LOS **SISTEMAS** DE **REDES** EN LA **GESTIÓN OPERATIVA**

Luis Isaías Bastidas Zambrano
Evelyn Concepción Ruíz Parrales
Joffre Vicente León Acurio

CIDE Editorial

www.cidepro.org

Luis Isaías Bastidas Zambrano
Evelyn Concepción Ruíz Parrales
Joffre Vicente León Acurio

LOS SISTEMAS DE REDES EN LA GESTIÓN OPERATIVA

NETWORK SYSTEMS IN OPERATIONAL MANAGEMENT

Luis Isaías Bastidas Zambrano
Evelyn Concepción Ruíz Parrales
Joffre Vicente León Acurio

Los Sistemas de Redes en la Gestión Operativa

Network Systems in Operational Management

CIDE Editorial

Autores:

Luis Isaías Bastidas Zambrano.
Facultad de Informática
Universidad Nacional de La Plata
Facultad de Ciencias de la Salud.
Universidad Técnica de Babahoyo.
lbastidas@utb.edu.ec
https://orcid.org/0000-00032985/5195

Evelyn Concepción Ruíz Parrales.
Facultad de Informática
Universidad Nacional de La Plata
Facultad de Ciencias de la Salud.
Universidad Técnica de Babahoyo.
eruiz@utb.edu.ec
https://orcid.org/0000-0003-2808-0834

Joffre Vicente León Acurio.
Facultad de Informática
Universidad Nacional de La Plata
Facultad de Administración,
Finanzas e Informática.
Universidad Técnica de Babahoyo.
jvleon@utb.edu.ec
https://orcid.org/0000-0002-7467-912X

Primera Edición, junio 2019

Los Sistemas de Redes
en la Gestión Operativa

ISBN: 978-9942-792-89-1 (eBook)

Editado por:
Centro de Investigación y Desarrollo Profesional

Isaías Chopitea y Juan X Marcos
Babahoyo, Ecuador
Móvil - (WhatsApp): (+593) 9 8 52-92-824
www.cidepro.org
E-mail: editorial@cidepro.org

Este texto ha sido sometido a un proceso de evaluación por pares externos con base en la normativa editorial de CIDEPRO.

Diseño y diagramación:
CIDEPRO Editorial

Diseño, montaje y producción editorial:
CIDEPRO Editorial

Hecho en Ecuador
Made in Ecuador

ÍNDICE

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ANEXOS

PREFACIO

Una red LAN es un conjunto de computadoras conectadas entre sí con la finalidad de compartir información, un tipo de red que une organizaciones que se hallan a distancias no más de 100 m.

La propuesta de solución al problema planteado en la parte inicial de este trabajo investigativo esencialmente consiste en complementar las redes que falten al sistema general de comunicación de datos que existe en las instituciones públicas. A las redes complementarias que unirán los diferentes departamentos aislados en este momento se puede señalar que se debe complementar con varios aspectos relacionados a seguridades en redes.

Se deduce que a más del diseño de enlaces cableados e inalámbricos, estos deben disponer de algunas estrategias tecnológicas relacionadas a realizar controles de seguridad como accesos no autorizados. A más de ello se debe tratar de difundir una cultura de seguridad a nivel de usuario, en sus propios equipos.

PREFACE

A LAN is a set of computers connected to each other for the purpose of sharing information, a type of network that links organizations that are at distances of no more than 100 m.

The proposed solution to the problem raised in the initial part of this research work essentially consists in complementing the missing networks to the general system of data communication that exists in public institutions. To the complementary networks that will unite the different isolated departments at this moment, it can be pointed out that it should be complemented with several aspects related to security in networks.

It is deduced that besides the design of wired and wireless links, these must have some technological strategies related to perform security controls such as unauthorized access. In addition, we must try to spread a safety culture at the user level, in their own teams.

FUNDAMENTACIÓN TEÓRICA

Capítulo 1

FUNDAMENTACIÓN TEÓRICA

REDES

Los autores RAYA José y Raya Elena (2008), emiten los siguientes conceptos básicos sobre redes:

"Una red de ordenadores es un sistema de interconexión entre equipos que permite compartir recursos e información. Para ello es necesario contar, además de con los ordenadores correspondientes, con las tarjetas de red, los cables de conexión, los dispositivos periféricos y el *software* conveniente".

Según su ubicación, se pueden distinguir varios tipos de redes en función de su extensión:

- Si se conectan todos los ordenadores dentro de un mismo edificio, se denomina *LAN (Local Area Network).*
- Si se encuentran en edificios diferentes distribuidos dentro de la misma universidad, se denomina *CAN (Campus Area Network).*
- Si se encuentran en edificios diferentes distribuidos en distancias no superiores al ámbito urbano, *MAN (Metropolitan Area Network).*
- Si están instalados en edificios diferentes de la misma o distinta localidad, provincia o país, *WAN (Wide Area Network).*

Entre las ventajas de las redes LAN tenemos:

- Posibilidad de compartir periféricos costosos como son: impresoras láser, módem, fax, etc.
- Posibilidad de compartir grandes cantidades de información a través de distintos programas, bases de datos, etc., de manera que sea más fácil su uso y actualización.
- Reduce e incluso elimina la duplicidad de trabajos.
- Permite utilizar el correo electrónico para enviar o recibir mensajes de diferentes usuarios de la misma red e incluso de redes diferentes.
- Reemplaza o complementa miniordenadores de forma eficiente y con un coste bastante más reducido.
- Establece enlaces con *mainframes.* De esta forma, un ordenador de gran potencia actúa como servidor haciendo que los recursos disponibles estén accesibles para cada uno de los ordenadores personales conectados.
- Permite mejorar la seguridad y control de la información que se utiliza, permitiendo la entrada de determinados usuarios, accediendo únicamente a cierta información o impidiendo la modificaci6n de diversos datos.

Inicialmente, la instalación de una red se realiza para compartir los dispositivos periféricos u otros dispositivos de salida caros; por ejemplo, las impresoras láser, los fax, etc.

Pero a medida que va creciendo la red, el compartir dichos dispositivos pierde relevancia en comparación con el resto de las ventajas. Las redes enlazan también a las personas proporcionando una herramienta efectiva para la comunicación a través del correo electrónico. Los mensajes se envían instantáneamente a través de la red, los planes de trabajo pueden actualizarse tan pronto como ocurran cambios, y se pueden planificar las reuniones sin necesidad de llamadas telefónicas[1].

Según TANENBAUM Andrew (2006), los elementos básicos de una red LAN son:

- Estaciones de trabajo o computadoras
- El servidor de red
- Los cables de comunicación
- Las tarjetas de interface
- El sistema operativo

El autor TERÁN David (2010) hace el siguiente análisis con respecto a la importancia de las redes:

> *"Cuando las redes de computadoras (locales o remotas) surgieron, hicieron posible compartir de una manera más eficiente los recursos informáticos (arquitectura de sistemas, paquetes y programas, y finalmente los datos), de los usuarios. En general, esos recursos son sistemas heterogéneos: Los equipos de fabricantes tienen características diferentes, utilizan y ejecutan programas con características específicas y distintas para las aplicaciones deseadas por los usuarios, y manipulan y producen datos con formatos incompatibles. Así mismo, equipos idénticos de un único fabricante, que se integran en aplicaciones distintas, pueden presentar características heterogéneas".*

Esa heterogeneidad de los sistemas beneficia al usuario, que no está así limitado a un único tipo de sistemas para sus distintas aplicaciones. Así, se puede seleccionar el sistema que mejor se adapte a las condiciones de aplicación que se requieran, así como al presupuesto disponible. Por otro lado, tal heterogeneidad dificulta considerablemente la interconexión de equipos de fabricantes diferentes, según Menasce (1994).

La interconexión de "redes", a su vez, contribuye a hacer más difícil el problema, ya que puede haber redes diferentes con servicios de transmisión diferentes, que requieran interfaces diferentes. Es necesario, pues, una manera con la cual el problema de las heterogeneidades no haga inviable la interconexión de sistemas distintos. En otras palabras, es como diseñar e implementar una red para la interconexión de sistemas heterogéneos. La incompatibilidad de equipos y/o redes fue inicialmente resuelta a través del uso de convertidores[2].

1. RAYA José, RAYA Elena, (2006), "Redes Locales", Editorial Alfaomega Ra-Ma, Madrid-España, Tercera edición.

2. TERÁN David, (2010), "Redes Convergentes", Editorial Alfaomega, Madrid-España, Primera edición

EI almacenamiento y análisis de información ha sido uno de los grandes problemas a que se ha enfrentado el hombre desde que se inventó la escritura. No fue sino hasta la segunda mitad del siglo XX, en que el hombre pudo resolver en parte este problema, gracias a la invención de la computadora.

MEDIOS DE TRANSMISIÓN GUIADOS.

