajo realizado dentro de la empresa.

Normas para el dictamen
El auditor profesional debe apegarse a normas internacionales que garanticen la calidad de su trabajo, y debe aclarar en lo posible su relación y responsabilidad con el área auditada.

5.3. Auditoría informática

Como mencionamos al inicio del presente capítulo, el hablar del término auditoría no es nada sencillo debido a las connotaciones que esto conlleva, más aún si hablamos de auditorías del tipo informático o simplemente auditorías informáticas. Y es que, el primer problema real está relacionado con la comprensión de su significado.

Mientras la palabra auditoría deja abierta muchas aristas en cuanto a su campo de aplicación y a la especialización que puede tener, la palabra informática crea un nuevo y vasto campo de aplicaciones que pueden ir desde la utilización de computadoras personales en juegos, hasta la planeación estratégica de toda una compañía basada en el uso de la información entre sus diversas sucursales.

La auditoría informática la podemos definir como aquel conjunto de procedimientos enfocados a revisar y evaluar, ya sea total o parcialmente, un sistema informático, con el fin de proteger sus activos y/o recursos, verificar que sus actividades se lleven a cabo de forma eficiente, en concordancia con la normativa existente en cada empresa y con apego a las normativas nacionales e internacionales con el fin de garantizar una adecuada toma de decisiones.

Por otro lado la IEEE en su estándar 803 define a la auditoría informática como la:

“Evaluación independiente de la organización, de los productos o procesos de software para asegurar el cumplimiento de estándares, lineamientos, especificaciones y

procedimientos, considerando como criterios objetivos de comparación los documentos que tienen que ver con:

- *La forma o contenido de los productos que se producirán.*
- *El proceso mediante el cual se desarrollan aplicaciones*
- *Los indicadores para asegurarse del cumplimiento de los estándares o lineamientos establecidos.*

Una última definición nos la proporciona la ISACA, organismo internacional encargado de establecer los estándares para las labores de auditoría informática:

"Una auditoría informática es cualquiera que considere la revisión y evaluación de cualquier aspecto de un sistema automatizado de procesamiento de información, incluyendo procesos relacionados no automatizados y la interfase entre ellos"

Como podemos notar en las definiciones anteriores, la auditoría informática no solamente abarca la evaluación de los equipos de cómputo, sino todos los sistemas de información en general, desde sus entradas, pasando por los procedimientos y controles que se tengan; archivos, seguridad y obtención de información, de un departamento o área específica.

El objetivo de una auditoría es verificar la conformidad de los procesos y productos, certificar el apego a estándares, lineamientos, especificaciones y procedimientos. Para lo cual el equipo auditor debe considerar los siguientes criterios a evaluar:

- Los elementos de software.
- Los procesos que los producen.
- Los proyectos.
- Los programas de calidad.

La función auditora se ejerce mediante el examen, revisión y evaluación de la fiabilidad de la información y la emisión de informes y certificaciones respecto al grado de cumplimiento de las políticas, normas, procedimientos y decisiones de carácter relevante en todo o en parte de la empresa, en el marco de los requerimientos que la justifique o en razón de los objetivos establecidos por la alta dirección. Surge como consecuencia del avance tecnológico en el que la información se convierte en un recurso más de la empresa y como tal debe ser administrado.

5.3.1. Clasificación de la auditora informática según su área de aplicación

La auditoría informática puede conducirse de dos maneras distintas, por un lado, puede auditar las principales áreas de cualquier departamento y por otro, puede auditar las aplicaciones que funcionan dentro de una empresa. Sin importar el rumbo de acción que tome, ambas auditorías siguen una serie de pasos característicos, aunque tengan un

objetivo distinto, para darnos una idea más clara de lo anterior, a continuación plantearemos algunos campos de aplicación de la auditoría informática.

Auditoría física
Tiene como objetivo asegurar el funcionamiento de los sistemas así como su integridad física. Evalúa tres tipos de seguridad: la lógica, la física y la de comunicaciones, ejemplos de lo anterior pueden ser edificios, instalaciones, equipamiento y telecomunicaciones, datos y personas.

Auditoría de la ofimática
Se le llama ofimática al conjunto de sistemas informáticos que generan, procesan, almacenan, recuperan y presentan los datos relacionados con el funcionamiento de una oficina. Una auditoría de la ofimática evalúa parámetros tales como: la economía de la empresa, la eficacia y eficiencia de la organización, la seguridad y los objetivos vigentes.

Auditoría de la dirección
Este tipo de auditoría se centra en evaluar más la gestión que las capacidades técnicas. Por ello las áreas de interés de este tipo de auditoría son:

- Planificación estratégica.- Se busca garantizar la existencia de un plan estratégico de los sistemas informáticos.

- Organización y coordinación.- Se evalúa la forma en cómo se encuentran estructurados los recursos, los flujos de información y los controles que nos van a permitir cumplir con los objetivos planeados.

- Control.- Se verifica el desarrollo de los planes estratégicos y operativos, así como de los proyectos que se desarrollan. Incluye aspectos tales como: ejecución del presupuesto, la evolución de los costos, planes de formación y capacitación, la evolución de la carga de las computadoras y otros recursos.

Auditoría del desarrollo
Abarca todas las fases que deben seguir desde que aparece la necesidad de contar con un determinado sistema, hasta que éste es construido e implantado. La auditoría del desarrollo verificará la existencia y aplicación de procedimientos de control adecuados, que puedan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según estos principios de ingeniería.

Auditoría del mantenimiento de software
La etapa de mantenimiento consume gran parte de los recursos asignados en un proyecto de software. Por lo que esta etapa debe ser considerada en los estudios de productividad y de auditoría.

Los aspectos más importantes que contempla este tipo de auditoría son:

- La documentación de los cambios realizados.

- La documentación de las revisiones técnicas formales.
- Control de la aceptación final de los cambios para saber que todo procedió satisfactoriamente.

Auditoría de base de datos
Este tipo de auditoría no requiere más detalles salvo que para su evaluación debe considerarse una revisión de todo el ciclo de vida de la misma.

Las principales áreas que considera la auditoría de base de datos son:

- Concepción de la base de datos y selección del equipo.
- Diseño de la base de datos y carga de información.
- Explotación y mantenimiento.
- Revisión post-implantación.

Auditoría de técnica de sistemas
Este tipo de auditoría consiste en la evaluación de un conjunto de actividades destinadas a la instalación y mantenimiento adecuado de la infraestructura informática. El cumplimiento de dichas características constituye el objetivo de los sistemas de información y el cual se expresa en términos de nivel de servicio.

Auditoría de calidad del software
La calidad del software se define como la concordancia con los requisitos funcionales y de rendimiento explícitamente establecidos, de acuerdo a los estándares existentes y con las características implícitas que se espera de todo software desarrollado profesionalmente. Una auditoría de calidad tiene como objetivo mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar adversamente esa confianza, se basa en 6 puntos primordiales: funcionalidad, fiabilidad, usabilidad, eficacia, mantenibilidad y portabilidad del software.

Auditoría de seguridad
Actualmente existe un tremendo “boom” por este tipo de auditoría ya que la información se ha convertido en un activo más de las empresas modernas, la seguridad informática puede llegar a relacionarse no sólo con los equipos y los entornos técnicos, sino también a la información que se encuentre almacenada en otros soportes tales como discos ópticos o discos extraíbles que requiere protección adicional.

Algunas áreas que puede abarcar una auditoría de seguridad pueden ser:

- Los controles directivos, donde se incluyen las políticas, normas, procedimientos, planes, funciones, objetivos de control, presupuesto y métodos de evaluación de riesgos.
- El desarrollo de políticas adecuadas: procedimientos, uso de estándares nacionales e internacionales, guías y recomendaciones.
- Amenazas físicas externas.

- Controles de acceso adecuados y suficientes, tanto a nivel físico como a nivel lógico para que cada usuario pueda acceder solamente a los recursos autorizados.
- Protección de datos.
- Comunicación y redes.
- Desarrollo de aplicaciones en un entorno seguro, con controles de seguridad en todos los productos desarrollados.

Auditoría de Redes
Dado que hoy en día la mayor parte de la información, por no decir toda, transita por lugares físicamente alejados de las personas responsables, supone también un mayor control de seguridad sobre todo en la instalación física, ya que por su naturaleza puede ser blanco de ataques relativamente sencillos.

En las redes de comunicación pueden presentarse tres tipos básicos de incidencias en la información: alteración de bits, alteración de tramas, alteración de secuencia. Lo cual nos lleva a que los principales riesgos a detener son: la “indagación”, que es cuando un mensaje es leído por un tercero; la “suplantación”, cuando un tercero introduce un mensaje espurio que el receptor cree proviene de un emisor legitimo y la “modificación”, cuando un tercero altera el contenido del mensaje real.

En la auditoría de redes uno de los primero puntos a revisar son aquellos concernientes con la administración de la red, entre los que podemos incluir:

- Gestión de la red, inventario del equipo de comunicaciones y normativa de conectividad.
- Revisión de costos, asignación de proveedores y servicio de transporte, balanceo entre tráfico de rutas y selección de equipo apropiado con los requerimientos de la empresa.
- Participación activa en la estrategia de procesos de datos, uso de estándares en el desarrollo de aplicaciones de red y evaluación de las necesidades de comunicación.

Auditoría de las aplicaciones
El objetivo que persigue una auditoría de aplicaciones es verificar el grado de cumplimiento de éstas de acuerdo a los requisitos documentados del cliente, así como el grado de alineación con las políticas de la empresa y el apego a estándares nacionales e internacionales.

5.4. Normas generales para la auditoría informática

A partir de los años noventas se han venido desarrollando una serie de normas generales asociadas a la auditoría en informática por medio de asociaciones tales como la ISACA. Actualmente existen 8 normas principales de auditoría informática y 12 normas relacionadas, como no es propósito de este trabajo tratar a fondo rubros de la informática

más especializados, solamente se trataran las 8 primeras normas concernientes a los principios generales para toda auditoría informática que se realice. Las normas generales son aquellas reglas mandatorias que deben seguir los auditores informáticos en la ejecución de la auditoría y la publicación de resultados.

Carta de Auditoría
Autoridad, responsabilidad y registro contable, toda esta información debe ser correctamente documentada en una gráfica de auditoría o carta compromiso

Independencia profesional
El auditor se sistemas de información debe ser completamente independiente al ente auditado en actitud y apariencia.

Relación Organizacional
La función auditora de sistemas de información debe ser suficientemente independiente del área a ser auditada para permitir cumplir con el objetivo completo de auditoría.

Ética profesional y Normatividad
Código de ética profesional.
El auditor de sistemas de información se debe adherir completamente al código de ética profesional de la auditoría de información y control de ISACA.

Cuidado Profesional
Debe existir un estricto cuidado profesional de observar y seguir todas las normas de la auditoría informática por parte de los auditores.

Competencia
Capacidades y conocimiento.
El auditor de sistemas de información debe ser técnicamente competente, contar con las capacidades y el conocimiento necesario para llevar a cabo el trabajo de auditoría que se le encomiende.

Continuidad en la educación profesional
El auditor de sistemas de información debe mantener actualizada su capacidad técnica, mediante el estudio continuo.

Planeación
Planeación de la auditoría.
El auditor de sistemas de información debe planear detalladamente su trabajo, para determinar claramente los objetivos que persigue la auditoría y cumplir estrictamente con todas las normas de auditoría de sistemas de información.

Medición del trabajo de auditoría
Supervisión.

El equipo auditor de sistemas de información debe ser supervisado para contar con la certeza de que los objetivos de la auditoría serán cumplidos y que las normas generales de auditoría se respetarán en todo el ámbito que aplique.

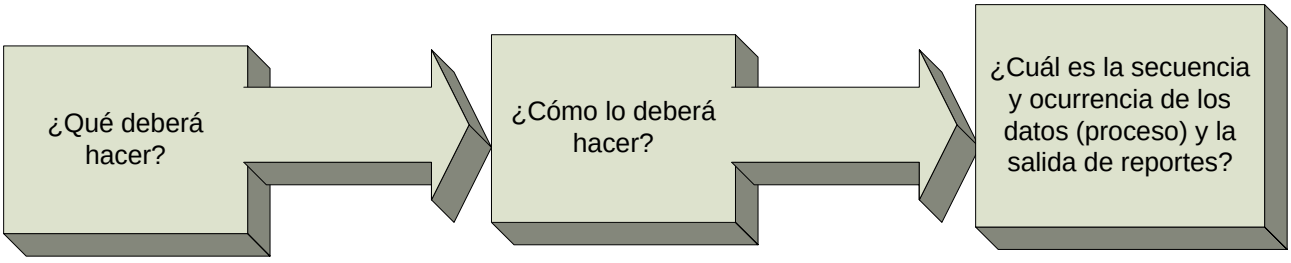
Evidencia
Durante la realización de la auditoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, relevante y útil para cumplir plenamente con los objetivos marcados en la auditoría. Los hallazgos encontrados en la auditoría y las conclusiones asociadas deben estar completamente sustentadas por un correcto análisis e interpretación de la evidencia encontrada.

Reportes
Reportes, contenido y formato.
El auditor de sistemas de información debe proporcionar todos los reportes en un formato adecuado, entendible, que comprenda todo el trabajo de auditoría. En el reporte de auditoría se deben marcar el alcance, los objetivos, periodo de análisis y la naturaleza y extensión del trabajo de auditoría. En el reporte se identificará plenamente a la organización, marcando aquellas áreas que deben tener acceso al reporte de auditoría y aquellas restricciones de circulación que apliquen. En el reporte se deben mostrar los hallazgos, conclusiones y recomendaciones y todas las calificaciones que el auditor tenga con respecto a la auditoría llevada a cabo.

Actividades de seguimiento
El auditor de sistemas de información solicitará y evaluará la información relacionada con hallazgos relevantes previos, conclusiones y recomendaciones para determinar dónde se deben implantar acciones de manera inmediata.

5.5. Estándares internacionales para la auditoría de sistemas de información

Para poder llevar a cabo una auditoría informática de calidad, es recomendable seguir algunas de las guías que se presentan a continuación. En esta etapa el auditor debería analizar las especificaciones del sistema, basándose en las siguientes premisas:



Cabe mencionar que los siguientes estándares o guías para la realización de auditorías no son los únicos, pueden existir muchos más o incluso uno propio desarrollado por cada empresa.

Estándares internacionales

Comité para el patrocinio de las organizaciones de la comisión treadway (COSO por sus siglas en inglés)

La meta del estándar COSO es mejorar la manera de controlar una empresa a través del establecimiento de un sistema integral de control. Este sistema permitirá cumplir con las metas económicas establecidas y administrar el riesgo de una empresa.

COSO hace recomendaciones de cómo definir, mejorar la eficiencia, evaluar, implementar e informar acerca de los sistemas de control. El estándar enfoca su marco de trabajo en la administración de la empresa y su control, también puede utilizarse como punto de referencia para enmarcar los esfuerzos para lograr la gobernabilidad de la tecnología de la información. Considera los requerimientos de la tecnología de la información de una manera general, sin embargo, sus conceptos y definiciones pueden aplicarse para administrar y controlar los diferentes usos de la misma.

Organización internacional para la estandarización / Comisión internacional electrotécnica 17799:2000

Este estándar fue publicado por la Organización Internacional para la Estandarización (ISO por sus siglas en inglés) y la Comisión Internacional Electro-técnica (IEC por sus siglas en inglés). El estándar BS 7799-1 publicado en el año 2000 contiene dos partes fundamentales: en la primera se establece un código guía para administrar la seguridad de la información y en la segunda la especificación para usar el código guía.
ISO/IEC 17799:2000 provee información a las áreas responsables de implementar la seguridad de la información en una organización. Puede ser punta de lanza para implementar un plan de desarrollo de los estándares de seguridad y de buenas prácticas de administración en una organización.