Tanenbaum Andrew (2006) emite los siguientes criterios sobre esto:

> *"Una de las formas más comunes para transportar datos de una computadora a otra es almacenarlos en cintas magnéticas o medios extraíbles (por ejemplo, DVDs grabables), transportar físicamente la cinta o los discos a la máquina de destino y leer dichos datos ahí. Si bien este método se no es tan avanzado como utilizar un satélite de comunicaciones geosincrono, con frecuencia es más rentable, especialmente para aplicaciones en las que un ancho de banda alto o el costo por bit transportado es un factor clave".*

Un cálculo simple aclarará este punto. Una cinta Ultrium estándar puede almacenar 200 giga- bits. Una caja de 60 x 60 x 60 cm puede contener aproximadamente 1000 de estas cintas, con una El capacidad total de 200 terabytes, o 1600 terabits (1.6 petabits). Una caja de cintas puede enviarse a cualquier parte de Estados Unidos en 24 horas por Federal Express y otras compañías. El ancho de banda efectivo de esta transmisión es de 1600 terabits /86,400 seg o 19 Gbps. Si el destino está a solo una hora por carretera, el ancho de banda se incrementa

a casi 400 Gbps. Ninguna red de computadoras puede aprovechar esto.

En el caso de un banco que diariamente tiene que respaldar muchos gigabytes de datos en una segunda máquina (para poder continuar en caso de que suceda alguna inundación o un terremoto), es probable que ninguna otra tecnología de transmisión pueda siquiera acercarse en rendimiento a la cinta magnética. Es cierto que la rapidez de las redes se está incrementando, pero también las densidades de las cintas.[3]

MEDIOS FÍSICOS DE TRANSMISIÓN

El autor Terán David (2010 señala lo siguiente con relación a los medios físicos de transmisión:

La industria de las telecomunicaciones ha empleado una gran variedad de medios físicos para la transmisión de la información. Gran parte de los medios físicos empleados en telecomunicaciones se han utilizado en la construcción de redes, cuatro medios de transmisión se usan con más frecuencia en la implementación de redes hoy en día. Estos son: par de cable trenzado *(twisted-wire pair),* cable coaxial, fibra óptica y transmisión inalámbrica.

Par trenzado

Este tipo de cable fue inventado par IBM y *se* ha utilizado en recientes fechas en redes Ethernet, soporta tasas de transmisión de 10 Mbps

3. TANENBAUN Andrew, 2006, "Redes de computadoras", Prentice-Hall, Madrid-España, Tercera edición

e incrementa la inmunidad a la interferencia magnética y al ruido, evitando el *efecto* NEXT *(Near End Cross Talk).* Permite la transmisión de voz, datos y soporta programas orientados a muchos fabricantes.

Es económico porque en general se usa en las instalaciones de edificios y el costo de instalación y adecuación se ve reducido. La longitud de transmisión es de 100 metros, pudiéndose incrementar a través de repetidores o amplificadores. Existe cable blindado y no blindado, el primero es más resistente al ruido eléctrico y soporta velocidades de transmisión mayores, en cambio el segundo es más fácil de instalar y menos costoso.

Cable coaxial

Básicamente es un cable de dos hilos, en donde existe un hilo central cubierto por un dieléctrico y sobre él una malla envolvente que realiza el papel de hilo secundario, todo esto cubierto por un plástico protector. La tasa de transmisión típica es de 10 Mbps (megabits por segundo), relativamente libre de error. El cable coaxial soporta transmisión simultánea de voz, datos y vídeo, es fácil de instalar y expandir. Este fue uno de los principales medios de transmisión usados en redes locales, pero a la fecha se ha sustituido por el uso de cable par trenzado, que es más manejable y más económico. Aún se le usa como columna vertebral para interconectar redes alejadas hasta 500 metros en forma directa. Existen dos tipos de cable: Coaxial delgado y coaxial grueso. El construir una red con este tipo de cable,

no requiere de algún equipo adicional para conectar las computadoras.

Fibra óptica

Este tipo de cable lleva información en forma de pulsos de luz a través de una fibra de vidrio. La luz tiene un ancho de banda mayor que la señal eléctrica, por lo tanto el cable de fibra óptica soporta tasas de transmisión de 100 Mbps. La fibra óptica consta de básicamente dos partes: Un centro llamado *core* y una capa envolvente de fibra de vidrio Ilamado *cladding,* en los cuales se propaga la luz. La señal es generada par un transmisor óptico, el cual convierte la señal eléctrica en un pulso de luz y transmitida a través de la fibra hasta alcanzar el receptor óptico que convierte la luz en señal eléctrica. El transmisor usa un LED, mientras que el receptor usa un fotodiodo. La fibra óptica es inmune al ruido eléctrico, y por lo tanto provee un bajo índice de error a grandes distancias de transmisión, además, este tipo de cable es ligero, flexible y no es costoso; sin embargo, no es fácil de acoplar, y por lo tanto no es fácil de instalar. La fibra óptica se usa cada vez más como columna vertebral de redes donde se requieren ambientes seguros y lugares en donde existe equipo eléctrico pesado, o en donde existen altos voltajes, motores, plantas de luz, etc. Los estándares para fibra óptica se encuentran descritos en IEEE FOIRL Y ANSI X3T9, el cual usa cable de fibra óptica multimodo con conectores ST y diámetros de 62.5/125 micras[4].

4. TERÁN David, (2010), "Redes Convergentes", Editorial Alfaomega, Madrid-España, Primera edición

Inalámbrico

La transmisión inalámbrica tiene diferentes usos. Uno es para interconectar dos LAN donde podría ser muy difícil interconectarlas físicamente. Par ejemplo, en lugar de interconectar dos edificios con un cable, podría ser usado un enlace de microondas. La transmisión vía satélite es otro ejemplo de transmisión inalámbrica. Otra manera más flexible en la cual la transmisión inalámbrica se utiliza, es la transmisión de radio y la sustitución de cable físico que se usa para conectar computadoras en una LAN. Esto hace muy sencillo poder cambiar de localidad los equipos sin necesidad de cambiar cables físicos.

La transmisión inalámbrica tiene desventajas. Las LAN que emplean radiofrecuencia(s) para transmitir están sujetas a la interface, la cual puede causar tasas de error muy altas. También, la distancia a la cual se puede expandir la red frecuentemente es limitada. La transmisión inalámbrica se utiliza comúnmente para conectar sistemas individuales a los concentradores, con cableado físico para conectar los concentradores. Las LAN que utilizan técnicas de transmisión inalámbricas diferentes a la de radio, tales como LAN que utilizan enlaces infrarrojos, usualmente requieren que no haya barreras físicas entre el transmisor y el receptor.

PROTOCOLO DE REDES

Los protocolos de red son una o más normas estándar que especifican el método para enviar y recibir datos entre varios ordenadores. Su

instalación está en correspondencia con el tipo de red y el sistema operativo que la computadora tenga instalado.

No existe un único protocolo de red, y es posible que en un mismo ordenador coexistan instalados varios de ellos, pues cabe la posibilidad que un mismo ordenador pertenezca a redes distintas. La variedad de protocolos puede suponer un riesgo de seguridad: Cada protocolo de red que se instala en un sistema queda disponible para todos los adaptadores de red existentes en dicho sistema, físicos (tarjetas de red o módem) o lógicos (adaptadores VPN). Si los dispositivos de red o protocolos no están correctamente configurados, se puede dar acceso no deseado a los recursos de la red. En estos casos, la regla de seguridad más sencilla es tener instalados el número de protocolos indispensable; en la actualidad y en la mayoría de los casos debería bastar con sólo TCP/IP.

Dentro de la familia de protocolos se pueden distinguir:

Protocolos de transporte:

- ATP (Apple Talk Transaction Protocol)
- NetBios/NetBEUI
- TCP (Transmission Control Protocol)

Protocolos de red:

- DDP (Delivery Datagram Protocol)
- IP (Internet Protocol)
- IPX (Internet Packed Exchange)
- NetBEUI Desarrollado por IBM y Microsoft.

Protocolos de aplicación:

- AFP (Appletalk File Protocol)
- FTP (File Transfer Protocol)
- Http (Hyper Text transfer Protocol)

Dentro de los protocolos antes mencionados, los más utilizados son:

- IPX / SPX, protocolos desarrollados por Novell a principios de los años 80 los cuales sirven de interfaz entre el sistema operativo de red Netware y las distintas arquitecturas de red. El protocolo IPX es similar a IP, SPX es similar a TCP por lo tanto juntos proporcionan servicios de conexión similares a TCP / IP.

- NETBEUI / NETBIOS (Network Basic Extended User Interface / Network Basic Input / Output System) NETBIOS es un protocolo de comunicación entre ordenadores que comprende tres servicios (servicio de nombres, servicio de paquetes y servicio de sesión, inicialmente trabajaba sobre el protocolo NETBEUI, responsable del transporte de datos. Actualmente con la difusión de Internet, los sistemas operativos de Microsoft más recientes permiten ejecutar NETBIOS sobre el protocolo TCP / IP, prescindiendo entonces de NETBEUI.

- APPLE TALK es un protocolo propietario que se utiliza para conectar computadoras **Macintosh** de **Apple** en redes locales.

- TCP/IP (Transmission Control Protocol / Internet Protocol) este protocolo fue diseñado a finales de los años 60, permite enlazar

computadoras con diferentes sistemas operativos. Es el protocolo que utiliza la red de redes Internet. (*Academia de Networking de Cisco Systems "Guía CCNA 1 y 2", Tercera Edición 2004)*

REDES WI-FI

El autor CARBALLAR José emite los siguientes criterios básicos sobre las redes Wi-Fi:

Una comunicación inalámbrica es aquella que se lleva a cabo sin el uso de cables de interconexión entre los participantes; por ejemplo, una comunicación con teléfono móvil es inalámbrica, mientras que una comunicación con teléfono fijo tradicional de cable no lo es. No cabe duda de que la tecnología inalámbrica está ocupando rápidamente las preferencias de todo tipo de usuarios. La telefonía móvil está cada vez más cerca de convertirse en un sistema de comunicación personal universal en el mundo occidental, los teléfonos inalámbricos de casa son cada vez más comunes en detrimento de los tradicionales teléfonos con cables y, desde hace pocos años, los ordenadores están también liberándose de sus ataduras. Cada a vez son más los hogares, los cafés, las pequeñas empresas, los aeropuertos o las grandes compañías en los que se dispone de redes inalámbricas.

Wi-fi es una tecnología que permite que una gran variedad de equipos informáticos (ordenadores, impresoras, discos duros, cámaras, etc.) puedan interconectarse sin necesidad de utilizar cables. La aplicación principal que está teniendo Wi-Fi en la actualidad es la de permitir que varios ordenadores de casa o de la oficina puedan compartir el

acceso a Internet (de ADSL o cable). No obstante, esta tecnología permite crear una red entre los distintos equipos para compartir todos sus recursos.

Por ejemplo, se puede utilizar un disco duro externo común para las copias de seguridad, compartir las carpetas de archivos locales pertenecientes a un proyecto común, compartir una impresora, pasarle las fotos de las vacaciones a la unidad multimedia conectada a la televisión o ver imágenes de video cámaras web entre otros muchos ejemplos.

Para hacernos una idea de cómo va esto, aunque Wi-Fi permite otras configuraciones, podemos decir que lo que hace que funcione Wi-Fi es un equipo conocido como punta de acceso. El punto de acceso es una caja que no suele tener más de 25 centímetros en su lado más ancho y unos 2 o 3 en su lado más estrecho (aunque las hay de todas las formas y colores). En las redes pequeñas, el punta de acceso suele estar colocado junto al equipo de acceso a internet (lo que se conoce como *router* ADSL o cable) o puede formar parte de él. Si la red es grande, lo normal es que se encuentren en las partes altas de las paredes de las oficinas, en los salones de los hoteles, de las cafeterías o de las estaciones de autobús, de tren o en los aeropuertos.

Una de las principales ventajas de Wi-Fi es que utiliza el mismo protocolo que internet (protocolo TCP/IP, ya hablaremos más adelante algo más sobre él). Este protocolo lo utilizan también las redes

locales de cable, por lo que interconectar una red Wi-Fi con internet o con una red local cableada es bastante simple[5].

CABLEADO ESTRUCTURADO

Los autores HAYES Jim y ROSENBERG Paul, emiten los siguientes criterios sobre el cableado estructurado:

Varios factores han influenciado enormemente el desarrollo de los sistemas de cableado estructurado estandarizados para construcción de redes. El primer factor fue la migración hacia sistemas abiertos, no propietarios. Con la desintegración de AT&T, el monopolio para el desarrollo de estándares de telecomunicaciones desapareció, siendo reemplazada por una menos dominante, Bellcore, y un mercado competitivo. Como las redes y los sistemas de comunicación se tornaban más populares y extendidos, los fabricantes notaron que los usuarios demandaban sistemas de cableado estandarizados que les permitieran utilizar productos de distintos pro- veedores y actualizar la instalación sin necesidad de realizar cambios totales.

El modelo para el cableado estructurado estándar proviene del desarrollo y uso del cableado UTP de bajo costo para redes de computadora por parte de proveedores de Ethernet y del desarrollo de estándares de performance de múltiples proveedores de cable UTP, con Anixter como distribuidor de cableado. Como el mercado y la mayoría de los proveedores adoptaron al UTP como tipo de cableado,

5. CARBALLAR José, 2010, "Wi-Fi, lo que se necesita conocer", Editorial Alfaomega, México-México, Primera edición

este se convirtió primero en un *estándar de facto* en el mercado, y luego en un *estándar de jure* por acuerdo entre los proveedores.

Hoy, la mayoría de las construcciones de cableado de comunicaciones siguen las pautas desarrolladas a lo largo de esta evolución y publicadas por el comité AlEIA TR41.8. A pesar de que no es un estándar mandatario, sino un estándar voluntario de interoperabilidad desarrollado por los proveedores de los productos contemplados en el estándar, es un enfoque de sentido común para el cableado de comunicaciones que permite la interoperabilidad simplificada y la actualización.

ESTÁNDARES PARA EL CABLEADO DE RED

Los orígenes de los estándares

El uso extendido de cualquier tecnología depende de la existencia de estándares aceptables. Los usuarios prefieren invertir en soluciones "estándar" y ahorrarse problemas, porque les aseguran interoperabilidad y expansión futura. Los estándares deben incluir estándares de componentes, estándares de red, estándares de instalación, estándares para métodos de prueba y buenos estándares de calibración[6]. Los estándares también incluyen seguridad, como lo establecido en las Normas Eléctricas, el único estándar obligatorio que la mayoría de las instalaciones de cable deben cumplir.

6. HAYES Jim, ROSENBERG Paul, 2009, "Cableado de redes para voz, video y datos. Planificación y construcción", Editorial CENGAGE Learning, Buenos Aires, Tercera edición

Estos estándares son desarrollados por una variedad de grupos que trabajan conjuntamente. Los estándares de red provienen de Bellcore, el Instituto Nacional Americano de Estándares (ANSI), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), la Comisión Electrotécnica Internacional (IEC) y otras organizaciones mundiales, mientras que los de componentes y prueba surgen de alguna de estas mismas instituciones, la unión entre la Alianza de Industrias Electrónicas y la Asociación de Industrias de Telecomunicaciones (llA/EIA) en los Estados Unidos y del IEC, la Organización de Estándares Internacionales (ISO) y otros grupos internacionales.

Las unidades básicas de medición (como "voltios" y "metros") son desarrolladas por laboratorios nacionales de estándares tales como el Instituto Nacional de Estándares y Tecnología (NIST), antiguamente la Agencia Nacional de Estándares de Estados Unidos, que existen en casi todos los países para regular todos los estándares de medición. La cooperación internacional es mantenida para asegurar conformidad mundial para todos los estándares absolutos.

También debemos discutir los estándares *de facto* aquellos que son generalmente aceptados para componentes y sistemas que evolucionaron en el mercado porque no había todavía estándares *de jure* y todos aceptaban la experiencia de un proveedor.

Los estándares de Facto vienen primero

En cualquier tecnología de rápido desarrollo como la computación y las comunicaciones, siempre hay resistencia a desarrollar estándares.

Los críticos dicen que los estándares retrasan el desarrollo de la tecnología. Algunos críticos se oponen porque sus estándares no son los que están siendo propuestos y en algunos casos, nadie realmente sabe cuáles son mejores. En estas circunstancias, los usuarios se adelantan, eligiendo las mejores soluciones para sus problemas y con ello avanzar.

Los vendedores más fuertes hacen los estándares *de facto.* Para el cableado de red, Anixter, un gran distribuidor de cableado y productos de red, desarrollo un grupo de estándares que fueron adoptados bajo la norma TIA / EIA, con modificaciones para adaptarse a los numerosos fabricantes que participan de los procesos de estandarización.

VOZ SOBRE IP

El autor TERÁN David, (2010), señala que mientras el ambiente de las redes de computadoras cambia extensamente en la última década, las redes de computadoras se mantienen más o menos como eran en la década de 1960. Cables individuales desde teléfonos únicos (individuales) que van hasta una cabina, y a segmentos de cables que van hasta un PBX. Desde 1960, obviamente han sido modificados a modelos digitales, así como los aparatos telefónicos son digitales conectados sobre líneas digitales. Pero la topología de red es la misma, para la misma razón.

La voz está situada en un ambiente conmutado, y los ambientes conmutados generalmente demandan una topología en estrella. La conmutación de la voz ha permanecido consolidada en una sola caja,

y algunas de las razones para ello son técnicas. Lo más importante fue la razón cultural; la industria ha tenido la idea de que el PBX era una caja en un cuarto, esto es porque la solución fue proporcionada de esta forma al mercado. La necesidad de encontrar enlaces entre el mundo de las telecomunicaciones y las computadoras se remonta a muchos años atrás. Hace solo algunas décadas, algunas grandes firmas observaron la ventaja de unir los sistemas de computadoras y la voz.

La telefonía IP consiste en emplear redes IP para prestar servicios de transmisión de voz, que son en mayor o menor grado equivalentes a los servicios tradicionales de la red de telefonía pública conmutada. La telefonía IP puede considerarse simplemente como una aplicación adicional de los servicios existentes.