Para la implementación de la administración de la seguridad, es necesario considerar los requisitos legales o las prácticas que mejor se adapten a cada organización. La seguridad de la información debe considerar por lo menos las siguientes partes:

- Política de Seguridad.
- Seguridad dentro de la organización.
- Clasificación adecuada y control de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Administración de las comunicaciones y la operación.
- Control de acceso.
- Desarrollo y mantenimiento de sistemas.
- Administración de la continuidad de la empresa.
- Indicadores del cumplimiento de los controles establecidos.

Como podemos observar, este estándar contempla de forma primordial la seguridad en la información, haciendo de lado las cuestiones relacionadas con la administración de la tecnología de la información.

Normas internacionales de auditoría de la federación internacional de contadores

La Federación Internacional de Contadores (IFAC por sus siglas en inglés) ha emitido las normas internacionales de auditoría (NIA) 15, 16 y 20.

La norma internacional de auditoría número 15 conocida también como "Auditoría en Entornos Informatizados", contiene una referencia de controles para el procesamiento electrónico de datos y la necesidad de éstos en ambientes donde los instrumentos tradicionales de auditoría (evidencias generalmente en papel) no son visibles para los auditores al momento de realizar su trabajo.

La norma internacional de auditoría número 16 referente a "Técnicas de Auditoría Asistidas por Computadora" describe técnicas y procedimientos de auditoría que se deberían seguir en entornos altamente informatizados con ayuda de computadoras y otras tecnologías.

Por último, la norma internacional número 20 nos presenta los efectos de un entorno informatizado en la evaluación de sistemas de información contables.

Control y auditoría de sistemas de la fundación para la investigación del instituto de auditores internos (SAC por sus siglas en inglés).

Ofrece una guía de estándares y controles para los auditores internos en el área de auditoría de sistemas de información y tecnología. Sus objetivos principales son el control de la efectividad y eficiencia de las operaciones, la integridad de la información y el cumplimiento de normas y regulaciones.

Metodología de análisis y gestión de riesgos de los sistemas de información (MARGERIT) del consejo superior de informática del ministerio de administraciones públicas de España.

Esta metodología fue emitida en España por el consejo superior de informática y recoge las recomendaciones de las directivas de la Unión Europea en materia de seguridad de sistemas de información, esta metodología se enfoca en el estudio de los riesgos que pueden afectar los sistemas de información así como su entorno.

Contiene una serie de recomendaciones que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados; además desarrolla el concepto de control de

riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de las normas legales.

5.6. Normatividad para auditores (código de ética)

La “Information Systems Audit and Control Association” o ISACA, ha desarrollado una normatividad o código de conducta personal para los miembros de dicha asociación y para las personas que cuenten con la designación de auditor de sistemas de información certificado, avalado por la Asociación Mexicana de Auditores en Informática (AMAI).

Los auditores de sistemas de información deberán:

- Apoyar el establecimiento y cumplimiento de las normas, procedimientos, estándares y controles para los sistemas de información.
- Servir en el interés de sus empleadores, cliente y al público en general de una manera diligente, leal y honesta; no se deberá tomar parte de ninguna actividad impropia o ilegal.
- Mantener la privacidad y la confidencialidad de la información obtenida en el curso de sus actividades a menos que se le requiera mediante una autoridad legal. La información no deberá utilizarse para beneficio personal o ser divulgada por terceros no autorizados.
- Desarrollar sus actividades de una manera independiente y objetiva y evitar que afecten o puedan afectar su independencia u objetividad.
- Mantener un nivel de competitividad en los respectivos campos de la auditoría de sistemas de información, participando en actividades de desarrollo profesional.
- Acordar emprender solamente aquellas actividades que estén dentro de la capacidad profesional de cada persona.
- Realizar sus actividades con el debido cuidado profesional.
- Informar a las partes los resultados de la auditoría a los sistemas de información realizada, revelando la evidencia y documentando el material suficiente sobre el cual se basan sus conclusiones y recomendaciones.
- Fortalecer el conocimiento de la dirección, clientes y el público en general para lograr el entendimiento de la auditoría de sistemas de información.
- Mantener altos estándares de conducta y carácter en actividades personales y profesionales.

5.7. Conducción de una auditoría

Muchas organizaciones se quejan de la poca claridad en las normas internacionales tales como la ISO 9001:2000, para comenzar a operar un sistema de gestión de la calidad, argumentando que si bien nos especifica lo que debemos o deberíamos hacer, no nos indica cómo realizarlo, lo mismo pasa con las auditorías.

Si bien es cierto que no nos dice cómo hacerlos, es porque cada organización, cada empresa, cada departamento, tiene una forma propia de hacer las cosas, una forma diferente y única para realizar una actividad, es por eso, que cada departamento debe ser auditado de una manera diferente, con un nivel distinto de interés de acuerdo a la importancia que juegue dentro de la organización. La auditoría informática es una actividad muy importante, es una auditoría que debe ser conducida con la responsabilidad y seriedad que se merece, ya que estamos hablando que la información contenida en los sistemas informáticos es de vital importancia para los planes de la empresa u organización.

Programa de Auditoría.

Toda auditoría formal comienza con un programa de auditoría, es decir, un grupo de procedimientos documentados y diseñados para cumplir con los objetivos planeados de la misma. En dicho programa se incluyen los siguientes rubros:

Sujeto de auditoría.- Es la entidad a auditar, puede ser un departamento, empresa, etcétera.

Objetivo de la auditoría.- Describe el propósito de la auditoría.

Alcance.- Se delimitan las fronteras de la auditoría describiendo su campo de acción, es decir, a qué departamento, sección o parte de la empresa, estará enfocada sola y exclusivamente.

Planeación de la auditoría.- En esta parte se hace una identificación de las herramientas, técnicas y recursos que se van a requerir para poder llevar a cabo la auditoría. Se identifican las fuentes de información a evaluar y se revisan aspectos tales como: diagramas de flujo, políticas, normas y procedimientos del área, así como la evidencia objetiva que dé plena validez del trabajo que se ha venido realizando por la organización.

Procedimientos y pasos de auditoría.- En este apartado es donde se describen las actividades secuenciales que se van a realizar en la auditoría; debiendo contener la información necesaria para facilitar su entendimiento y aplicación. Aquí se le da respuesta a las siguientes preguntas:

¿Qué es lo que se va a hacer?
¿Quién lo va a hacer?
¿Cómo lo va a hacer?

Su objetivo es determinar si los controles están siendo aplicados de acuerdo con la documentación generada por el ente auditado. En otras palabras, determina si los controles están siendo aplicados de forma que cumplan con las políticas y procedimientos establecidos por la alta dirección.

Procedimientos para examinar los resultados de pruebas o análisis.- Establece los parámetros y niveles de aceptación de las evidencias recabadas por el equipo auditor.

Procedimiento de comunicación con la alta dirección.- Se establecen los canales de comunicación entre la alta dirección y los distintos departamentos de una empresa.

Procedimiento para la preparación del informe de la auditoría.- Establece los lineamientos necesarios y suficientes para poder realizar un informe de auditoría.

Procedimiento de análisis del seguimiento.- Normas para evaluar la eficiencia y la efectividad, contiene procedimientos para examinar controles, revisar y evaluar la validez de documentos, políticas y procedimientos.

Aunque un plan de auditoría solamente es el primer paso para llevar a cabo una auditoría de calidad, éste nos servirá para establecer la secuencia de actividades que el equipo auditor realizará dentro de la empresa, además, permite comprender la situación de la misma, evaluar su estructura de control y después comenzar a desglosar cada medio de control uno por uno. Para este trabajo se han divido las actividades de la auditoría en seis etapas primordiales: alcance y objetivo de la auditoría, estudio inicial del entorno auditable, determinación de los recursos necesarios para realizar la auditoría, planeación, actividades propiamente dichas de la auditoría y el informe final.

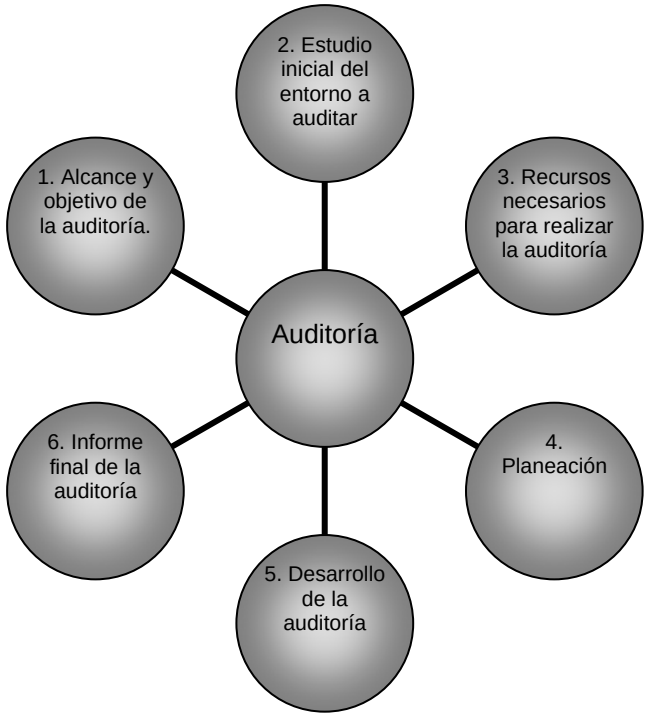


Figura 5.1 Actividades de una auditoria

5.7.1 Establecimiento del alcance y objetivo de la auditoría informática

Uno de los puntos más importantes es establecer los límites de lo que queremos evaluar, delimitar claramente lo que se desea sin irnos más allá de nuestros alcances. Muchas organizaciones modernas se enfrentan a la problemática de definir cuáles son los alcances de un proceso de auditoría, ya que siempre se va a querer ir más allá de lo que realmente somos capaces de demostrar. En este punto de lo que se trata, es de establecer un estado actual que sea medible y comprobable mediante evidencia objetiva, esto último muy importante.

El alcance de la auditoría debe expresar claramente y por escrito los límites de la misma, se deben establecer las funciones, aplicaciones, áreas a ser auditadas, así como aquellas excepciones (lo que no se va a auditar).

Sus objetivos primordiales son:

- Establecer las garantías necesarias de que los objetivos de control se satisfacen.
- Identificar las oportunidades de mejora si es que existen.
- Dar consejos sobre posibles acciones correctivas dentro de la empresa.

Para que podamos establecer los alcances reales de una auditoría podemos llevar a cabo una serie de actividades que nos serán de ayuda, entre las que se encuentran:

Investigación y análisis del entorno auditable
Es decir, los procesos de negocio involucrados; las plataformas y sistemas de información que sostienen el proceso de negocio, y su relación para/con los demás sistemas y plataformas dentro de la organización; los roles del personal del área de sistemas y los riesgos asociados al proceso.

Identificación de los requisitos de información
Algunos sistemas por su naturaleza pueden ser fuente de riesgos, que por lo general tienen más que ver con cuestiones lógicas del sistema y no operativas. Es por eso, que la alta dirección debería contar con controles diseñados, que reduzcan al mínimo los riesgos propios del sistema. Haciendo importante su identificación. Entre los parámetros más comunes que se pueden tomar existen:

- Cambios recientes en el medio ambiente del negocio que puedan afectar el desempeño de los sistemas.
- Cambios recientes del personal del área de sistemas.
- Controles de monitoreo al área de sistemas por parte de la alta dirección.
- Reportes de auditorías recientes.
- El grado de dependencia de la organización hacia los sistemas de información.
- El uso de software de sistemas sensibles que puede permitir a los empleados hacer cambios.

5.7.2. Estudio inicial del entorno auditable

Esta etapa comienza en el momento que es documentada la comprensión de los aspectos más importantes de los sistemas informáticos y sus controles generales asociados.

Dichos controles pueden ser clasificados en tres rubros principales:

Control de ambiente
Describe las condiciones generales en las que operan los sistemas de control. Esto nos permitirá tener mayor confianza en los controles como fuente de satisfacción de la auditoría y de reducir la cantidad de evidencia requerida.

Controles directos
Son aquellos diseñados para evitar o detectar errores o irregularidades que afectarían directamente a la información en general y aquellas funciones de procesamiento.

Controles Generales
Son lineamientos generales que pueden abarcar a toda la empresa y que contribuyen significativamente a la efectividad de todos los controles directos.

Una vez que son conocidos todos los controles con los que cuenta la empresa, se hace necesario que el equipo auditor conozca las funciones y actividades generales del personal del lugar, es decir, debe conocer la organización. Un documento muy útil para ello es el llamado: "organigrama general de la empresa", donde se expresa su estructura oficial, contiene todos los departamentos y sus relaciones jerárquicas o funcionales, algunos pueden incluir los flujos de información. Otro documento muy importante es el "manual de la organización", en donde se documentan entre otras cosas las funciones del personal, sus responsabilidades, así como el organigrama de cada departamento.

El equipo auditor deberá hacer hincapié en el cumplimiento de lo escrito en dicho manual y para ello debe considerar los siguientes puntos:

Organigrama.- Es un documento en donde se expresa la estructura oficial de la organización a auditar. Si se descubriese que existe más de un organigrama oficial, el equipo auditor deberá poner de manifiesto tal circunstancia.

Departamentos.- Son aquellos órganos que siguen inmediatamente a la dirección. El equipo auditor deberá describir brevemente las funciones de cada uno de ellos.

Relaciones jerárquicas y funcionales.- Una relación de jerarquía implica la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente de subordinación. Es responsabilidad el equipo auditor verificar que ambas relaciones se cumplan y sean respetadas.

Flujos de información.- Los flujos de información dentro de una organización son necesarios para una gestión eficiente. En ocasiones, las organizaciones crean de forma

espontánea canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeñas o grandes fallas en la estructura y en el organigrama que los representa. Otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Ambos flujos de información son indeseables y producen graves perturbaciones en la organización.

La tarea del auditor es verificar que los canales de comunicación se encuentren establecidos, sean usados y conocidos por todo el personal del área.

Número de puestos de trabajo.- El auditor informático debe verificar que se cuenta con el número apropiado de personal en cada departamento. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno Operacional.- El equipo auditor debe conocer el entorno auditable, el cual abarca los siguientes puntos o áreas de observación:

- Situación geográfica de los sistemas. El lugar físico donde se encuentran los sistemas informáticos.

- Arquitectura y configuración del hardware y software. Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismo deben constituir un sistema compatible e intercomunicado.

- Inventario de hardware y software. El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación.

- Comunicación y redes de comunicación. En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.

- Aplicaciones, bases de datos y archivos. En este punto se consideran aspectos tales como el volumen, antigüedad y complejidad de las aplicaciones; las metodologías con que se cuenta para el diseño y programación; los modelos de documentación de cada aplicación; la cantidad y complejidad de las bases de datos y archivos; y en general una descripción de los sistemas instalados.

5.7.3. Recursos necesarios para realizar la auditoría

Una vez que se tiene el estudio inicial, el equipo auditor está en condiciones para determinar los recursos humanos y materiales, que han de emplearse en la auditoría. Dichos recursos pueden incluir en la parte material cosas tales como software: programas propios de la auditoría y algunos programas de monitoreo, los cuales se utilizan en función del grado de desarrollo observado en los sistemas auditados y de la cantidad y

calidad de los datos que ya existen. Con respecto a los recursos humanos, su cantidad y características estarán en función del volumen y la materia auditable.

Los puntos primordiales que debe cumplir todo el personal auditor es la capacitación constante, con alto sentido de la moralidad, al que se le pueda exigir la optimización de recursos y se le retribuya justamente por su trabajo.

También se debe contar con personas asignadas por los usuarios para que en el momento en el que se le solicite información, o se efectúe alguna entrevista, se nos sea proporcionada de forma inmediata.