INTEGRACIÓN DE LA TELEFONÍA EN LAS COMPUTADORAS (CTI)

La tecnología CTI (Computer Telephony Integration: Telefonía Integrada por Computadora), se ha utilizado desde la década de 1980, con la integración entre telefonía y computadoras mediante un conjunto de técnicas cuyo fin es coordinar el funcionamiento de los sistemas telefónicos e informáticos. Sus primeras aplicaciones se circunscribían a nichos de mercado muy específicos tales como centros de llamadas *(call centers)* en los que el alto volumen de llamadas justificaba el empleo de una solución de este tipo. Fue hasta la década de 1990 que se despertó el interés del mercado en este tipo de aplicaciones, cuya consecuencia lógica fue la aparición

de estándares y productos comerciales que contribuyeron a una evolución vertiginosa.

La primera integración de la telefonía en las computadoras, fue conectando una **mainframe** con un **PBX**. Esto se realizó varios años antes de que la identificación de la línea de llamada estuviera disponible, pero habilitó algunas aplicaciones altamente efectivas.

REDES PRIVADAS VIRTUALES

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado en la actualidad que las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja, sobre todo para las empresas que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial.

El autor TRUJILLO Edison (2006) menciona que el alto costo necesario para implementar y mantener enlaces privados, involucra invertir en hardware y software y en servicios de telecomunicaciones para crear redes amplias de servicio (WAN), ha llevado a las empresas

a una situación insostenible. Las líneas de larga distancia, así como los servicios conmutados, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar las tecnologías complejas conlleva a un crecimiento continuo tanto en el número de personas como en su experiencia. Igualmente, la dependencia de aplicaciones de red requiere un aprovisionamiento separado de BACKUP además de una expansión de la infraestructura de la red privada ya existente. Los ahorros de costos son el poderoso atractivo que ofrecen las redes virtuales privadas ya que se construyen sobre una red pública, sin olvidar la seguridad de los datos transmitidos.

Virtual Private Network (VPN) es un grupo de dos o más sistemas de ordenadores, generalmente conectados a una red corporativa privada, que se comunican “con seguridad” sobre una red pública. Es decir, que para transmitir información a través de una red pública (insegura) en la VPN se aplican métodos de seguridad para garantizar la privacidad de los datos que se intercambian entre ambas, y protocolos de túneles.

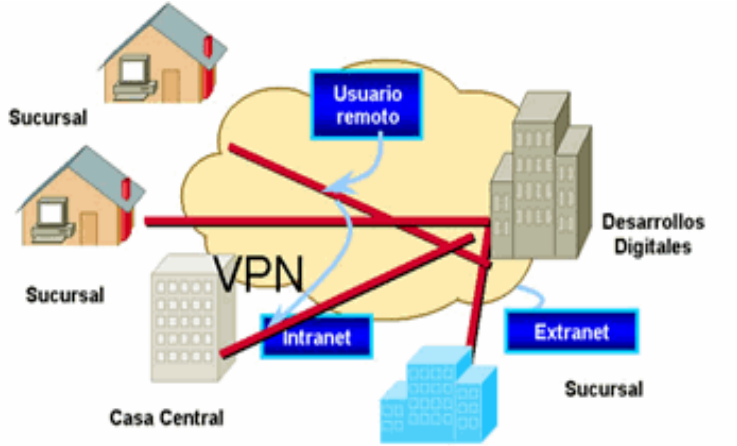
A las redes privadas virtuales, se les considera “privadas” porque se establecen exclusivamente entre el emisor y el receptor de la información, y “virtuales” porque no se necesita un cable o cualquier otro medio físico directo entre los comunicantes.

Las VPN extienden la red corporativa de una empresa a las oficinas distantes, por ejemplo. En lugar de alquilar oficinas dedicadas con un

costo muy elevado, utilizan los servicios mundiales de IP, incluyendo el internet. Usando una VPN, se crea una conexión privada segura a través de una red pública como internet. Los usuarios remotos pueden hacer una llamada local a internet, y no usar llamadas de larga distancia.

La VPN lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura pública, usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como en internet o en alguna otra red comercial, en el túnel privado se simula una conexión punto a punto. Este recurso hace que por la misma red puedan crearse muchos enlaces por diferentes túneles virtuales a través de la misma infraestructura. También hace universales para su transporte los diferentes protocolos LAN entre los que se encuentran ip, ipx, appletalk y netbeui, de allí la característica de multiprotocolo que hace sumamente universal la tecnología de las redes virtuales privadas.

Figura 1. Redes Privadas Virtuales



Fuente: http://www.internueve.com.ar/?q=node/63.

Requerimientos básicos de una VPN

Una red privada virtual ha de proveer de los siguientes mecanismos básicos, aunque en ocasiones puede obviarse algunos:

- Autenticación de usuarios, verificar la identidad de los usuarios.
- Administración de direcciones, debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.
- Encriptación de datos, los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.
- Administración de claves, mantenimiento de claves de encriptación para los clientes y los servidores.

- Soporte multiprotocolo, ha de ser capaz de manejar protocolos comunes, usando la red pública.

SEGURIDAD INFORMÁTICA

El autor RODAO Jesús (2004), define a la seguridad informática como: "El conjunto de procedimientos que nos permite que nuestros datos de hoy puedan ser utilizados mañana sin ninguna norma de calidad en los mismos. Por ello, la seguridad abarca muchos temas aparentemente diferentes como el mantenimiento regular de los equipos, la ocultación de datos, la protección de los mismos con claves de acceso y más".

> *"El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora."*[7]

La seguridad informática no solo debe encargarse de los posibles fallos desaprensivos, sino que también debe tener en cuenta los errores que se pudieran generar por el mal funcionamiento del hardware, así como prevenir acciones involuntarias que puedan afectar la seguridad de la información que se encuentre contenida en los sistemas. La seguridad informática también ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares a tener una aplicación de dimensiones inimaginables y crecientes que incluyen transacciones

7. ALDEGANI, Gustavo, 2003"Seguridad Informática."MP Ediciones. Argentina.

financieras, acuerdos contractuales, información personal, archivos médicos, negocios por internet y más. (AREITIO Javier, (2008)).

Importancia de la Seguridad Informática

Hoy en día no existe duda de que nos encontramos en una nueva era caracterizada por el uso masivo de la información, que adicionalmente ha acarreado mucha más relevancia que en anteriores épocas, debido lo cual es fundamental dentro de las organizaciones el poder detectar las vulnerabilidades del sistema de información para contrarrestar las amenazas y riesgos por el gran número de usuarios con potencial de ataque, que no tan solo se centran en el ambiente que se ubica fuera de la organización, sino también en los usuarios comunes que trabajan y son una gran amenaza a la seguridad si no se tienen políticas claras de acceso a la información.[8]

Después de conocer las amenazas y puntos débiles del ambiente, adquiridos en el análisis de riesgos, o después de la definición formal de las intenciones y actitudes de la organización que están definidas en la política de seguridad de la información, debemos tomar algunas medidas para la implementación de las acciones de seguridad recomendadas o establecidas. Recuerde que las amenazas son agentes capaces de explotar fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causan pérdidas o daños a los activos de una empresa y afectan sus negocios.

8. ACISSI, 2011, "Seguridad Informática", Ediciones ENI, Primera edición, Barcelona – España.

No basta conocer las fragilidades del ambiente o tener una política de seguridad escrita.

Se debe instalar herramientas, divulgar reglas, concienciar a los usuarios sobre el valor de la información, configurar los ambientes etc. Debemos elegir e implementar cada medida de protección, para contribuir con la reducción de las vulnerabilidades; cada medida debe seleccionarse de tal forma que, al estar en funcionamiento, logre los propósitos definidos. (FINE Leonard, 2005).

Gran parte de esa concientización está en manos de los responsables de seguridad de la información apoyados en todo momento por la Gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas

Principios de la Seguridad Informática

La seguridad informática se centra en 3 principios básicos, los cuales son de gran importancia para el plan de seguridad informática.

- Confidencialidad
- Integridad
- Disponibilidad

Confidencialidad

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático, basándose en este principio, las herramientas de seguridad informática deben proteger el sistema

de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.[9]

Integridad

Se refiere a la validez y consistencia de los elementos de información almacenados y procesador en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

Disponibilidad

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran, este principio es importante

9 ATELIN Philippe, 2006, “Redes Informáticas”, ediciones ENI, Primera Edición, Barcelona-España.

en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.[10]

Norma ISO 27002

Esta norma de la organización IOS-IEC consiste en un conjunto de recomendaciones que indican acerca de sobre qué medidas tomar en la empresa para asegurar los Sistemas de Información, está compuesta por objetivos, los objetivos de seguridad recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada una de las áreas que los agrupa. Para conseguir cada uno de estos objetivos la norma propone una serie de medidas o recomendaciones (controles) que son los que en definitiva se aplicaran para la gestión del riesgo analizado. (AREITIO Javier, (2008)).

Áreas / Secciones sobre las que actúa

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información, para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades, las principales áreas son:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.