Cabe mencionar que la auditoría informática deber ser ejercida por personal experto en campos muy especializados y que esté en capacitación constante. Esto debido a que la tecnología está en evolución continua, y se hace necesario mantener la competencia del auditor a través de las actualizaciones técnicas que surjan.

5.7.4. Planeación

Cuando se han establecido los recursos necesarios para la auditoría se procede a establecer un plan de trabajo. No hay que olvidar que un componente básico en todo proyecto es la planeación, el cual constituye un delicado trabajo de balanceo de recursos que el auditor debe considerar al preparar el plan. Generalmente para realizar un plan de trabajo se siguen los siguientes criterios:

Revisión por áreas generales o áreas específicas
Entre mayor sea el tamaño del área a auditar, implicará una elaboración más compleja y costosa; mientras que entre más especifica y pequeña, menos compleja y mucho más económica.

Volumen de la auditoría
Se refiere a la cantidad de auditores que formarán al equipo auditor así como el número de especialistas requeridos para llevar a cabo la auditoría.

Actualmente existen muchas herramientas de administración de proyectos que bien pueden ser aplicadas para administrar auditorías. Básicamente todas incorporan los siguientes pasos:

- Desarrollo de un plan detallado, donde se desglosen todos los pasos de auditoría necesarios a través de una línea de tiempo.
- Reporte de la actividad real del proyecto contra lo planeado, debe existir un sistema mediante el cual los avances del proceso de auditoría sean registrados y documentados, contra los tiempos estimados en el plan maestro de auditoría.
- Ajuste del plan y realización de acciones correctivas (si es que se requieren), cualquier desviación en el tiempo o aquellos objetivos que no se han cumplido en tiempo y forma, pueden generar cambios al plan, por ello se hace necesario el contar con “acciones correctivas” que permitan recuperar el tiempo perdido.

Una vez realizado el plan de auditoría se procede a la programación de las actividades y el desarrollo de la auditoría.

5.7.5. Desarrollo de la auditoría

En esta parte se llevan a cabo todas las actividades planeadas, las cuales pueden incluir distintas técnicas o herramientas para la consecución de los objetivos planteados. Generalmente una auditoría comienza con una reunión de entrada con el personal del departamento a auditar, o con la alta dirección si es que se va a auditar a toda la organización. En dicha reunión se exponen puntos tales como la agenda, el objetivo y alcance de la auditoría, los canales de comunicación, el personal a ser contactado por los auditores y se define la hora para la reunión final o de salida, también se puede abrir un espacio de aclaración de dudas.

A continuación se empieza la investigación por parte de los auditores, las listas de verificación son una guía indispensable para no olvidar nada, se examina la "evidencia objetiva" con las que cuenta la organización, y se toman notas de las observaciones pertinentes así como de detalles para referenciar y discriminar entre una posible no conformidad y una mera observación. Algunas otras herramientas para llevar a cabo la investigación incluyen entrevistas con el personal, muestreos aleatorios de funcionamiento de los sistemas, simulación de situaciones que se pueden presentar, uso de estadísticas históricas para cotejar el desempeño de los sistemas de información, y en general aquellas herramientas que el auditor considere necesarias, algunos otros ejemplos incluyen:

- Cuestionarios generales para el personal.
- Conocimiento de estándares por parte del personal.
- Monitores o indicadores de desempeño.
- Matrices de riesgo.

Una vez que se ha llevado a cabo la investigación, el equipo auditor se reúne para analizar las observaciones encontradas, y discutir cuales de ellas son posibles no conformidades, se debe asegurar en base a evidencia objetiva cuáles sí son de aquellas que no lo son, se documentan los reportes de no conformidad y se prepara un resumen de la auditoría a presentar en la reunión de salida con el personal de la empresa.

Como última actividad dentro del día de auditoría, se lleva a cabo la reunión final o de salida con el personal de la empresa, aquí se presenta un resumen general de la auditoría, donde se da a conocer el reporte de no conformidades y se pide su firma por parte del personal auditado, se recomienda al auditor ser la parte conciliadora, ya que generalmente las empresas "no reconocen los hallazgos de la auditoría". Se debe dar oportunidad de aclarar todas las dudas que sean necesarias a la organización auditada, con el fin de suavizar las cosas y evitando entrar en debate. Se dan las conclusiones del equipo auditor y se solicita el programa de acciones correctivas a tomar por parte de la empresa. Se

indica la fecha de entrega del reporte final de auditoría y se agradece la colaboración de la empresa.

5.7.6. Informe final de auditoría

Toda auditoría no se puede considerar completa hasta que no se tenga un documento donde estén plasmados sus resultados (oportunidades de mejora y recomendaciones), dicho documento es conocido como reporte de auditoría o informe final.

Todo informe de auditoría comienza con la fecha de comienzo de la misma y la fecha de redacción del informe. Se incluye un número de auditoría único de control interno, los datos del área o empresa auditada, los objetivos y alcance de la auditoría y aquellos documentos que sirven de referencia; los nombres de todo el personal contactado dentro de la organización así como los nombres del personal del equipo auditor, la descripción de la auditoría, las fortalezas de la organización, las oportunidades de mejora y los compromisos establecidos por la organización, las firmas del equipo auditor y las conclusiones finales.

Por cada tema dentro de la descripción de la auditoría se debería seguir el siguiente orden en los párrafos:

- **Situación actual.-** Se expone la situación que se encuentra planeada y se compara contra la situación real que se encontró al momento de realizar la auditoría.
- **Tendencias.-** Se establecen los parámetros que permitan estados deseados o pretendidos.
- **Puntos débiles o amenazas.-** Áreas de oportunidad de las empresas, para corregir o fortalecer posibles observaciones y no conformidades.
- **Recomendaciones.-** Se exponen sugerencias o posibles cambios en el modo de hacer alguna actividad.

Para el caso de las oportunidades de mejora, se hace necesario el establecer una serie de hechos que deben ser consignados en el informe de auditoría, y que se muestran a continuación:

Hecho encontrado

- Debe ser relevante tanto para el auditor como para el cliente.
- Ha de ser preciso y por ende convincente.

Consecuencias del hecho

- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho

- Se debe redactar las influencias directas de un hallazgo para/con respecto a los demás procesos dentro de la organización.

Conclusión del hecho

- Solamente cuando la exposición del hallazgo haya sido extensa.

Recomendaciones

- Deben ser lo suficientemente claras por simple lectura.
- Deben ser concretas.
- Su redacción debe ser de forma que vaya dirigida expresamente a la persona o las personas que pueda implementarlas.

Por último, el auditor será requerido para presentar el resultado del trabajo de auditoría en los diferentes niveles de administración dentro de una empresa.

5.8. Beneficios de seguir una normatividad de calidad en la auditoría informática

Con cada día que pasa, las empresas modernas se enfrentan a diversos problemas, los cuales van desde conflictos internos con los empleados, hasta problemas en la economía mundial, eso sin mencionar, los costos de producción y la inestabilidad del tipo de cambio de cada país. Sin duda alguna, la calidad es el factor que determinará en un futuro qué empresas sobreviven y cuales no, y es que las presiones internacionales y nacionales están generando la obligación de certificarse. Aquellas que no lo hagan tarde o temprano se verán desplazadas por aquellas que sí siguieron las recomendaciones e invirtieron en su mejoramiento. Por ello, las empresas que se dedican al negocio de los sistemas deben considerar la inversión en el área de calidad como un “cheque al portador”.

Diversos son los beneficios que aporta una auditoría al conjunto de una organización:

1. Anima a los directivos a que examinen la gestión de recursos humanos en conjunto.

2. Fomenta la idea de que todos los directivos son directivos de recursos humanos.

3. Programa espacios de tiempo para estudiar el valor de las prácticas existentes en la gestión de recursos humanos y anima a directivos y al personal a informar sobre cuestiones importantes.

4. Estimula el cambio.

5. Valora la contribución de los recursos humanos al logro de los objetivos estratégicos de la organización.

6. Determina periódicamente los puntos fuertes y áreas de mejora que afectan a las personas.

7. Poder justificar inversiones o recortes de presupuesto, determinar las prácticas que ya no contribuyen y son perjudiciales e identificar las que se han de potenciar.

8. Evitar la reincidencia de posibles fallos o errores.

9. Contribuir a conocer el estado de salud/calidad de vida del factor humano y descubrir las áreas problemáticas.

10. Ayudar a anticipar posibles problemas.

11. Detectar los costos sociales ocultos o excesivos.

12. Progresiva disminución de los costos.

13. Minimiza problemas actuales y futuros.

14. Identifica ahorros potenciales.

15. Racionaliza los recursos disponibles.

16. Conoce el estado de los equipos.

17. Evalúa la gestión de mantenimiento.

Los beneficios de una auditoría informática son inmediatos, ya que la organización trabajará sobre un sistema informático confiable que se verá reflejado en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso de mejora continua del personal hacia su área de trabajo.
- Compromiso con la política de calidad de la empresa, así como con la misión y visión.
- Mejora de la relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora los climas laborales.

En el mismo sentido algunos de los beneficios que se obtienen de un proyecto de auditoría interna:

- Permite determinar si los sistemas y procedimientos establecidos son efectivos para alcanzar los objetivos fijados y asegurar el cumplimiento de las políticas establecidas.
- Recomendaciones para el mejoramiento de las políticas, procedimientos, sistemas, etcétera.
- Suministra un medio de proveer un mayor grado de delegación de autoridad y si es necesario, un medio para facilitar la descentralización de las operaciones

El éxito de la auditoría interna depende no solo de la actitud de la dirección superior, sino también del grado de aceptación acordado por el equipo de trabajo de auditoría y por los niveles medio y bajo de la empresa.

CONCLUSIONES

La calidad es un factor que determinará la supervivencia de una empresa en el futuro inmediato, esta frase sin duda resumiría en gran medida la pretensión del presente trabajo. Y es que, hablar de calidad sigue siendo (desgraciadamente), un tema poco claro para la mayoría de las empresas mexicanas, cansadas de lidiar con tanta burocracia y con poco interés por parte del personal. Surge entonces un fenómeno sumamente curioso conocido como “la calidad fantasma”, donde el personal adopta una postura sumamente radical y busca una mayor remuneración por “aplicar un sistema de calidad”, desde luego esto es absurdo, ya que sería algo así como decir que una persona desea que “se le pague más por ser mejor hijo”, siendo que cada uno de nosotros deberíamos ser mejor día con día en todo lo que hacemos. De la misma forma, la calidad debe ser vista como una forma de superarse, de hacer mejor nuestro trabajo, de querer hacer las cosas bien y a la primera y sin errores, ahora podríamos preguntarnos ¿esto es posible?, claro que sí, para eso son los sistemas de gestión de la calidad y si aún esto no es argumento suficiente para convencer, basta con nombrar empresas mexicanas como *“bimbo”* o *“grupo modelo”*, ¿le suenan conocidas?, siempre se les relaciona con productos de muy buena calidad y que siempre son y saben iguales, ya sea que los compremos en la tienda de la esquina o en algún supermercado, no parece raro entonces, que si a esas empresas les ha funcionado la calidad, ¿no pueda funcionar dentro de su organización?. Muy bien, cierto que son grandes empresas y que tienen mucho capital y personal para hacer las cosas, pero de nada les serviría, si no tuvieran una cultura de calidad muy alta, donde cada persona sabe la importancia de su trabajo y de lo que hace, así como del compromiso que significa trabajar en una empresa de esta índole. Por ello, esas empresas han llegado hasta donde están, ahí es cuando uno se da cuenta de la importancia y la relevancia del papel que juega la calidad hoy día, así como de los beneficios tanto económicos como sociales que pueden tener dentro de una empresa que sigue un sistema de gestión de la calidad.

En el presente trabajo, abordamos una problemática similar, basándonos en la premisa de que todas las actividades deberían estar documentadas por el personal, y se seleccionó la implementación de una red de computadoras, ya que uno de los propósitos de la

computación es lograr la comunicación de datos, y que mejor manera que mediante una red de computadoras. Esta propuesta surgió a raíz de lo abordado en el curso “Redes de Computadoras”, donde como proyecto final se nos pidió elaborar una cotización de la implantación de una red, en ese entonces recopilamos mucha información para lograr una cotización adecuada, y todo el trabajo fue basado en la experiencia de cada uno de los integrantes del proyecto, esto es muy similar a la forma en que se trabaja en las empresas, unos proponen algo, los otros dicen sí o no, y finalmente se realizan las compras o se posponen para tiempos mejores.

Tiempo después en el curso de “Calidad”, nos dimos cuenta que estábamos abordando el trabajo desde la perspectiva errónea, hubiera sido más fácil establecer por escrito las características de los equipos y cada quien hiciera propuestas de cotizaciones, entendiendo que cualquier cotización que no cumpliera con las características no sería tomada en cuenta. Con ello nos hubiéramos evitado reunirnos semanalmente para discutir si la información era correcta o no; en las empresas este acto de volver a hacer las cosas se le conoce con el nombre de “reproceso” y muchas veces representa pérdidas de capital para la empresa. Afortunadamente en nuestro proyecto solamente lo que se perdía era tiempo, aunque si nos estuvieran pagando, hubiera representado una cantidad considerable de dinero para la empresa. Es triste, pero muchas organizaciones no se dan cuenta de esto, hasta que las pérdidas comienzan a ser considerables y por lo general tratan de arreglar el barco cuando se encuentra al borde del hundimiento, y no cuando apenas presentaba las primeras imperfecciones. Después comienzan a buscar al personal responsable de esto, y por lo general terminan por despedir al que se deje, pensando que con ello el problema ha sido erradicado y que pronto se recuperará el rumbo, cometiendo con ello un gran error, ya que empezará a generar temor y desconfianza en el personal que labora, en vez de generar soluciones y acciones correctivas que puedan sacar adelante la nave.

Lo mismo pasa en el área de redes de cómputo, nos referimos a que muchas veces el equipo se compra en base a lo que aprueba el jefe, haciendo de lado si el equipo es caro y/o funcional, a él lo que le interesa es que el servicio se preste acomodé lugar. No sería

más fácil si se contara con manuales donde se nos responda preguntas tales como: ¿cuántas cotizaciones se deben hacer y cómo?, ¿quién es el personal responsable?, ¿qué características debe tener el equipo?, entre otras más, aquí es donde entra nuestra propuesta.

Sobre el establecimiento de los conceptos básicos.

Sin duda, algo contra lo que nos hemos topado es que la mayoría de las personas que quieren implementar un sistema de calidad, no están familiarizados con la terminología que se usa, mucho menos si hablamos de conceptos tales como normas, políticas o procedimientos, por ello, se hace necesario que el personal sea sensibilizado sobre el empleo de éstos conceptos, que los entienda y los comprenda, con la finalidad de que más adelante los pueda abordar desde el punto de vista adecuado. La sensibilización del personal es una etapa muy importante para el trabajo que se va a realizar, es la columna vertebral de todo sistema basado en la calidad, y es el punto de partida para el compromiso del personal para con su trabajo, si en esta etapa se logra convencer al personal de los beneficios de los sistemas de calidad, se creará una cultura de la calidad, que poco tiempo después empezará a ser permeada a todo el personal, y facilitará la implementación de este sistema en los demás lugares que se deseé.

Con un adecuado liderazgo, la empresa debe ser capaz de superar esta etapa sin contratiempo alguno. La empresa debe refrendar el compromiso con sus clientes y para ello, la alta dirección debe satisfacer sus necesidades, ofreciéndole productos con una mayor calidad cada vez, sin olvidar el sentido humano de hacer las cosas.

Sobre el trabajo a realizar, redes de computadoras.

No solamente aspectos de calidad son necesarios para implementar un sistema de gestión, sino también aquellos relacionados con el aspecto técnico, en este caso redes de computadoras. El personal involucrado dentro de este ramo, debe establecer comunicación eficaz con la alta dirección con el fin de emitir sugerencias y reclamos en las decisiones tomadas. Siendo que se desea instalar redes de computadoras, lo natural sería

contratar personal experto en esta área o si se cuenta con él, involucrarlo en la toma de decisiones dentro del sistema.

La alta dirección no podría equipararse en el grado de conocimiento que el personal especializado tiene sobre la materia, además de que estos últimos mejor que nadie, deberían conocer el trabajo que hacen. Aquí, la responsabilidad de la alta dirección es mantenerse informada con grado de conocimiento básico en cuanto al trabajo a desarrollar (en este caso redes de computadoras), ya que finalmente ellos son los que deben aprobar o desaprobar una decisión. En este trabajo, en el capítulo 2 se presentó un panorama suficientemente claro de lo que son las redes de computadoras, y que puede servir para la elaboración de un manual de referencia para la alta dirección.

Sobre la normatividad existente en el trabajo a realizar.

La siguiente tarea fue buscar la normatividad adecuada para nuestro trabajo, por ejemplo, si lo que hacemos es instalar redes de computadoras, podríamos empezar buscando en lo establecido por la IEEE o incluso por la misma ISO; otro ejemplo podría ser si nuestra empresa se dedica a realizar pruebas de laboratorio a aparatos electrodomésticos, entonces podríamos pensar en las normas ANCE en fin, ejemplos hay muchos, lo verdaderamente importante es que la alta dirección adquiera el liderazgo de comprometerse no solamente a normalizar su trabajo, sino también, de poder competir contra empresas nacionales o internacionales. Esta es la gran ventaja de normalizar su trabajo bajo normas reconocidas a nivel mundial. El apego a estándares nacionales y/o internacionales nos garantizará que el trabajo que estemos realizando es competitivo tanto a nivel nacional e internacional. Y no solamente eso, sino también será una ventaja, un valor añadido con respecto a nuestros propios competidores, más ahora que la tendencia mundial de las grandes empresas, es contratar otras que al menos se encuentren certificadas bajo una normatividad que ellos necesiten.

Sobre la implantación de políticas, normas y procedimientos dentro de la organización.

Una vez establecida la normatividad bajo la cual se desea trabajar, el siguiente paso es ocuparse para la implantación de ésta. Realizar una serie de normas, políticas y procedimientos, alinearlas bajo los estándares establecidos por la alta dirección y comenzar la etapa de introducción del sistema en el área o departamento deseado. En el presente documento se plantearon una serie de normas, políticas y procedimientos, pensados en la instalación de una red de computadoras, con el propósito de mostrar que no es difícil la elaboración de éstos si se conoce el trabajo que se debe hacer. El personal debe estar conciente de esto y aportar sus comentarios y sugerencias acerca de la redacción de cada uno de ellos.

La valía de contar con un marco normativo adecuado, es que nos va a permitir mantener todo el proceso bajo control, bajo estándares de calidad, haciendo posible la identificación de alguna no conformidad que se haya detectado dentro del sistema. Claro, siempre y cuando se haga valer la autoridad de las políticas, normas y procedimientos. Por ello, la alta dirección debe concentrar una parte de sus esfuerzos en hacer cumplir su normatividad.

Sobre la evaluación del sistema de calidad, las auditorias.

Las auditorias son un método eficaz de conocer las fortalezas y debilidades de nuestro sistema de calidad, más aún, las auditorias informáticas nos van a permitir conocer mejor nuestra red de datos, los lugares donde puede ser mejorada y dónde se necesita de una mayor atención. Este instrumento de trabajo además nos va a permitir contar con evidencia objetiva de que lo que planeamos, es decir, lo que se encuentra escrito, se lleva a cabo tal cual, y si no es así, corregir de inmediato esas no conformidades. Cabe resaltar que las auditorias, no son ni deben ser un instrumento para amedrentar al personal, de que si no hace su trabajo como debiera, se le va a castigar. Por el contrario, nos van a decir las oportunidades de mejora, o dicho de otro modo dónde es posible de perfeccionar lo que se hace. Esta etapa del sistema de calidad, es sumamente benéfica a la empresa,

ya que desde que se empieza a implantar, se conoce dónde se puede mejorar, y de ahí comenzar un circulo virtuoso de mejora continua en el trabajo.

Finalmente, todo el proceso de desarrollo e implementación de una red de computadoras, aplicando la calidad, queda a consideración de usted amable lector, que nos ha acompañado a lo largo de esta propuesta, esperamos que pueda servirle como guía en la implementación de su sistema.

Por su atención

Gracias

Atte. Los autores

Apéndices

A. Diagrama de cable de par trenzado UTP y fabricación con conectores RJ45.

B. Propuesta de formato de apertura de cuenta.

C. Metodología para la elaboración de manuales.

D. Lineamientos para la integración de documentos.

E. Preparativos para recibir una auditoría.

APÉNDICE A

DIAGRAMA DE CABLE DE PAR TRENZADO UTP Y FABRICACIÓN CON CONECTOR RJ45

La especificación IEEE para Ethernet 10 Base T requiere usar **solo dos pares trenzados**, un par es conectado a los pines 1 y 2, y el segundo par a los pines 3 y 6. Si, así es, los pines 4 y 5 son saltados y son conectados a uno de los restantes pares trenzados.

Par #1:	**Blanco/Azul Azul**
Par #2:	**Blanco/Naranja Naranja**
Par #3:	**Blanco/Verde Verde**
Par #4:	**Blanco/Café Café**

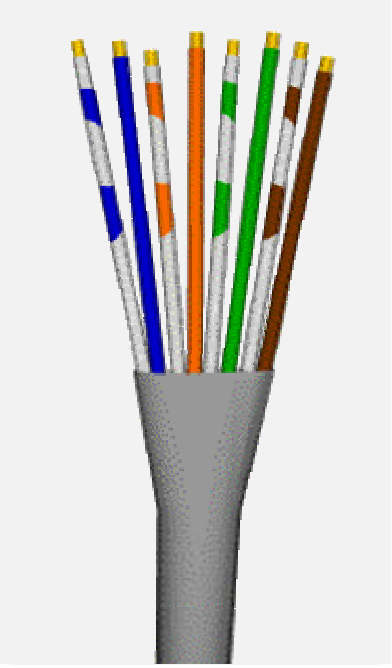


Figura A.1 Diagrama de pares de cable de par trenzado UTP

De acuerdo con la **Norma EIA/TIA 568B RJ45**:

El Par #2 (blanco/naranja, naranja) y el Par #3 (blanco/verde, verde) son los únicos usados para datos en 10 Base T.

Par # 2 conectado a pin 1 y 2:	
Pin 1 color:	**blanco/naranja**
Pin 2 color:	**naranja**
Par # 3 conectado a pin 3 y 6:	
Pin 3 color:	**blanco/verde**
Pin 6 color:	**verde**

Tabla A.1 Conexión de pares de acuerdo a la norma EIA/TIA 568B

Los 2 pares trenzados restantes se conectan como sigue:

Par # 1	
Pin 4 color:	**azul**
Pin 5 color:	**Blanco/azul**
Par # 4	
Pin 7 color:	**Blanco/café**
Pin 8 color:	**Café**

Tabla A.2 Continuación de conexión de pares de acuerdo a la norma EIA/TIA 568B

Para que no haya confusiones aquí esta el ejemplo gráfico de la **Norma 568B EIA/TIA**

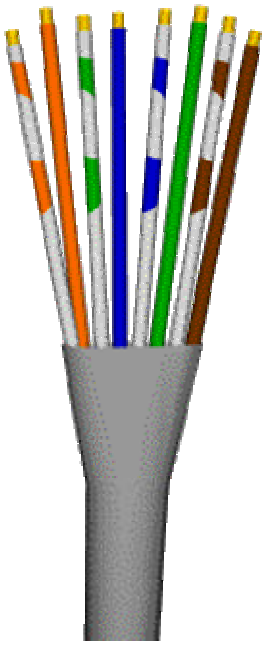


Figura A.2 Cable de par trenzado UTP ordenado de acuerdo a la norma EIA/TIA 568B

Ya ordenados, los cables deben juntarse y cortar las puntas, para que esten todas al mismo nivel y no haya problemas al insertalos en el conector RJ45. Los pares juntados y nivelados deben verse asi:

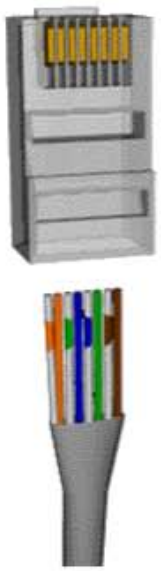


Figura A.3 Cable UTP ordenado y cortado, listo para ser ponchado

Asegúrese que todas las puntas lleguen hasta el tope del canal dentro del conector. Una vez insertados será necesario "poncharlos" con las pinzas adecuadas. No es necesario "pelar" el cable antes de insertarlo, las laminas en el conector perforarán el recubrimiento de los cables. Además, un seguro, en la parte posterior del conector "sujetará" el cable para evitar que se deslice hacia afuera. Ya "ponchado", el conector y el cable se verá así:

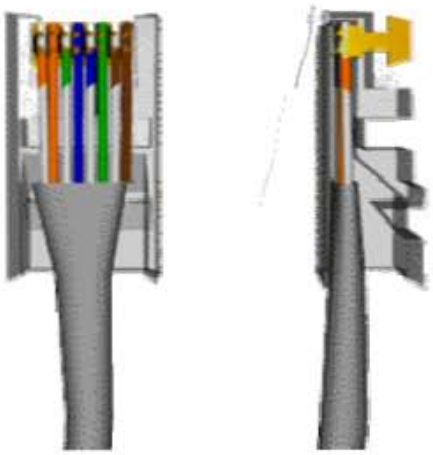


Figura A.4 Vista frontal y transversal del cable UTP ponchado

Si se va a usar un concentrador, las dos puntas del cable (la que se conecta al concentrador y la que se conecta a la tarjeta de red en la computadora) deberán poncharse usando la misma norma.

Para hacer un cable cruzado usaremos otro orden conocido como la norma 568A. Una de las normas se aplicará en una de las puntas del cable y la otra en la otra punta, no importa que norma se conecte en cada computadora ¡solo son dos computadoras! .

Las dos puntas se verán asi:

De un lado:	**Del otro lado:**
Punta Estandar 568B	**Punta Cruzada 568A (Crossover)**
Pin 1 Blanco/Naranja	Pin 1 Blanco/Verde
Pin 2 Naranja	Pin 2 Verde
Pin 3 Blanco/Verde	Pin 3 Blanco/Naranaja
Pin 4 Azul	Pin 4 Azul
Pin 5 Blanco/Azul	Pin 5 Blanco/Azul
Pin 6 Verde	Pin 6 Naranaja
Pin 7 Blanco/Café	Pin 7 Blanco/Café
Pin 8 Café	Pin 8 Café

Este es el orden correcto de los pines y pares de color para la punta cruzada

Par # 2 conectado a pins 1 y 2:	
Pin 1 color:	**blanco/verde**
Pin 2 color:	**verde**
Par # 3 conectado a pins 3 y 6:	
Pin 3 color:	**blanco/naranja**
Pin 6 color:	**naranja**

Tabla A.2 Conexión de punta cruzada bajo la norma EIA/TIA 568A

Una vez más, para evitar las confusiones:

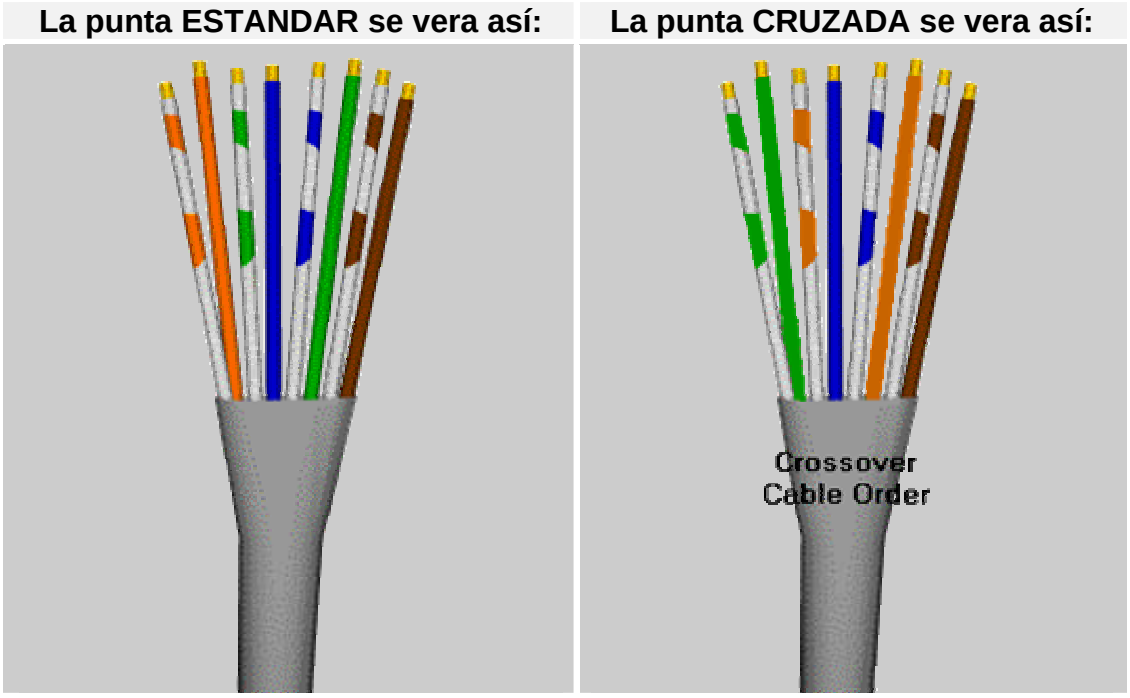


Figura A.5 Diagrama de cable crossover, bajo la norma EIA/TIA 568A

Cuando los pares estén insertados en el conector RJ45 deben verse así:

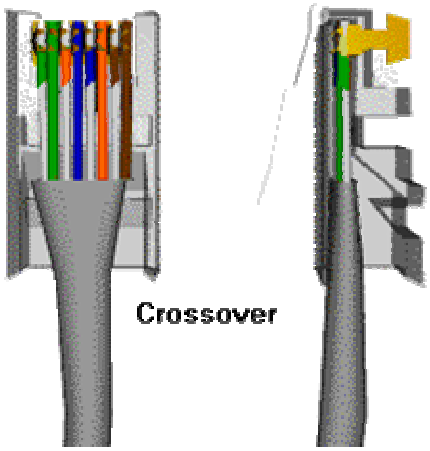


Figura A.6 Vista frontal y transversal del cable de punta cruzada bajo la norma EIA/TIA 568A

NOTA:

Es muy importante recordar que cuando se conectan computadoras en red no solo se les está conectando físicamente, sino que también se las está conectado eléctricamente. Una descarga de voltaje puede dañar una o varias maquinas. Es por esto que es de vital importancia aplicar una buena tierra física a la instalación eléctrica y así evitar sorpresas desagradables.

APÉNDICE B

FORMATO DE APERTURA DE CUENTA

Logo de la institución.

(Clave del formato)

Apertura de Cuenta

Fecha: ___/___/_____

Nombre del solicitante:_____
Institución:_____

División:_____
Departamento:_____

Proyecto:_____
Responsable:_____

Usuario (login):_____
Clave de usuario (password):_____
Clase de usuario:_____
Extensión telefónica:_____

¿Se compromete a obedecer el reglamento de uso de la red?

SI: ❍ **NO**:❍

NOTA: Llene todos los campos de la forma; si la información es insuficiente, no será procesada.