10. BAETA Jesús, "Seguridad Informática "en línea : http://es.scribd.com/doc/95069532/Seguridad-Informatica

- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Marco Legal, y Buenas Prácticas.[11]

Política de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir

11. ISO, "ISO27000" http:/www.iso.org

en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.[12]

Elementos de una política de seguridad informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a toda la información a la que tiene acceso.

12.CALDER Alan, 2009, "Information Security Base on ISO 270001 / ISO 270002", Editorial Van Haren, Wilco - Amersfoort

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones. Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

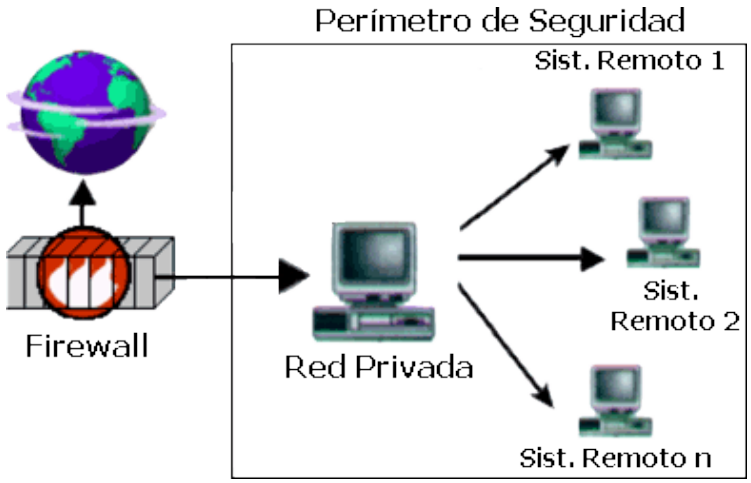
Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc. (RODAO Jesús, (2004))

FIREWALL O CORTAFUEGO

El autor AREITIO Javier (2004) señala que: "Un cortafuegos o firewall es un dispositivo de seguridad de red diseñado para restringir el acceso a los recursos, tanto a la información como a los servicios, de acuerdo a una política de seguridad basada en reglas. Los cortafuegos no son la solución definitiva a todos los problemas de seguridad en red, a los ataques remotos o al acceso no autorizado a los datos del sistema, sino que sirven para conectar dos partes de una red y

controlar el tráfico de datos entre ellas. A menudo se instala entre una red completa de la organización e Internet. También puede colocarse entre departamentos dentro de una Intranet, o bien puede utilizarse entre socios corporativos conectados mediante una extranet".

Figura 2. Seguridad de la información



Fuente: Areito Javier (2004).

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa. Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

LA GESTIÓN OPERATIVA

Varios autores tratan de explicar a la gestión operativa o "gestión hacia abajo" la que realiza el funcionario o directivo público hacia el interior de su organización para aumentar su capacidad de conseguir los propósitos de sus políticas. Cubre los cambios en la estructura de la organización y en el sistema de roles y funciones, la elección de personal directivo y asesor de mediano nivel, los procesos de capacitación del personal de planta permanente, la mejora continua del funcionamiento de la organización con su actual tecnología y la introducción de innovaciones técnicas y estratégicas acordes con los proyectos en curso. Sus principales tareas son:

- **Análisis de los servicios**: Fundamentalmente se refiere al análisis de la concordancia entre los servicios ofrecidos o que se piensa ofrecer y los requerimientos de los ciudadanos. También se refiere al cumplimiento de las especificaciones técnicas propias de cada producto o servicio, y a las pruebas de su correcto funcionamiento.

- **Análisis de los procesos:** Se refiere a los procesos técnicos y administrativos, y a su encuadre legal, que se utilizan o van a utilizarse para la realización de proyectos, prestación de servicios, etc., tanto en lo referente a la relación con el público destinatario como a la relación con otras organizaciones de la administración pública.
- **Revisión de los modos de diseñar y dirigir:** El enfoque

estratégico de la administración pública entraña, a diferencia del enfoque burocrático, un permanente proceso de búsqueda de procedimientos más eficientes para la realización de proyectos y la prestación de servicios, tratando de lograr resultados acordes con los requerimientos de la gente sin malgastar los recursos públicos disponibles.

La tarea esencial de la gestión operativa es el despliegue de recursos y capacidades para obtener resultados concretos. Requiere objetivos acertados (acordes con los requerimientos sociales), capacidad de conseguir recursos y lograr implantar sistemas, procedimientos y personal en forma acorde con lo que se quiere conseguir.

Según una visión estratégica de la gestión operativa, los directores son responsables del uso que hacen del poder y del dinero público, en una actuación que debe ser imparcial, creando organizaciones adaptables, flexibles, controlables y eficientes.

La visión convencional del funcionamiento del sector público lo considera un caso especial de creación de valor en condiciones de pocos cambios y conflictos, con innovaciones mínimas, manteniendo a la capacidad operativa contenida dentro del sistema de la organización misma. La nueva visión estratégica aparece como realmente necesaria cuando hay muchos cambios y conflictos y, por ende, necesidad de innovar para asumir los nuevos desafíos con posibilidades de éxito.

Desde el punto de vista de la gestión operativa, se puede incrementar

significativamente el valor público mediante:

- El aumento de la cantidad o la calidad de las actividades por recurso empleado.
- La reducción de los costos para los niveles actuales de producción.
- Una mejor identificación de los requerimientos y una mejor respuesta a las aspiraciones de los ciudadanos.
- Realizar los cometidos de la organización con mayor imparcialidad.
- Incrementar la disponibilidad de respuesta e innovación.

Para reestructurar sus organizaciones con los lineamientos de una gestión operativa innovadora, los directivos públicos deben analizar cinco cuestiones principales:

- Decidir que producir y cómo actuar para ofrecer esos productos.
- Diseñar las operaciones necesarias para obtener esos productos o servicios.
- Utilizar y ajustar los sistemas administrativos de su organización, e innovar en ellos, para aumentar la calidad, flexibilidad y productividad de los sistemas.
- Atraer colaboradores nuevos para la realización de los objetivos de la organización.

- Definir tipo, grado y ubicación de las innovaciones que se consideren necesarias.

Es muy importante definir la misión y los objetivos de la organización en forma simple, clara y general. Debe existir, a partir de allí, una jerarquía de finalidades y metas, de diferentes grados de abstracción, que orienten las actividades operativas, hasta llegar a los exhumo propiamente dichos (productos o servicios).

Esas pirámides de objetivos son muy útiles, aparte de la orientación interna, para el seguimiento y control externo de las organizaciones. La base para diseñar procesos, y para hacer la revisión de dichos procesos en el tiempo, es el diseño y revisión de los exhumo (productos o servicios) de la organización. Algunos aspectos que conviene tener en cuenta son los siguientes:

- No se puede diseñar un proceso sin saber que producto se quiere conseguir.
- En las operaciones, frecuentes en la Administración Pública, que combinan servicios a prestar y obligaciones a asumir, la diferencia entre producto y proceso es más ambigua.
- Para los funcionarios identificados con la cultura burocrática tradicional, los procesos suelen ser más importantes que los productos.

Los sistemas administrativos incentivan y orientan la actividad de la organización, garantizan la realización de los objetivos y la

prestación efectiva de los servicios. Los sistemas administrativos más importantes son los que:

- Establecen la estructura administrativa, es decir, definen los grados y áreas de autoridad, las responsabilidades y las funciones.
- Estipulan los procedimientos para los procesos de toma de decisión sobre temas clave (la planificación estratégica).
- Definen las tecnologías de la organización para la configuración de políticas, programas y actuaciones.
- Gestionan el personal, es decir, reclutan, seleccionan, entrenan, evalúan, recompensan y promocionan a los empleados.
- Definen los sistemas de control y gestión de la información, en lo referente al empleo de los recursos, los niveles de actividad y los logros obtenidos.

Desde una perspectiva estratégica, los sistemas administrativos deben ser vistos, no aislados, sino en su conjunto, y evaluados según su aporte a la estrategia general de la organización.

SITUACIÓN PROBLEMÁTICA

Capítulo 2

SITUACIÓN PROBLEMÁTICA

La calidad de la gestión pública puede significar la diferencia entre una ciudad caracterizada por el crecimiento y la prosperidad, y una caracterizada por la decadencia y la exclusión social. La buena gobernanza contempla que los mecanismos, los procesos y los instrumentos para la toma de decisiones y acciones faciliten el compromiso cívico y la rendición de cuentas. La promoción de la transparencia puede desempeñar un papel protagónico en el mejoramiento de la calidad del desarrollo sostenible local.

Se entiende por gestión operativa o “gestión hacia abajo” la que realiza el directivo público hacia el interior de su organización para aumentar su capacidad de conseguir los propósitos de sus políticas. Abarca los cambios en la estructura de la organización y en el sistema de roles y funciones, la elección de personal directivo y asesor de mediano nivel, los procesos de capacitación del personal de planta permanente, la mejora continua del funcionamiento de la organización con su actual tecnología y la introducción de innovaciones técnicas y estratégicas acordes con los proyectos en curso.

Las instituciones públicas en cuanto a las intercomunicaciones entre el edificio matriz con bodega y equipo caminero se refiere, ha venido trabajando de manera manual, ya que no cuenta con una red informática para la respectiva comunicación entre ellas, lo que hace que los procesos se realicen de una forma muy lenta.