APÉNDICE C

METODOLOGÍA PARA LA ELABORACIÓN DE MANUALES

La elaboración de manuales es sin duda una tarea exhaustiva y minuciosa, que requiere de una metodología mínima necesaria, que pueda conducirnos en el menor tiempo posible a su elaboración, es por ello que se vuelve fundamental este punto y cobra mayor relevancia en el presente trabajo. En las siguientes hojas el lector encontrará una propuesta de dicha metodología, desde una perspectiva generalizada, que puede servirle de guía para la elaboración de una propia, o bien adoptarla para el desarrollo de sus manuales.

Nuestra propuesta consiste en ocho puntos esenciales.

1.- Planeación del estudio.

Uno de los puntos fundamentales para asegurar la integración de documentos es algo que llamaremos *planeación del estudio*, y que consiste en la programación de las acciones pertinentes, es decir, el diseño de programas de trabajo donde se consignen los requerimientos, fases y procedimientos que fundamenten su ejecución. Se debe determinar al responsable de la conducción del trabajo en la entidad administrativa que se trate, o en su caso, definir el servicio profesional externo con quién se trabajará, con el propósito de establecer estándares en cuanto al contenido y presentación de los manuales a desarrollar.

2.- Recopilación de los datos.

Consiste en recabar documentos y datos de forma general con el fin de organizarlos y analizarlos en fases posteriores.
Para recabar la información, se hace necesario recurrir a distintas fuentes tales como:

- Archivos de la organización (manuales existentes, boletines, oficios, formatos entre otros).
- Funcionarios y empleados.
- Observación directa.
- Entrevistas.
- Cuestionarios.

3.- Análisis de la información.

Una vez recopilada toda la información concerniente a la entidad, se procede al análisis de la información, la cual constituye una fase muy importante para la elaboración de manuales.

Es necesario asegurarse que los datos obtenidos sean relevantes, precisos y representativos de la situación que se vive actualmente en la entidad, de la misma forma

la información proveniente de las entrevistas debe ser cuidadosamente validada en el momento mismo en que son llevadas a cabo, juzgando la veracidad de las respuestas a través de la observación directa. Lo anterior, garantiza que el personal coopere proponiendo sugerencias.

4.- Registro de información.

Cuando se tiene la información ya "filtrada", se hace necesario documentarla, para ello, se usan documentos tales como:

- Formatos de descripción y registro de actividades.
- Organigramas.
- Descripción de puestos.
- Procedimientos.
- Diagramas de flujo.
- Manuales.

Esto nos permitirá organizar la información, de forma que pueda ser fácil de leer y entender por todo el personal que labora en la organización.

5.- Validación y autorización de la documentación.

Para que todo documento adquiera validez legal, el área responsable deberá remitirlo a las instancias correspondientes para su validación y autorización. Una vez aprobado, se diseñará en definitiva el formato, tomando en cuenta que debe ser redactado usando un leguaje claro y sencillo, que permita un fácil entendimiento por parte de todo el personal.

6.- Presentación y reproducción del proyecto final.

En este punto se definen aspectos tales como el tipo de impresión, material, formato y número de ejemplares a reproducir. Algunas recomendaciones son:

- Unificar la redacción del manual con objeto de mantener la unidad.
- Utilizar formatos de hojas intercambiables, a fin de facilitar su revisión y actualización.
- Utilizar el método de reproducción en una sola cara de las hojas.
- Procurar que las secciones o capítulos del manual queden separadas por divisiones, las cuales presenten pestañas impresas con el nombre de cada sección.
- Seguir las políticas, normas y procedimientos de las publicaciones oficiales en el momento de su impresión y distribución.

7.- Distribución e implantación.

Una vez editado el manual, su distribución quedará a cargo del responsable de la unidad de sistemas y procedimientos o de un órgano particular (por ejemplo el comisionado de

calidad de la organización), y deberá llevarse un registro de los poseedores de los manuales.

El método de implantación se definirá en base a las necesidades específicas del área, haciendo uso del método instantáneo, piloto, paralelo, combinado.

8.- Revisión y actualización.

La mayoría de las veces la necesidad de revisar y actualizar los manuales surge al modificarse las tareas al interior de los órganos administrativos. En ese sentido, los responsables de las diferentes áreas deberán informar oportunamente a los responsables de elaborar los manuales, sobre algún posible cambio en torno a las actividades o responsables de proporcionar algún servicio. Deberá seguir el procedimiento de revisión y actualización de la empresa, con objeto de que se realicen las adecuaciones correspondientes.

Recomendaciones para que la elaboración de manuales sea una práctica común.

1.- Que los empresarios y directivos reconozcan la importancia de usar manuales dentro de la organización.

¿Cómo?

Conociendo de las organizaciones certificadas bajo la norma ISO 9001:2000 los beneficios y ventajas que trae consigo el contar con una documentación adecuada.

2.- Que la alta dirección apoye y facilite su elaboración.

¿Cómo?

Capacitando a sus colaboradores y definiendo la elaboración de la documentación de los procesos como parte de los objetivos de la empresa.

3.- Que la alta dirección apruebe el trabajo en equipo.

¿Cómo?

Permitiendo que los involucrados en los diferentes procedimientos se reúnan periódicamente para su elaboración, revisión, aprobación y difusión.

Debido a que el ser humano es un ser social por naturaleza, con una tendencia a organizar y administrar sus asuntos, la elaboración de manuales puede facilitarle a la organización el cumplimiento de sus propósitos y objetivos de manera efectiva y ordenada.

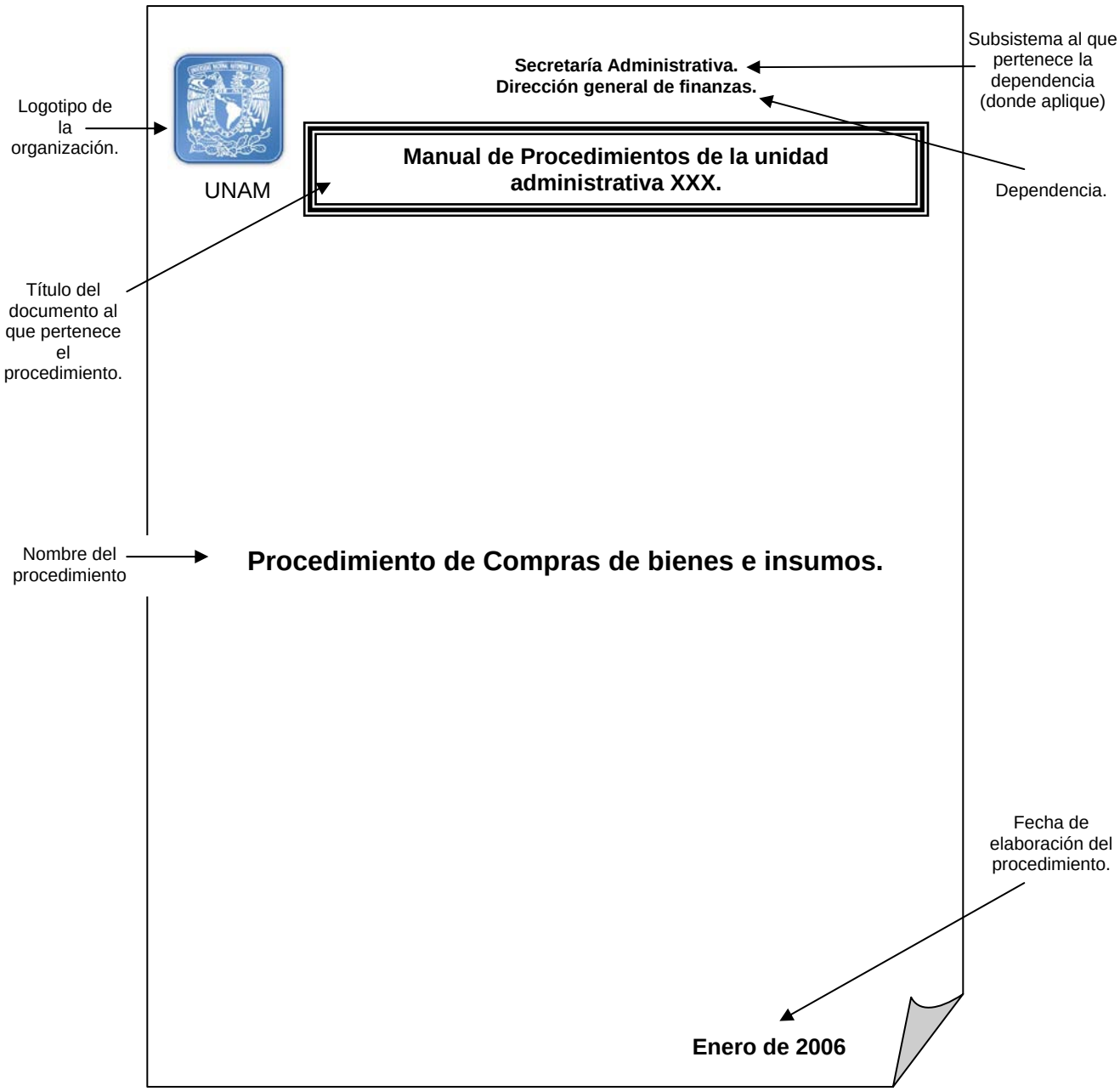
APÉNDICE D

LINEAMIENTOS PARA LA INTEGRACIÓN DE DOCUMENTOS

En este apartado describiremos los diferentes elementos que debe contener cada procedimiento que se elabore o actualice antes de la integración de los manuales.

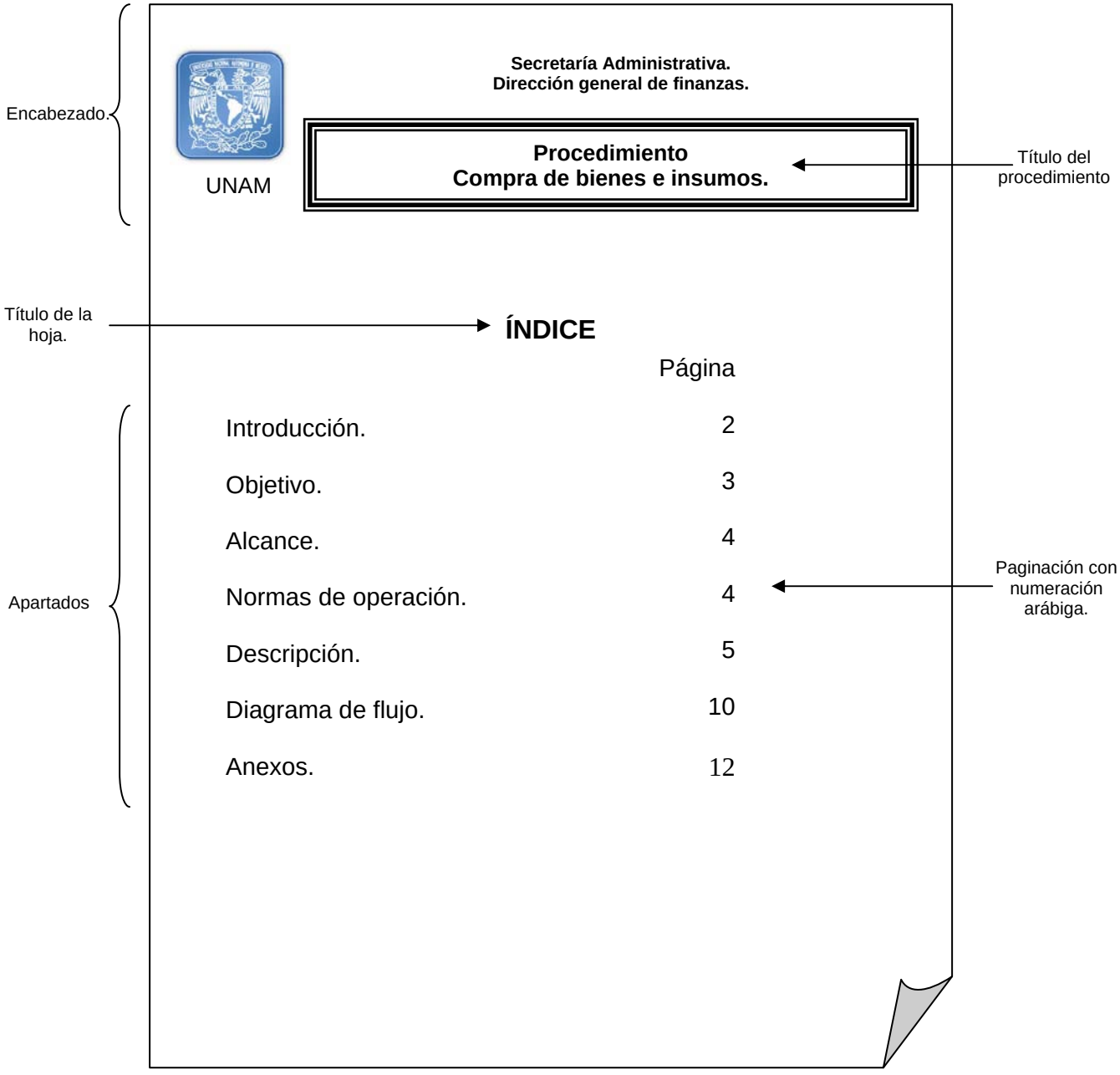
Carátula del procedimiento.

Es la primera hoja del procedimiento, cuyo fin es identificarlo plenamente. Por ejemplo:



Índice del procedimiento.

Esta parte tiene como finalidad relacionar de forma secuencial los rubros que integran al documento, con su respectiva paginación para facilitar su localización.
Por ejemplo:

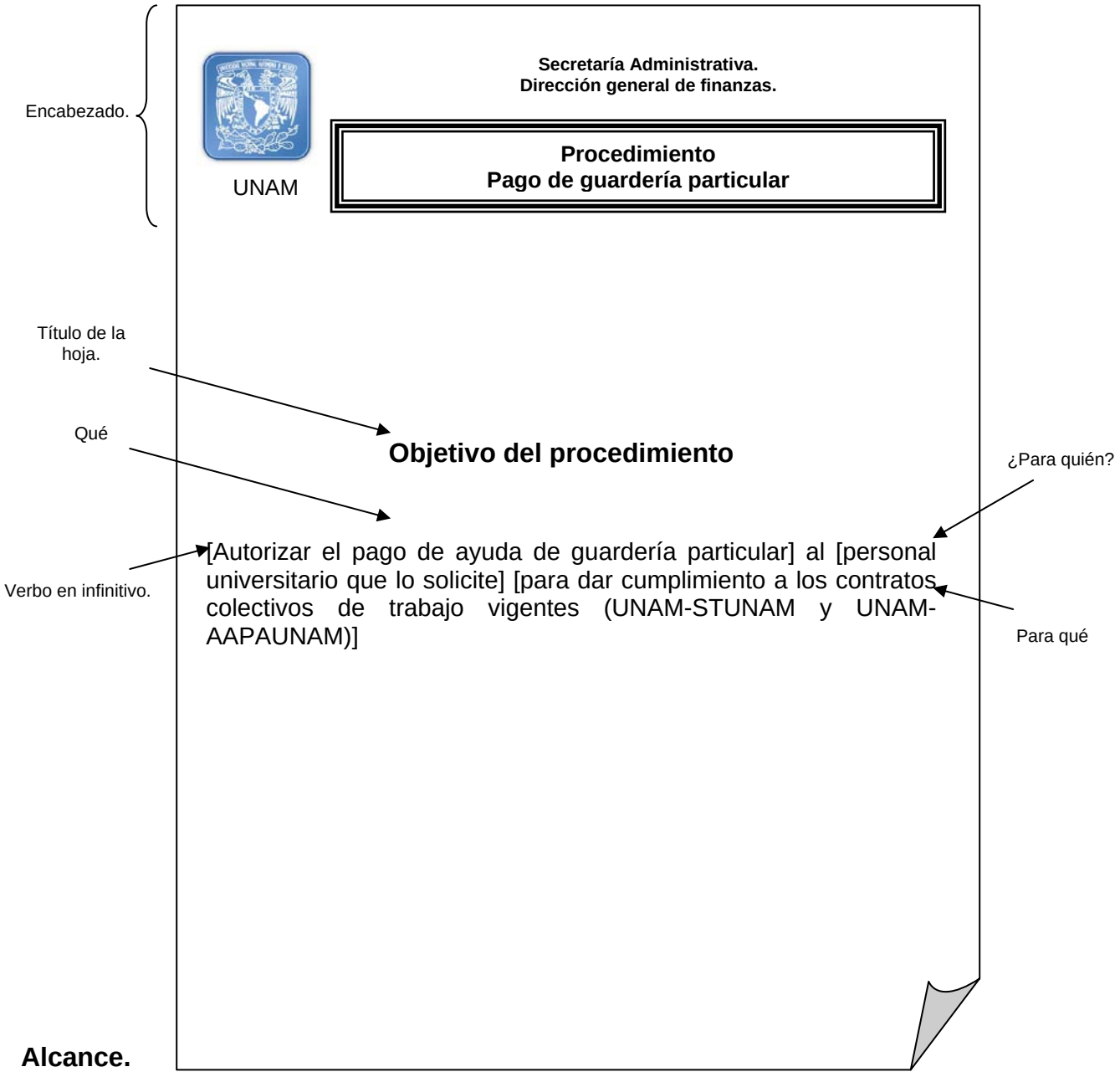


Objetivo del procedimiento.

El objetivo debe expresar claramente los resultados que se pretenden obtener al llevarse a cabo las actividades que integran cada procedimiento. Para ello se pueden seguir las siguientes recomendaciones para su redacción:

- Iniciar con un verbo en tiempo infinito.
- Especificar con claridad qué, para qué y para quienes se ha elaborado el procedimiento.
- Evitar el uso de adjetivos calificativos.
- No subrayar conceptos.
- Utilizar una redacción clara, precisa.

Por ejemplo:

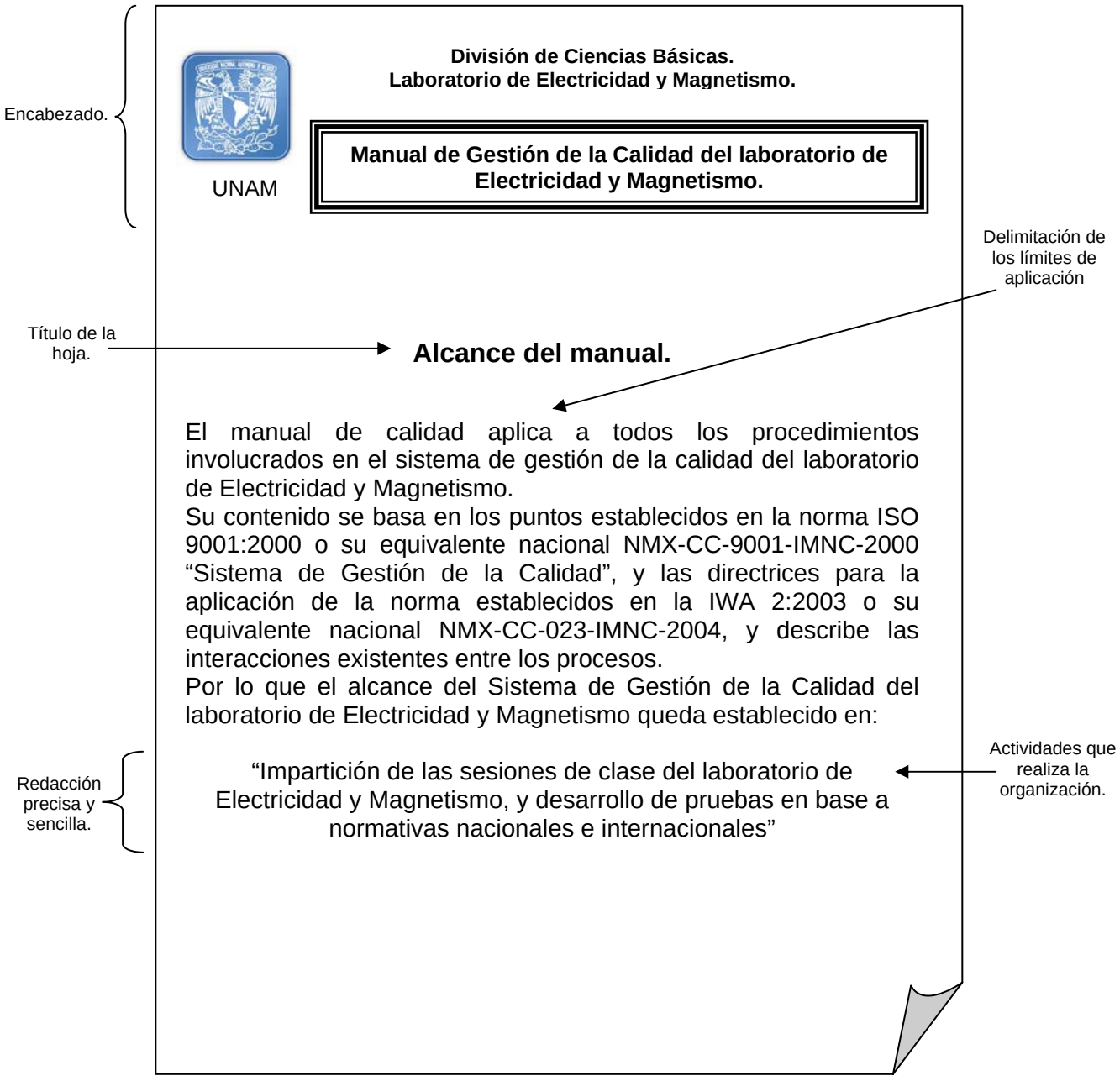


Alcance.

Se delimitan las fronteras de aplicación del procedimiento al cual se refiere el documento y se describe su campo de acción, es decir a qué proceso, servicio, documento o área es aplicable. Algunas recomendaciones para su redacción son:

- Debe ser realizable por la empresa, es decir, no es un estado deseado, sino un estado actual.
- Debe establecer claramente y sin lugar a dudas, los límites de la aplicación del documento.
- Debe mostrar la esencia de las actividades del procedimiento.

Por ejemplo:

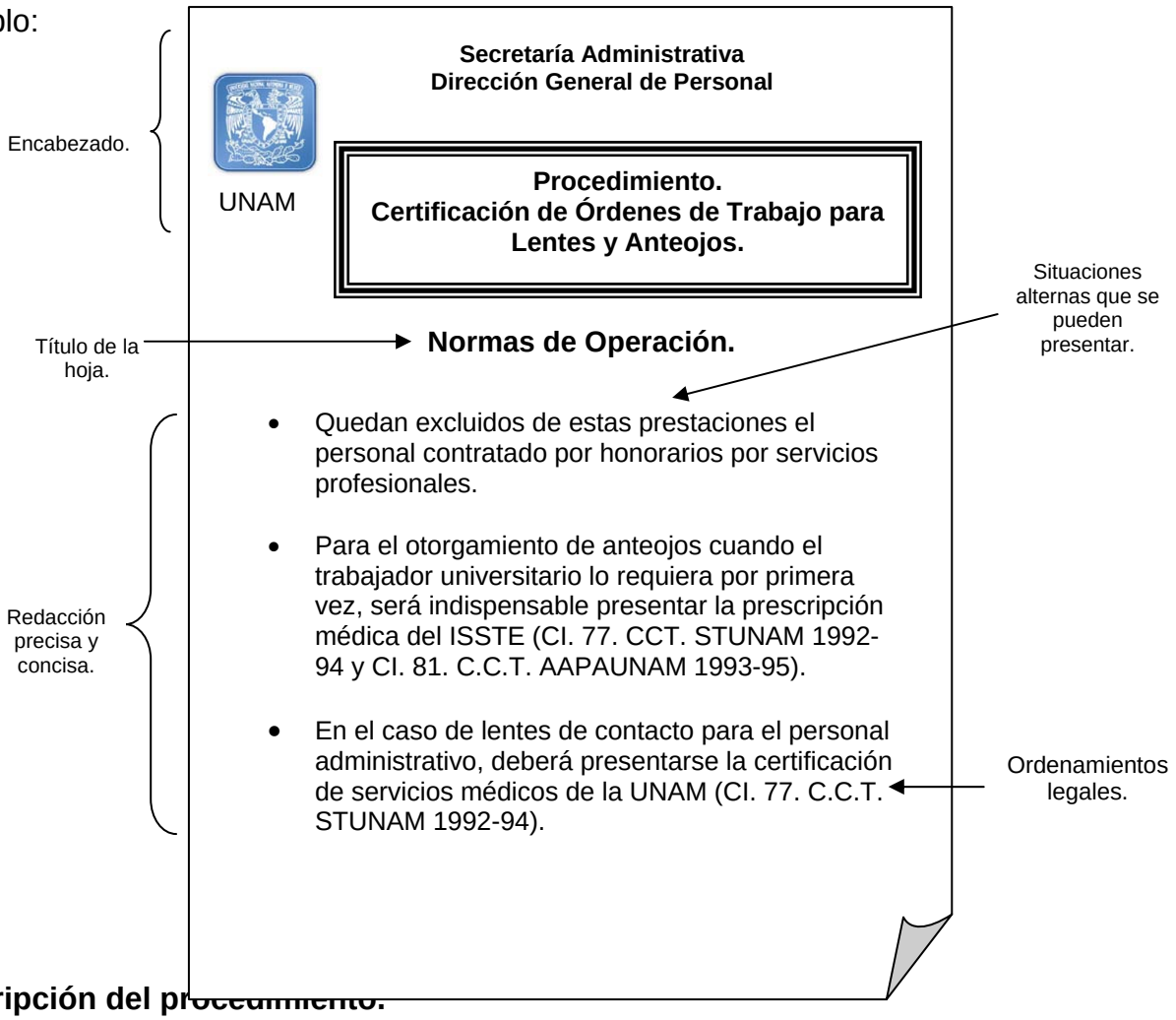


Normas de operación.

Cada procedimiento documentado deberá incluir todos los lineamientos que regulen la actuación del personal asignado a la ejecución de las tareas, aquí se deberán anotar todas aquellas normas y políticas de la empresa así como referencias a otros procedimientos si es necesario. Algunas recomendaciones para elaborar normas pueden incluir las siguientes:

- Deben comprender todas las situaciones alternativas que pudieran presentarse en la ejecución del procedimiento.
- Deben ser redactadas claramente con el fin de que sean comprendidas por el usuario, e incluso por quienes no estén familiarizados con el procedimiento.
- Debe establecer claramente la responsabilidad del personal a efecto de evitar desviaciones en la ejecución del procedimiento.
- Deben redactarse en tiempo futuro o presente, prefiriéndose el primero.
- Deben ser precisas, concisas y claras para evitar interpretaciones equivocadas.
- En caso de que alguna norma se sujete a ordenamientos legales se deberá hacer referencia al marco jurídico que la sustenta (leyes, reglamentos, acuerdos, circulares, oficios.)

Ejemplo:



Descripción del procedimiento:

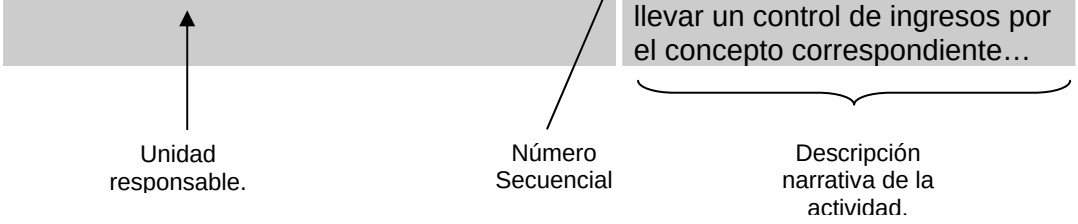
Como su nombre lo indica, es la explicación escrita, en forma lógica y secuencial de cada una de las actividades que realiza la organización responsable para efectuar un trabajo determinado.

Los procedimientos pueden ser estructurados en dos formas: libreto o bloque.

Libreto.
La descripción se realiza mediante tres columnas: en la primera se indica la unidad responsable, en la segunda el número consecutivo de la actividad y en la tercera la descripción de la actividad a desarrollar.

Por ejemplo:

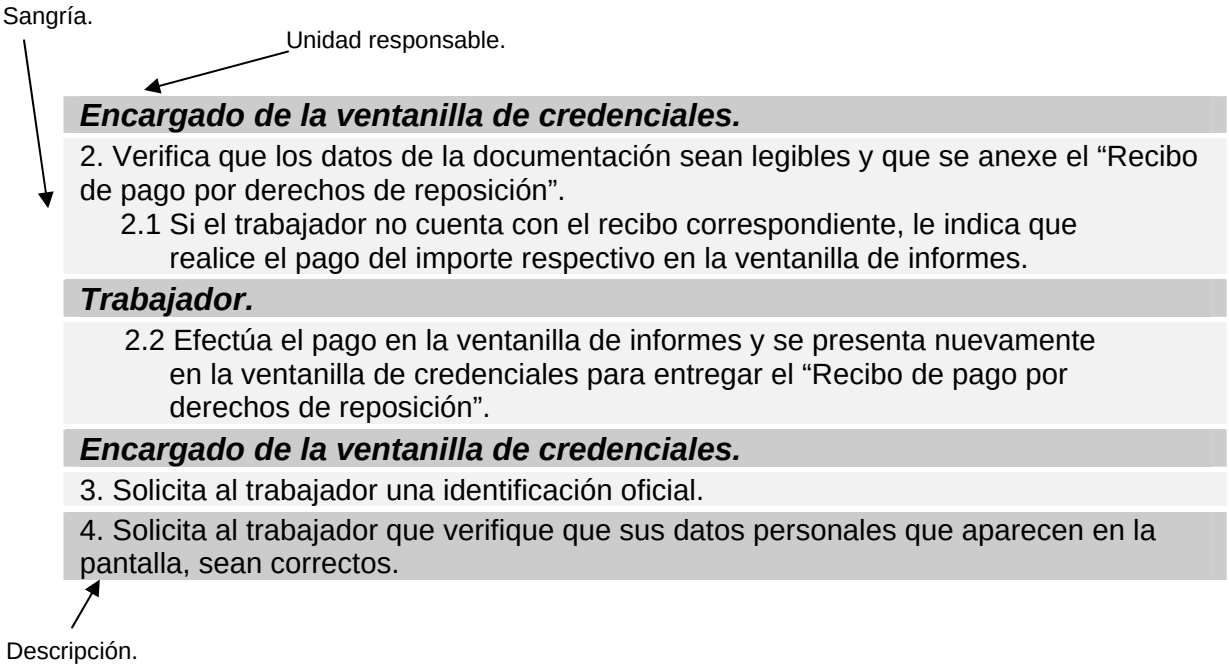
Procedimiento: Reexpedición de credenciales al personal	
Responsable	**Actividad**
Encargado de la ventanilla de credenciales	2. Verifica que los datos de la documentación sean legibles, que el “Recibo de pago” corresponda a la última quincena de pago y que se anexe el “Recibo de pago por derechos de reposición”. 2.1 Si la documentación no está completa, indica al usuario que el trámite no procede.
Trabajador	2.2 Efectúa el pago en la ventanilla de informes y se presenta nuevamente en la ventanilla de credenciales para entregar el “Recibo de pago por derechos de reposición”.
Encargado de la ventanilla de credenciales	3. Archiva temporalmente el “Recibo de pago” para efecto de llevar un control de ingresos por el concepto correspondiente…



Bloque.

En una sola columna se describe el procedimiento, identificando cada actividad con numeración progresiva y con sangrías aquellas actividades que son de excepción, desviaciones o subactividades; las responsabilidades se deben indicar en un subtítulo.