Actualmente la Institución se halla muy empeñada en cumplir una tarea modernizadora en sus edificios, la misma que implica una mejora en la gestión operativa, pero durante esta labor se ha podido observar algunas dificultades relacionadas con el aspecto tecnológico, entre ellas podemos señalar:

- Actualmente las instituciones públicas tienen una red poco estructurada con cable categoría 6.
- Necesidad de una red para comunicación de datos entre todas las dependencias de la institución, incluyendo a la bodega y equipo caminero, que se hallan a gran distancia.
- No se ha explotado avances tecnológicos como el Internet, redes inalámbricas, voz y video sobre IP.
- La consulta de existencia de los materiales en bodega se lo hace realizando una llamada telefónica, esto debido a que no se tiene una red que comunique estas dependencias.
- El departamento de Equipo Caminero no tiene ninguna comunicación con las demás dependencias.
- El proceso de registro de asistencia que se lleva a cabo en los departamentos externos es todavía de tipo manual, lo que produce demoras y errores frecuentes en cálculos.
- Se hace difícil el control de los empleados de los departamentos que están fuera del edificio principal.

- Muchos departamentos están sin red de datos, por lo cual, él envió de información se lo hace manualmente y en varias ocasiones esta se ha perdido o a llegado deteriorada.
- El nivel de seguridad a nivel de redes inalámbricas es sumamente bajo.

MÉTODOS, TÉCNICAS Y HERRAMIENTAS UTILIZADAS

Capítulo 3

MÉTODOS, TÉCNICAS Y HERRAMIENTAS UTILIZADAS

Específicamente se han aplicado dos tipos de investigación que son:

Bibliográfica

Consiste en la recopilación de información existente en libros, revistas e internet, este tipo de investigación permitió la elaboración del marco teórico referido especialmente a redes, seguridades y más, el mismo que fundamenta científicamente la propuesta de solución.

De campo

Se utilizó para diagnosticar y ratificar la problemática expuesta inicialmente, esta fue llevada a cabo en el sitio mismo donde se tienen las manifestaciones del problema, es decir en las instituciones públicas, las técnicas para la recopilación de información fueron la encuesta y la entrevista, las encuestas fueron realizadas tanto a empleados del departamento de sistemas (usuarios internos) como a los empleados de la institución (usuarios externos); mientras que las entrevistas se las realizó al director del departamento de informática de una instituciones públicas. Los instrumentos asociados a las técnicas para recopilar informaciones antes mencionadas fueron el cuestionario y la guía de entrevista.

La modalidad investigativa que se ha utilizado en esta investigación es la denominada cuali-cuantitativa. La investigación cualitativa es el **procedimiento metodológico** que se caracteriza por utilizar palabras,

textos, discursos, dibujos, gráficos e imágenes para comprender la gestión operativa por medio de significados y desde una perspectiva holística, pues se trata de entender el conjunto de cualidades interrelacionadas que caracterizan a un determinado fenómeno y se la aplico para determinar los objetos cualitativos del problema como el mal servicio, eficiencia y más.

La investigación cuantitativa se caracteriza por recoger, procesar y analizar datos cuantitativos o numéricos sobre variables previamente determinadas. Esto ya hace darle una connotación que va más allá de un mero listado de datos organizados como resultado; pues estos datos que se muestran en el informe final, están en total consonancia con las variables que se declararon desde el principio y los resultados obtenidos van a brindar una realidad específica a la que estos están sujetos. Dicha metodología se la aplico para ratificar estadísticamente los síntomas de la problemática.

Los tipos de investigación aplicados son:

Bibliográfica

Este tipo de investigación se la desarrolla en base a la recopilación de la información de fuentes primarias, se la utilizó para desarrollar el marco teórico caracterizado por aspectos de redes de diverso tipo y la seguridad en las mismas.

De Campo

Se la lleva a cabo en base a encuestas o entrevistas y se la aplicó para desarrollar el marco metodológico, fue llevada a cabo en el Departamento de Sistemas de una institución pública.

POBLACIÓN Y MUESTRA

La población involucrada en la problemática descrita en el inicio de este trabajo investigativo está estructurada de la siguiente forma:

Cuadro 1. Número de población

FUNCIÓN	NÚMERO
Director departamental	1
Funcionarios del departamento	15
Funcionarios públicos	150
TOTAL	**166**

Elaborado por: Los Autores

Se define como la muestra a un porcentaje de la población a investigar, se la calculó en base a la siguiente fórmula:

$$M = \frac{\mathrm{P}}{(\mathrm{P}-1) * \mathrm{E}^2 + 1}$$

$$M = \frac{166}{(166-1) * 0.05^2 + 1}$$

$$M = \frac{166}{1.415}$$

$$\boldsymbol{M = 117}$$

La muestra quedó estructurada de la siguiente forma:

Cuadro 2. Muestra

FUNCIÓN	NÚMERO
Gerente	1
Funcionarios del departamento	15
Funcionarios públicos	101
TOTAL	**117**

Elaborado por: Los Autores

Las técnicas de investigación aplicadas fueron:

- Entrevista al director departamental y encuesta tanto a los funcionarios del departamento de sistemas como a los empleados públicos.

Los instrumentos utilizados fueron:

- Cuestionarios específicos para funcionarios públicos **(Ver Anexo A)**.
- Cuestionarios específicos para empleados del departamento de sistemas **(Ver Anexo B)**.
- Guía de entrevista para el Director **(Ver Anexo C)**.

RESULTADOS OBTENIDOS

Capítulo 4

RESULTADOS OBTENIDOS

Luego de realizada la investigación de campo se procedió a tabular sus resultados de las encuestas, los cuales se detallan a continuación:

Resultados de la encuesta realizada a los funcionarios públicos

Pregunta N° 1

¿En qué porcentaje cree usted que la gestión operativa se apoya en la tecnología de redes?

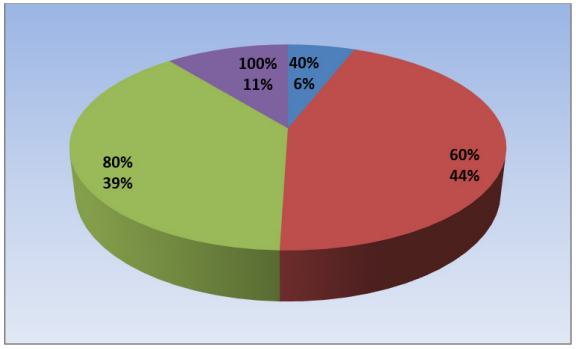
40%_____ 60%_____ 80%_____ 100%_____

Cuadro 3. Pregunta 1

Respuesta	Frecuencia	Porcentaje
40%	6	6%
60%	45	45%
80%	39	39%
100%	11	11%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 3



Elaborado por: Los Autores

Un 80% de los encuestados considera que la gestión operativa se apoya en la tecnología informática y en especial en las redes, esto denota una elevada dependencia tecnológica que tiene una institución moderna.

Pregunta N° 2

¿Existen algunos departamentos que están sin un enlace de red y sin poder compartir la información que ellos generan?

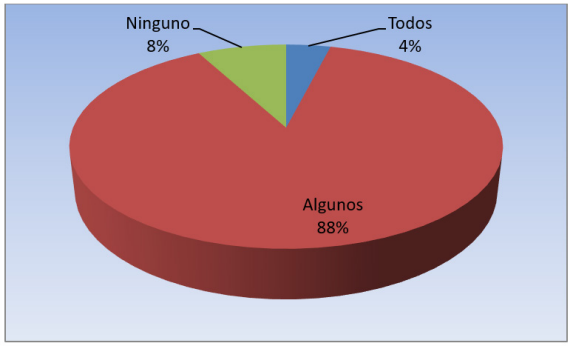
Todos_____ Algunos_____ Ninguno_____

Cuadro 4. Pregunta 2

Respuesta	Frecuencia	Porcentaje
Todos	4	4%
Algunos	89	88%
Ninguno	8	8%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 4



Elaborado por: Los Autores

Se puede apreciar que la mayoría considera que existen algunos departamentos que no están enlazados en la red pública, esto genera una demora en sus actividades operativas hasta realizar la transportación física de la documentación.

Pregunta N° 3

¿Se han producido pérdidas o deterioros de información por tener que ser transportada físicamente desde un sitio a otro?

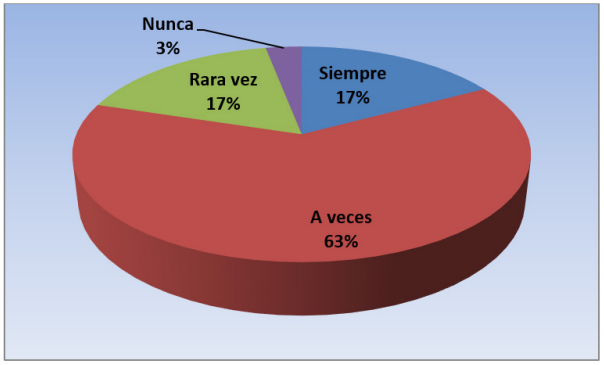
Siempre_____ A veces_____ Rara vez_____ Nunca_____

Cuadro 5. Pregunta 3

Respuesta	Frecuencia	Porcentaje
Siempre	17	17%
A veces	62	61%
Rara vez	17	17%
Nunca	5	5%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 5



Elaborado por: Los Autores

Aproximadamente un 70% considera que se han producido pérdidas o deteriores de la información, el momento de transportarla de manera física de un lugar a otro, generalmente se han dado alojamiento así como también ha quedado abierta la posibilidad de alteraciones del documento.