Por ejemplo:



Algunas recomendaciones para la redacción y presentación de los procedimientos.

a) Cada actividad deberá comenzar con un verbo en tercera persona del singular en tiempo presente. Cuando se redacten actividades que no forman parte de la secuencia principal del procedimiento y que se puedan referir como opciones, desviaciones o subactividades, se usan términos tales como: “si”, “cuando”, “en caso”.
b) La redacción de cada actividad deberá ser clara, concisa y precisa: responder siempre a preguntas tales como: ¿Qué, cómo y con qué se realiza una actividad?, y si es necesario también se recomienda preguntar; ¿a quién se canaliza el trabajo? y ¿para qué?.
c) Deberán numerarse las distintas actividades del procedimiento en forma progresiva con números arábigos enteros.
d) En los casos que a una actividad le prosigan otras (de excepción), que no forman parte de la secuencia principal del procedimiento, éstas deberán numerarse con fracciones decimales a partir de la actividad de la cual se desprenden.
e) Se procurará que cada una de las actividades del procedimiento contenga sólo una acción, aunque en algunos casos se justifica que contenga dos.
f) En caso de existir actividades que por su naturaleza se realicen simultáneamente, en una forma casi inmediata o se consideren de poca importancia, éstas se redactarán en un solo párrafo.

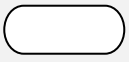
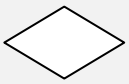
g) En las actividades que se realizan con una frecuencia establecida, se deberá indicar la periodicidad en un renglón antes de iniciar el párrafo de la actividad.
h) Cuando la participación de una unidad responsable se limita a una sola intervención, para efectos prácticos, esa actividad se redactará como si fuera una nota.
i) Al describir las actividades de un procedimiento, se anotará el nombre completo de la unidad responsable cuando haga su primera aparición en el mismo; posteriormente se podrá utilizar un nombre más corto.
j) Cuando una actividad implique la utilización de algún formato, y éste haga su primera aparición en el procedimiento, se deberá anotar su nombre completo entre comillas.
k) Finalmente, algunos de los verbos más utilizados en la descripción narrativa de procedimientos son: llenar, requisitar, elaborar, enviar, entregar, turnar.

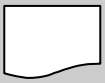
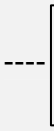
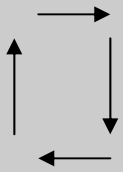
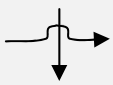
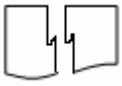
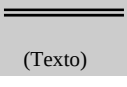
Diagramas de flujo.

Son la representación gráfica en que se realizan las actividades necesarias para desarrollar un trabajo determinado. La ventaja de llevar a cabo este tipo de diagramas son muchas, entre las que podemos mencionar:

- Explica a través de símbolos y textos cortos, las actividades que componen un procedimiento.
- Permite al personal identificar en forma rápida, la manera de realizar las actividades de forma eficaz.
- Facilita la comprensión de un procedimiento en cualquier nivel jerárquico.
- Facilita el análisis e interpretación de cada procedimiento, ya que muestra la secuencia de actividades y la distribución de los documentos.
- Permite analizar cada actividad por sí misma y su relación con las demás.
- Ahorra tiempo en la inducción de personal de recién ingreso.

Simbología.
Se usa la simbología establecida por la ANSI (American Nacional Standard Institute) con el fin de unificar la aplicación de los símbolos.

Símbolo	Nombre	Descripción
	Inicio, término o unidad responsable	Señala donde incida o termina un procedimiento. Además puede utilizarse para indicar el nombre de la unidad responsable de ejecutar ciertas actividades.
	Actividad	Representa la ejecución de una o más tareas de un procedimiento.
	Decisión	Indica las opciones que se pueden seguir en caso de que sea necesario tomar caminos alternativos.

Símbolo	Nombre	Descripción
	Conector	Mediante este símbolo se pueden unir dentro de la misma hoja, dos o más actividades separadas físicamente en el diagrama.
	Conector de página.	Similar al significado del símbolo anterior, sólo que éste se emplea cuando las actividades queden separadas en diferentes hojas.
	Archivo temporal.	Indica que se guarda un documento durante un periodo determinado.
	Archivo definitivo.	Indica que se guarda un documento permanentemente.
	Documento	Representa un documento, formato o cualquier escrito que se recibe, elabora o envía.
	Nota	Se utiliza para indicar comentarios o aclaraciones adicionales a una actividad y se puede conectar con cualquier símbolo del diagrama en el lugar donde la anotación sea significativa, Dentro de este símbolo se puede informar: - El nombre del procedimiento que antecede al que se describe, esto cuando el procedimiento se ha dividido en varios. - Tiempo necesario para realizar cierta(s) actividad(es). - La(s) actividad(es) genérica(s) realizada(s) por una instancia que esporádicamente intervenga en el procedimiento.
	Líneas de dirección.	Conecta símbolos, señalando la secuencia en que deben realizarse las actividades.
	Puente entre líneas de flujo.	Cuando en el diseño del diagrama existe la necesidad de pasar una línea de flujo sobre otra ya existente.*
	Documento opcional.	Representa un documento que dentro del procedimiento puede o no elaborarse, requerirse o utilizarse.*
	Documento destruido.	Indica la destrucción o eliminación de un documento, por no ser necesario.*
	Tiempo o interconexión.	Lapso que tarda una tercera instancia para realizar alguna actividad no relacionada con la unidad responsable en cuestión. También puede usarse

Símbolo	Nombre	Descripción
		para representar la conexión con otro procedimiento.

*Simbología no perteneciente a la ANSI.

APÉNDICE E

PREPARATIVOS PARA RECIBIR UNA AUDITORIA

Cuando una empresa está próxima a recibir una auditoria no sabe cómo debe comportarse, de ahí que por más bien que los empleados sepan su trabajo y lo hagan de la mejor manera, los nervios pueden llegar a traicionarlos y volver un verdadero dolor de cabeza esta actividad. En esta sección trataremos de hacer más ameno este proceso a través de una serie de recomendaciones.

Antes de la auditoria.

Con respecto al lugar.
Debemos asegurarnos que el equipo auditor sepa cómo llegar a su área, especialmente si vienen de otra, para esta actividad es muy recomendable que se le haya enviado a todos y cada uno de los auditores, una hoja con un mapa de localización de la empresa con referencias del lugar.

Con respecto al horario.
Es necesario confirmar la hora de llegada de los auditores, y comunicársela al personal, de forma que no haya sorpresas en su arribo y todo salga de acuerdo a lo planeado.

Estacionamiento.
Como cortesía para el grupo auditor, se recomienda reservar un lugar de estacionamiento para cada uno de ellos.

Acceso y listado de áreas.
Hacer un listado de las áreas que recorrerán los auditores, así como la estimación de la agenda de la auditoria y distribuirlo al personal aplicable.
La primera impresión cuenta mucho, de ahí que las áreas por donde transitarán los auditores deben encontrarse impecablemente limpias y en perfecto orden, la limpieza y el orden son factores que indirectamente los auditores toman mucho en cuenta al momento de tomar decisiones.

Acondicionamiento de una oficina.
Para poder llevar a cabo sus actividades de la forma más eficiente, los auditores van a necesitar de un aula u oficina privada para trabajar. Es necesario reservar un lugar donde puedan reunirse sin ser interrumpidos, procurando tener a su disposición un teléfono, una computadora y una fotocopiadora.

Documentación.
Tener listo para los auditores una copia controlada del manual de calidad y si es posible de los procedimientos. Otra actividad que se recomienda es la elaboración de folletos informativos de cada área auditada, esto servirá para entender mejor el sistema.

Cambios.
Si es necesario hacer un cambio de última hora, habrá que informarlo de inmediato a todo el personal involucrado.

Disponibilidad.
La alta dirección debe asegurarse por todos los medios posibles que todo el personal clave esté disponible en el momento de la auditoria. Lo anterior significa que debe pedirse a todos los posibles auditados, que no reciban llamadas telefónicas, recados ni existan interrupciones mientras el equipo auditor se encuentre en sus áreas.

Preparativos de comida.
Durante la auditoria el tiempo apremia y cada minuto debe ser aprovechado al máximo, por lo que no es conveniente que los auditores salgan a buscar comida. En lugar de ello se recomienda pedir al personal adecuado de la organización les reserve comida en algún lugar dentro del área. Platillos tales como pizza, hamburguesas, refrescos, etcétera, son muy recomendables.

Limpieza.
Es muy importante asegurarse que se efectúe la limpieza de los lugares comúnmente sucios, que puedan visitar los auditores, tales como accesos a oficinas, áreas operativas, planta, almacén y en especial los sanitarios.

Entrenamiento.
Se recomienda llevar a cabo con el personal sesiones de entrenamiento simulando una auditoria con ellos. Esta práctica servirá para dar confianza a los auditados y a nosotros mismos para darnos cuenta si efectivamente el personal conoce y aplica los procedimientos establecidos, para ello hay que asegurarnos de que todos tengan a la mano sus manuales y registros de calidad.
Un día antes de la auditoria, se recomienda pedir al personal que repase de nuevo sus procedimientos, sus políticas y sus objetivos.

Recorrido.
Un día antes de la auditoria se recomienda hacer un recorrido general con los auditores internos de la empresa, no debe haber ninguna no conformidad a la vista.

El día de la auditoría.

Temprano.
Estar presente en la junta de apertura, llegar 15 minutos antes de que de inicio. Se puede aprovechar este tiempo para aclarar dudas o para dar un repaso final con el personal auditado.

Arribo de los auditores.
Los auditores llegarán puntualmente. Será el representante de la dirección quien los reciba y lo lleve hacia la sala o cuarto donde será la junta de apertura.

Reunión de Apertura.
Con esta actividad se inicia la ejecución de la auditoría. El auditor líder abre y controla la reunión, asimismo, presenta a su grupo de auditores, solicitando acceso a la empresa de un guía, un aula y explicará el seguimiento a seguir.

Por su parte el representante de la dirección presentará un discurso de bienvenida en donde informa al auditor líder su disposición a ser auditados y agradece las no conformidades que se encuentre.

La auditoria.

Durante la auditoria, el objetivo de los auditores es verificar las correcciones a los hallazgos encontrados en la auditoria, el apego a las normas en las que la empresa solicitó la auditoria, así como sus procedimientos.
Su objetivo es buscar evidencias objetivas que demuestren que los procedimientos se están llevando a cabo de acuerdo a lo documentado.

Consejos al personal auditado.

- Trate de no estar nervioso, pensar en lo bien que ha realizado las actividades, esto le dará confianza y seguridad al momento de responder las preguntas de los auditores.
- Tener confianza, no hay que olvidar, que nadie sabe mejor su trabajo que usted mismo.
- Revisar antes las políticas, objetivos e instrucciones de trabajo.
- Ser honesto y no tratar de engañar al auditor, ya que solo mostrará una mala imagen de la empresa.
- No adivinar las respuestas, si no se sabe es mejor decir “no sé”.
- Contestar solo lo que se le pregunte.
- Ser agradable hasta hacer sentir confortable al auditor.

Junta de cierre.
Al terminar la auditoria se clausura formalmente con una junta de cierre que puede durar de 30 minutos a 1 hora. En la junta de cierre: asiste el representante de la dirección y se dan las conclusiones de la auditoria.

Todos los puntos anteriores corresponden a la ejecución de una auditoria, y pueden servir para preparar una si es que está próximo a recibirla, o simplemente planificarlo antes de que los tiempos se nos vengan encima.

Glosario de términos

GLOSARIO DE TÉRMINOS

Access point: Dispositivo que ejerce básicamente funciones de puente entre una red Ethernet con una red WiFi.

Acción correctiva: de acuerdo con la ISO 9000:2000, acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.

Acción preventiva: de acuerdo a ISO 9000:2000, es la acción tomada para eliminar la causa de una no conformidad potencial u otra situación parcialmente indeseable.

AENOR: siglas para Asociación Española de Normalización.

Alta dirección: de acuerdo a ISO 9000:2000, es la persona o grupo de personas que dirigen y controlan al más alto nivel de una organización.

AMAI: Asociación Mexicana de Auditores en Informática

ANSI: siglas para American National Standards Institute, Instituto Nacional Americano de Estandarización.

ARPANET: Advanced Research Projects Agency NETwork, Red Avanzada de Agencias para Proyectos de Investigación Red de Investigación.

Auditor: de acuerdo con ISO 9000:2000, es la persona con la competencia para llevar a cabo una auditoria.

Auditoria: de acuerdo a la ISO 9000:2000, es el proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente para determinar la extensión en que los criterios se cumplan.

Backbone: la palabra backbone se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.

Base band: banda- base, transmisión digital.

Bases de datos remotas: bases de datos que no se encuentran en el lugar de aplicación, aquellas que se pueden consultar a distancia.

Bit: es el acrónimo de Binary digit. (dígito binario). Un bit es un dígito del sistema de numeración binario. El equivalente español para este anglicismo es bitio.

BNC: British Naval Connector, conector para cable coaxial, utilizado típicamente para redes.

Broad band: banda ancha, transmisión analógica.

Broadcasting: distribución de señales de datos a un número de destinarios remotos.

Byte: voz inglesa que describe la unidad básica de almacenamiento de información, equivale a ocho bits. En español el equivalente para este anglicismo es octeto.

Calidad: propiedad o conjunto de propiedades inherentes a algo, que permiten apreciarla como igual, mejor o peor que las restantes de su especie. De acuerdo a la Norma Oficial Mexicana NMX-CC-9000-IMNC-2000, se define como el grado en el que un conjunto de características inherentes cumple con la necesidad o expectativa establecida generalmente implícita u obligatoria.

Cable coaxial: Cable formado por dos conductores concéntricos. El conductor central o núcleo está formado por un hilo sólido de cobre (llamado positivo o vivo), rodeado por una capa aislante (llamado dieléctrico) que lo separa del externo, formado por una malla trenzada de cobre o aluminio, este conductor produce un efecto de apantallamiento y además sirve como retorno de las corrientes.

Cheapernet: red tipo bus con cable coaxial delgado RG58, banda base y que puede transmitir a 10 Mbps a una distancia de 200m.

CSMA/CD: Carrier Sense Multiple Access / Collition detection, Acceso Múltiple con Escucha de Portadora y Detección de Colisiones.

Cliente: en comercio y marketing, un cliente es el que coloca el dinero para la compra de un producto o servicio; en el área de informática, cliente es una computadora que accede a recursos y servicios brindados por otro llamado servidor, generalmente en forma remota. En términos de calidad y de acuerdo a la definición de ISO 9000:2000, cliente es la organización o persona que recibe un producto.

DARPA: Defense Advanced Research Projects Agency – agencia de proyectos de investigación avanzada de defensa.

Dato: un dato es una representación simbólica (numérica, alfabética, etc.), de un atributo o característica de una entidad.

Datagramas: un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia la computadora receptora, de manera independiente a los fragmentos restantes.

Demonios: Se conoce como demonio (principalmente en entornos UNIX) al programa que ejecuta/lanza un servicio. Viene del término inglés daemon.

Demodulación: el término demodulación engloba el conjunto de técnicas utilizadas para recuperar la información transportada por una onda portadora, que en el extremo transmisor había sido modulada con dicha información. Este término es el opuesto a modulación.

Departamentos: son aquellos órganos que siguen inmediatamente a la dirección.

DQDB: Distributed Queue Dual Bus o bus dual de cola distribuida, estándar utilizado para la implantación de redes de área metropolitana (MAN).

Encriptación: es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.

Ethernet: nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de *ether*.

Evidencia objetiva: de acuerdo con ISO 9000:2000, son los datos que respaldan la existencia o veracidada de algo.

Fast Ethernet: ethernet de alta velocidad, la cual trabaja a 100 Mbps puede manejar cables como el UTP categoría 5 o la recién liberada GigaEthernet.

FC: Fiber Connector, conector cilíndrico para fibra óptica que se enrosca fácilmente.

Fibra óptica: es una guía de ondas en forma de filamento, generalmente de vidrio (en realidad, de polisilicio), aunque también puede ser de materiales plásticos, capaz de guiar una potencia óptica (lumínica), generalmente introducida por un láser, o por un led.

Firewall: es un elemento de hardware o software, utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidos, según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

FDDI: (Fiber distributed data interface) se define como una topología de red local en doble anillo y con soporte físico de fibra óptica.

FTP: significa *File Transfer Protocol* (Protocolo de Transferencia de archivos) y es el ideal para transferir grandes bloques de datos por la red.

Gestión de la calidad: de acuerdo a ISO 9000:2000, actividades coordinadas para dirigir y controlar una organización en lo relativo a la calidad.

GigaEthernet: ethernet de alta velocidad que trabaja a velocidades de Gbps.

Hacker: neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

Hardware: Se denomina hardware o soporte físico al conjunto de elementos materiales que componen una computadora. Hardware también son los componentes físicos de una computadora tales como el disco duro, CD-Rom, disquetera, etc.

Helicoidal: en forma de hélice.

Host: computadora en red capaz de brindar algún servicio. Se utiliza para denominar a una computadora principal que puede desarrollar los procesos por sí misma y recibir usuarios.

http: protocolo de transferencia de hipertexto (*HTTP, HyperText Transfer Protocol*) es el protocolo usado en cada transacción de la Web (WWW).

Hub o concentrador: equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Se debe recordar que el hub ya no es usado en gran escala ni a un nivel medio o alto, debido a el gran nivel de colisiones que pueda suceder si alguien pide y luego otro desea lo mismo.

IEEE: siglas de Instituto de Ingenieros Electrónicos y Eléctricos.

Internet: es una red de redes a escala mundial de millones de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP.

IP: es un número que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

IRDA: Infrared Serial Data Link, es un estándar que define una forma de implementar el uso de la tecnología infrarroja por los fabricantes.

ISACA: Asociación de Auditores de Sistemas Informáticos y Control, organismo internacional encargado de establecer los estándares para las labores de auditoria informática.

ISDN: Red Digital de Servicios Integrados, red que procede por evolución de la Red Digital Integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados.

ISO: International Organization for Standardization. Fundada en 1946, es una federación internacional que unifica normas en unos cien países. Una de ellas es la norma OSI, modelo de referencia universal para protocolos de información.

IVD: siglas en inglés para Integrated Voice and Data, integración de voz y datos.

LAN: Local Area Network (Red de Área Local o simplemente Red Local).

LLC: siglas para *Logical Link Control,* control de enlace lógico.

Login: Autenticación o autentificación en términos de seguridad de redes de datos.

Lux: símbolo lx, es la Unidad derivada del SI de iluminancia o nivel de iluminación. Es igual a un lumen por m^2.

MAC: acrónimo de Media Access Control address, dirección de Control de Acceso al Medio de un dispositivo de una red de datos, es un identificador físico, un número, único en el mundo de 48 bits, almacenado en fábrica dentro de una tarjeta de red o una interface usada para asignar globalmente direcciones únicas en algunos modelos OSI (capa 2) y en la capa física del conjunto de protocolos de Internet.

Mainframe: es una computadora grande, potente y cara usada principalmente por una gran compañía para el procesamiento de una gran cantidad de datos; por ejemplo, para el procesamiento de transacciones bancarias.

MAN: red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbits/s hasta 155 Mbits/s.

Mejora continua: de acuerdo a ISO 9000:2000, es la actividad recurrente para aumentar la capacidad de cumplir los requisitos.

Microprocesador: conjunto de circuitos electrónicos altamente integrado para cálculo y control computacional.

MILNET: red precursora de lo que actualmente conocemos como Internet, fue una red militar creada por los Estados Unidos de Norteamérica.

Módem : acrónimo de las palabras modulador/demodulador. El módem actúa como equipo terminal del circuito de datos permitiendo la transmisión de un flujo de datos digitales a través de una señal analógica.

Modulación: técnicas utilizadas para transportar información por una onda portadora.

Multidifusión: es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

NIC: (Network Interface Card, Tarjeta de Interfaz de Red en español), es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment) computadora o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc).

No conformidad: de acuerdo con ISO 9000:2000, es el incumplimiento de un requisito.

Norma: Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc. Mandato u orden que el superior hace observar y guardar al inferior o súbdito.

Normas Jurídicas: las normas jurídicas, tienen como objetivo la regulación de la conducta para con los demás, a fin de organizar la vida social al prevenir conflictos y dar las bases para la solución. Son disposiciones que la alta dirección, por medio de los diferentes departamentos señala como obligatorias, plasmada en los códigos y reglamentos.

Ofimática: conjunto de sistemas informáticos que generan, procesan, almacenan, recuperan y presentan los datos relacionados con el funcionamiento de una oficina.

Organigrama: documento en donde se expresa la estructura oficial de la organización a auditar.

Organización: de acuerdo con ISO 9000:2000, es el conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

OSI: modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

Par trenzado: es uno de los tipos de cables de pares compuesto por hilos, normalmente de cobre, trenzados entre sí.

Password: es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

PGEEE: planta de generación de energía eléctrica para emergencias.

Plotter: dispositivo de impresión conectado a una computadora, y diseñado específicamente para trazar gráficos vectoriales ó dibujos lineales: planos, dibujos de piezas, etc.

Política: arte o traza con que se conduce un asunto o se emplean los medios para alcanzar un fin determinado. Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.

Política de calidad: de acuerdo a la ISO 9000:2000, son las intensiones globales y orientación de una organización, relativas a la calidad tal como se expresan formalmente por la alta dirección.

Política Específica de un tema: son aquellas políticas que están orientadas a tópicos con un interes en específico, por ejemplo, política de adquisición de equipo nuevo.

Política General: es un estado deseado por la empresa respecto a algún rubro en específico, por ejemplo, una política general podría ser la política de calidad de la organización.

Política Particular a una aplicación: *s*on todas aquellas políticas que se enfocan a la toma de decisiones por parte de la alta dirección para responder ante contingencias en algún área en específica, por ejemplo, políticas de protección de la información ante un incendio.

Portabilidad: en programación se entiende como portable cuando un programa puede tener una Compilación en diferentes plataformas y en cualquier Sistema operativo

Procedimientos: acción de proceder. Método de ejecutar algunas cosas, actuación por trámites judiciales o administrativos, es el cauce formal de la serie de actos, en que se concreta la actuación administrativa para la realización de un fin. En calidad y de acuerdo a ISO 9000:2000, un procedimiento se define como la forma especifica para llevar a cabo una actividad o un proceso.

Programas remotos: son programas a los cuales se puede acceder por medio de una terminal hasta una máquina origen que contenga dicho programa, esto por medio de la comunicación a través de una red.

Protocolos: conjunto de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

Protocolo de red: se le llama protocolo de red o protocolo de comunicación, a los diversos conjuntos de reglas que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red.

Proveedor: según la norma ISO 9000:2000, es la organización o persona que prporciona un producto.

PTT: es un método para hablar en líneas half-duplex de comunicación, empujando un botón para mandar, permitiendo comunicación de voz para ser transmitida, y liberando para permitir que comunicación de voz sea recibida.

Rack: armazón metálico con un ancho normalizado de 19 pulgadas. El armazón cuenta con guías horizontales donde puede apoyarse el equipamiento, así como puntos de anclaje para los tornillos que fijan dicho equipamiento al armazón. En este sentido, un rack es muy parecido a una simple *estantería*.

Receptor: como su propio nombre lo dice, es la persona o dispositivo que recibe el mensaje, realiza un proceso inverso al del emisor ya que en él está el descifrar e interpretar lo que el emisor quiere dar a conocer.

Reproceso: de acuerdo a ISO 9000:2000, es la acción tomada sobre un producto no conforme para que cumpla con los requisitos.

Requisito: de acuerdo a ISO 9000:2000, es la necesidad o expectativa establecida, generalmente implícita u obligatoria.

RJ11: es una interfaz física usada para conectar redes de teléfono.

RJ45: es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). *RJ* es un acrónimo inglés de Registered Jack.

Router: (enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

SC: Subscriber Connector, conector cilíndrico para fibra óptica utilizado en enlaces más dedicados.

Servidor: aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas terminales.

Software: conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina.

Spyware: aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas . Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.

ST: Straight Tip, es un conector de fibra óptica que sujeta a la fibra por medio de una aguja y un cilindro que son cerámicos.

STP: acrónimo de Shielded Twisted Pair o Par Trenzado Apantallado. El cable de par trenzado apantallado es justamente lo que su nombre implica: cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie.

Subred: Cuando una red de computadoras se vuelve muy grande, conviene dividirla en redes más pequeñas, éstas son llamadas sudredes.

Switch: o conmutador, es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconection*). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

TELNET: Es un protocolo de comunicaciones que permite al usuario de una computadora con conexión a Internet, establecer una sesión como terminal remota de otro sistema de la Red.

Transceivers: dispositivo que realiza, dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción, utilizando componentes de circuito comunes para ambas funciones.

ThickLAN: modelo de cable coaxial con diámetro de 0.4 pulgadas de 50 ohms .

ThinLAN: modelo de cable coaxial con un diámetro de 0.2 pulgadas de 50 ohms que pueden abarcar una distancia de 185m.

Token: en computación, un token es un bloque primitivo de texto estructurado. Un token puede ser cualquier cosa: español, inglés, símbolos aleatorios etcétera; la única condición es que sea parte útil del texto estructurado. Generalmente, los espacios en blanco no son tomados en cuenta aunque pueden ser parte del token si así se desea. En redes de computadoras, un token es un paquete especial que contiene datos y actúa como mensajero o portador entre cada computadora y dispositivo en una topología anillo.

Token Bus: es un protocolo para redes de área local análogo a Token Ring, pero en vez de estar destinado a topologías en anillo está diseñado para topologías en bus.

Token passing: código de autorización que actúa como método de acceso al medio.

Token ring : tecnología desarrollada por IBM, corresponde al estándar IEEE 802.3, el diseño básico es un anillo de nodos que no superan 256 y que operan de 4 16 Mbps.

Topología: estructura física de una red, puede ser de anillo, de bus, de árbol, jerárquica o bien puede ser una combinación de topologías puras.

Transmisor: o emisor es la persona o dispositivo que elige y selecciona los signos adecuados para transmitir su mensaje, es decir los codifica para poder llevarlo de la manera más entendible al receptor.

USB: Bus de Serie Universal USB, es una interfaz que provee un estándar de bus serie para conectar dispositivos a una computadora,

UTP: es un tipo de cableado estructurado (sistema de cableado para redes interiores de comunicaciones) basado en cable de par trenzado sin blindaje (UTP - Unshielded Twisted Pair).

Valor añadido: en un producto o servicio brindado por una empresa o un distribuidor, se conoce como valor añadido, a todo aquello que agregue características extras a las requeridas por el cliente.

WAN: acrónimo de Wide Area Network que en español significa red de área amplia.

WIFI: es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11. Wi-Fi no es un acrónimo de "Wireless Fidelity";

VAX: fue la primera máquina comercial de arquitectura de 32 bits, lo que la convierte en un hito destacable en la historia de la computación.

BIBLIOGRAFÍA

Apuntes

CARRANZA TORRES, EDUARDO. *"Apuntes del curso de Calidad",* Ciudad de México, 7 de febrero de 2005 al 3 de junio de 2005. Facultad de Ingeniería, Universidad Nacional Autónoma de México, 2005.

Libros

OLGUÍN ROMO, Heriberto; *"Organización y administración de centros de cómputo".* México 1997, Universidad Nacional Autónoma de México, Facultad de Ingeniería. 339 p.

Normas

ISO 9000:2000, COPANT/ISO 9000-2000, NMX-CC-9000-IMNC-2000. *"Sistemas de gestión de la calidad – Fundamentos y vocabulario".*

ISO 9001:2000, COPANT/ISO 9001-2000, NMX-CC-9000-IMNC-2000. *"Sistemas de gestión de la calidad – Requisitos".*

Páginas de Internet

Aguilar Huanuco, Josué J., *"Las categorías IEEE 802" [en línea]*
<http://galeon.hispavista.com/jhosua/IEEE1.htm>
[consulta: 8 de agosto de 2005, 17:55 hrs.]

Capuccio, Víctor E. *"Políticas y procedimientos en la seguridad de la información" [en línea].* <http://www.ilustrados.com/publicaciones/EplpVplEZlTOfazBIB.php>
[Consulta: 28/marzo/2006, 8:38 hrs.]

Farrán Leiva, Yuseff E. "Curso de redes de computadoras" *[en línea].*
<http://inf.udec.cl/~yfarran/web-redes/sub-capa-mac/sub-capa-Mac.htm>
[Consulta: 4 de agosto de 2005, 19:02 hrs.].

Organización Internacional del Trabajo [en línea]. "*Introducción a las NIT: cómo las NIT se crean".* Ginebra, Suiza: Oficina Internacional del Trabajo.
< http://www.ilo.org/public/spanish/standards/norm/introduction/created.htm>
[Consulta: 1 abril 2006, 21:00 hrs.]

Secretaría del Consejo Superior de Administración Electrónica [text/html]
<http://www.map.es/csi/silice/Redlan25.html>
[consulta: 10 de agosto de 2005]

Universidad Veracruzana, México. *"COMPILACIÓN DE PRINCIPIOS Y NORMAS NACIONALES E INTERNACIONALES DE CALIDAD TOTAL: Una guía de consulta para la planeación y certificación empresarial"* [en línea]. "Revista Ciencia Administrativa". Publicación de junio del 2001 número 1.
<http://www.uv.mx/iiesca/revista2001-1/normas.htm>
[Consulta: 1/abril/2006, 20:06 hrs.]

<http://www.lania.mx/biblioteca/newsletters/1998-otono-invierno/internet2.html>
[consulta: 26 junio de 2005]

<http://www.olivo.usal.es/~nines/dalumnos/lan1/parte4.html>
[consulta: 28 de junio de 2005]

<http://elqui.dcsc.utfsm.cl/apuntes/redes/2001/pdf/2-5-Capa-Datos-Versiones-de-Ethernet.pdf>
[consulta: 4 de agosto de 2005]

<http://www.geocities.com/Eureka/Plaza/2131/primeras.html >
[consulta: 23 de septiembre de 2005]

<http://www.tiny.uasnet.mx/prof/cln/ccu/mario/REDES/node35.html>
[consulta: 6 noviembre de 2005]

<http://www.ran.es/personal/enrique/ether.html>
[consulta: 6 de noviembre de 2005]

Tesis consultadas

CABRERA ROSALES, Carlos David; GARCÍA MARTIN, Marcos Moisés. "Diseño e implementación de una red inalámbrica para una cadena de restaurantes". Tesis de licenciatura. Universidad Nacional Autónoma de México, 2004.

CRUZ GARCES, Gustavo Adolfo de la; GOVANTES SALDIVAR, Ángel César. "Propuesta de políticas, normas y procedimientos para la elaboración de sistemas de información con orientación a objetos, bajo la norma ISO 9000". Tesis de licenciatura. Universidad Nacional Autónoma de México, 1997.

FRANCO DELGADO, Guadalupe; GONZÁLEZ MURGUÍA, Daniel; HERNÁNDEZ Y HERNÁNDEZ, Gerardo Alfredo; THAN GÓMEZ, Ruth María; VILLAFUERTE LERÍN, José Antonio. *"La auditoría informática".* Tesis de licenciatura. Universidad Nacional Autónoma de México, 2005.

RENDÓN CATAÑO, José Uriel. *"Diseño y desarrollo de una metodología para la determinación y el establecimiento de normas de seguridad informática"*. Tesis de licenciatura. Universidad Nacional Autónoma de México, 2004.