Pregunta N° 4.

¿Todos los departamentos de la institución disponen del servicio de Internet?

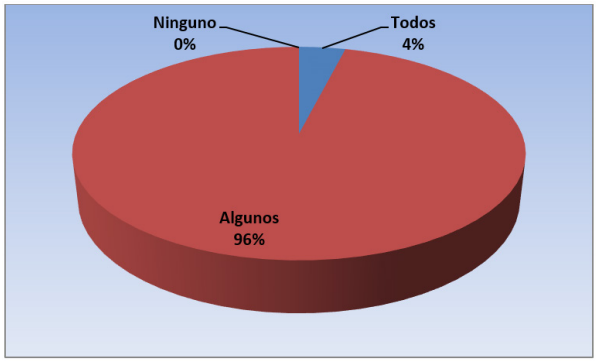
Todos_____ Algunos_____ Ninguno_____

Cuadro 6. Pregunta 4

Respuesta	Frecuencia	Porcentaje
Todos	4	4%
Algunos	97	96%
Ninguno	0	0%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 6



Elaborado por: Los Autores

No todos los departamentos disponen del servicio de Internet, esto se debe esencialmente a que no están enlazados en red. Claro que se debe mencionar que si se dota de este servicio de Internet deberá fijarse limitantes para ello. En departamentos como financiero y recursos humanos este servicio es imprescindible.

Pregunta N° 5.

¿Conoce usted si la institución ha utilizado la tecnología de redes para otras actividades como vigilancia y comunicación telefónica?

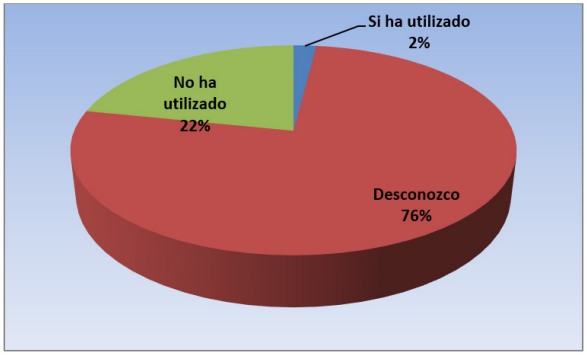
Si ha utilizado_____ Desconozco_____ No ha utilizado_____

Cuadro 7. Pregunta 5

Respuesta	Frecuencia	Porcentaje
Si ha utilizado	2	2%
Desconozco	77	76%
No ha utilizado	22	22%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 7



Elaborado por: Los Autores

La gran mayoría desconoce si la institución ha utilizado las redes para telefonía y vigilancia IP. Cabe señalar que estos son nuevos servicios y es por ello que muchos no conocen de esta posibilidad de uso.

Pregunta N° 6.

¿Cree usted que hay que ampliar y mejorar todo el sistema de redes que tiene la institución?

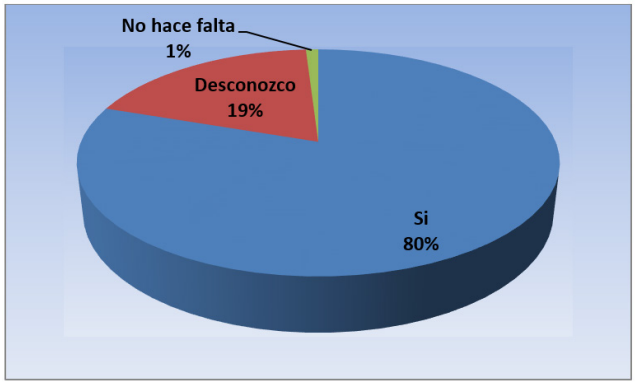
Si_____ No hace falta_____ Desconozco_____

Cuadro 8. Pregunta 6

Respuesta	Frecuencia	Porcentaje
Si	81	80%
Desconozco	19	19%
No hace falta	1	1%
Total	**101**	**100%**

Elaborado por: Los Autores

Figura 8



Elaborado por: Los Autores

La gran mayoría considera que debe mejorase el sistema de redes de la institución ya ello posibilitaría la optimización de determinados trámites en los cuales el usuario tiene que ir de una dependencia a otra.

Tabulación de resultados de la encuesta realizada al personal del departamento de sistemas.

Pregunta N° 1.

¿Todos los departamentos de la institución disponen del servicio de Internet?

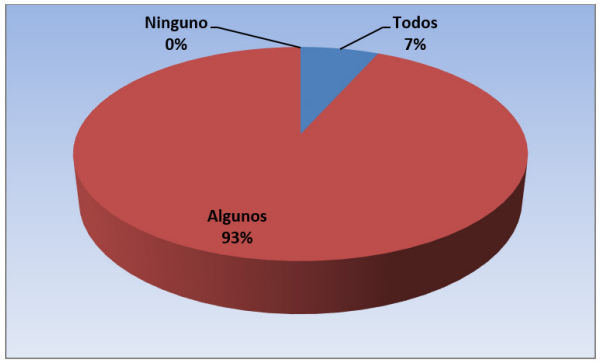
Todos_____ Algunos_____ Ninguno_____

Cuadro 9. Pregunta 1

Respuesta	Frecuencia	Porcentaje
Todos	1	7%
Algunos	14	93%
Ninguno	0	0%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 9



Elaborado por: Los Autores

Los funcionarios ratifican que no todos los departamentos están en red y que se hace necesaria la comunicación informática entre los mismos con el fin de optimizar los procesos.

Pregunta N° 2

¿Conoce usted si la institución ha utilizado la tecnología de redes para otras actividades como vigilancia y comunicación telefónica?

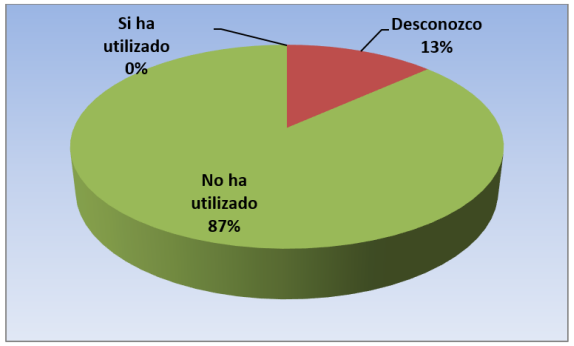
Si ha utilizado_____ Desconozco_____ No ha utilizado_____

Cuadro 10. Pregunta 2

Respuesta	Frecuencia	Porcentaje
Si ha utilizado	0	0%
Desconozco	2	13%
No ha utilizado	13	87%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 10



Elaborado por: Los Autores

La institución no ha utilizado las redes como elementos para telefonía y vigilancia IP.

Pregunta N° 3

¿Cree usted que hay que ampliar y mejorar todo el sistema de redes que tiene la institución?

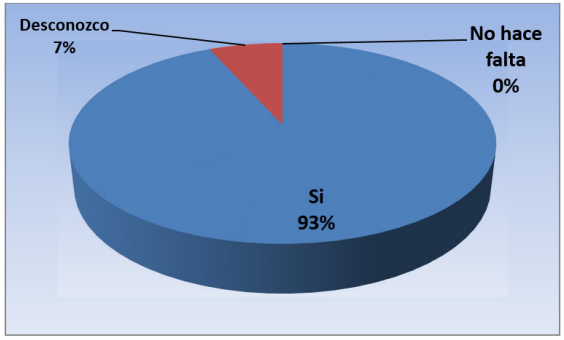
Si_____ No hace falta_____ Desconozco_____

Cuadro 11. Pregunta 3

Respuesta	Frecuencia	Porcentaje
Si	14	93%
Desconozco	1	7%
No hace falta	0	0%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 11



Elaborado por: Los Autores

Casi la totalidad de investigados considera que debe mejorarse el sistema de redes dentro de la institución porque no llega a todos los departamentos y consecuentemente los servicios son ineficientes.

Pregunta N° 4

¿Las redes existentes tienen los estándares de calidad requeridos para un cableado estructurado?

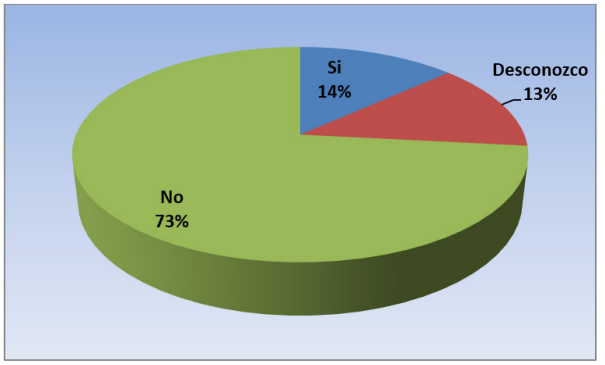
Si_____ No _____ Desconozco_____

Cuadro 12. Pregunta 4

Respuesta	Frecuencia	Porcentaje
Si	2	13%
Desconozco	2	13%
No	11	73%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 12



Elaborado por: Los Autores

Las redes que existen actualmente en la institución no cumplen con los estándares internacionales requeridos, esto implica que no se tiene una cableado estructurado certificado y llevado a cabo aplicando estándares internacionales.

Pregunta N° 5

¿Qué nivel de seguridades a nivel interno cree usted que tiene la institución?

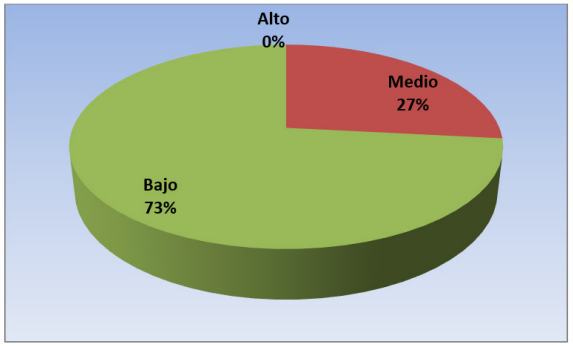
Alto_____ Medio_____ Bajo_____

Cuadro 13. Pregunta 5

Respuesta	Frecuencia	Porcentaje
Alto	0	0%
Medio	4	27%
Bajo	11	73%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 13



Elaborado por: Los Autores

El nivel de seguridades en redes internas es muy bajo, apenas una que otra red inalámbrica cuenta con una clave de acceso la cual nunca es renovada y no posee encriptación.

Pregunta N° 6.

¿Qué nivel de seguridades a nivel externo, cree usted que tiene la institución?

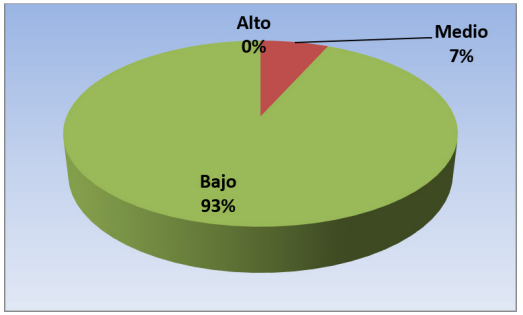
Alto_____ Medio_____ Bajo_____

Cuadro 14. Pregunta 6

Respuesta	Frecuencia	Porcentaje
Alto	0	0%
Medio	1	7%
Bajo	14	93%
Total	**15**	**100%**

Elaborado por: Los Autores

Figura 14



Elaborado por: Los Autores

El nivel de seguridades en redes externas es muy bajo, este implica que hay vulnerabilidades que necesariamente deben ser cubiertas y que ponen en riesgo el funcionamiento operativo de la institución.

Entrevista al Director del Departamento de Sistemas de una institución pública.

¿Cree usted que la institución dispone de todas las redes necesarias?
Lamentablemente no, existen muchos departamentos que están sin los enlaces respectivos, esto generalmente produce dificultades en las actividades operativas del departamento, así como en los procesos interdepartamentales, generalmente su efecto está en la demora por la trasportación manual de los datos de uno a otro.

¿Considera que es necesario un nuevo sistema de redes?
Bueno, nuevo no creo que sea necesario, lo que sí se necesita es que se complemente el actual con el enlace de algunos departamentos, e incluso no solo dentro de la ciudad sino en lugares cercanos.

¿Cómo está el nivel de seguridades en las redes públicas?
Aquí también se tienen algunas dificultades, lamentablemente el nivel de seguridades a nivel general es bastante bajo, también no hay una cultura de seguridad en todos los funcionarios públicos, por otro lado la institución no ha diseñado ningún plan de seguridad y peor aún haber invertido en él.

¿Considera usted que la carencia de redes afecta a la operatividad de la institución?
Definitivamente, la ausencia de redes en algunos departamentos de las instituciones públicas hace lentos los procesos y en determinados casos obligan a una transportación manual con todos los riesgos que esto implica, como daño de la información, pérdida y más. Personalmente considero que la imagen pública también está siendo afectada ya que la lentitud y la ineficiencia hace que se vea como una institución pública atrasada y sin mayor apoyo tecnológico.

CONCLUSIONES

- No todos los departamentos de la institución están en red y por ello es que algunos tampoco disponen del servicio de internet.
- Muchas operaciones no se pueden hacer rápidamente por falta del enlace de red e incluso la información generada se ha perdido o deteriorado el momento de transportarla físicamente de un sitio a otro.
- El cableado existente no está acorde a los estándares internacionales de un cableado estructurado.
- La institución no aprovecha sus redes para otro tipo de servicios como voz sobre IP y vigilancia.
- Los niveles de seguridad que existen en algunas redes especialmente inalámbricas son muy bajos.
- El nivel de seguridad a nivel de redes externas es prácticamente nulo.
- Se requiere complementar a toda la institución con un sistema de redes.

ANEXOS

ANEXOS

ANEXO A: Cuestionario para los funcionarios públicos

Pregunta N° 1. ¿En qué porcentaje cree usted que la gestión operativa se apoya en la tecnología de redes?

40%_____ 60% _____ 80% _____ 100% _____

Pregunta N° 2. ¿Existen algunos departamentos que están sin un enlace de red y sin poder compartir la información que ellos generan?

Todos_____ Algunos_____ Ninguno_____

Pregunta N° 3. ¿Se han producido pérdidas o deterioros de información por tener que ser transportada físicamente desde un sitio a otro?

Siempre_____ A veces_____ Rara vez_____ Nunca_____

Pregunta N° 4. ¿Todos los departamentos de la institución disponen del servicio de Internet?

Todos_____ Algunos_____ Ninguno_____

Pregunta N° 5. ¿Conoce usted si la institución ha utilizado la tecnología de redes para otras actividades como vigilancia y comunicación telefónica?

Si ha utilizado_____ Desconozco_____ No ha utilizado_____

Pregunta N° 6. ¿Cree usted que hay que ampliar y mejorar todo el sistema de redes que tiene la institución?

Si_____ No hace falta_____ Desconozco_____

ANEXO B: Cuestionario para el personal del departamento de sistemas.

Pregunta N° 1. ¿Todos los departamentos de la institución disponen del servicio de Internet?

Todos_____ Algunos_____ Ninguno_____

Pregunta N° 2. ¿Conoce usted si la institución ha utilizado la tecnología de redes para otras actividades como vigilancia y comunicación telefónica?

Si ha utilizado_____ Desconozco_____ No ha utilizado_____

Pregunta N° 3. ¿Cree usted que hay que ampliar y mejorar todo el sistema de redes que tiene la institución?

Si_____ No hace falta_____ Desconozco_____

Pregunta N° 4. ¿Las redes existentes tienen los estándares de calidad requeridos para un cableado estructurado?

Si_____ No_____ Desconozco_____

Pregunta N° 5. ¿Qué nivel de seguridades a nivel interno cree usted que tiene la institución?

Alto_____ Medio_____ Bajo_____

Pregunta N° 6. ¿Qué nivel de seguridades a nivel externo, cree usted que tiene la institución?

Alto_____ Medio_____ Bajo_____

ANEXO C: Guía de entrevista al Director del departamento de sistemas.

Pregunta N° 1. ¿Cree usted que la institución dispone de todas las redes necesarias?

Pregunta N° 2. ¿Considera que es necesario un nuevo sistema de redes?

Pregunta N° 3. ¿Cómo está el nivel de seguridades en las redes de las instituciones públicas?

Pregunta N° 4. ¿Considera usted que la carencia de redes afecta a la operatividad de la institución?

ACERCA DE LOS AUTORES

LUIS ISAÍAS BASTIDAS ZAMBRANO

Ingeniero en Sistemas, desde el año 2007 comienza su vida profesional en el sector público poniendo en práctica sus conocimientos adquiridos en el G.A.D.M. de Babahoyo, llegando a ocupar el cargo de Coordinador General de Contratación Pública. Continuando con sus aspiraciones personales siguió ampliando sus conocimientos; y es así que obtiene los títulos de Diploma Superior en Sistemas de Información Empresarial, Especialista en Redes de comunicación de Datos y Magíster en Informática Empresarial hasta el año 2013, además obtiene un Diploma en Docencia en la Educación Universitaria, desde septiembre del 2014 empieza como docente de la Universidad Técnica de Babahoyo, ha participado como ponente en congresos y escrito artículos en el área de la informática y en la actualidad está cursando un Doctorado en Ciencias Informáticas en la Universidad Nacional de la Plata - Argentina.

EVELYN CONCEPCIÓN RUÍZ PARRALES

Profesional de la ciudad de Babahoyo, obtiene su título Tecnólogo en Informática-Análisis de Sistemas en el Instituto Tecnológico Superior Babahoyo, en Abril del 2006, y en Octubre del 2007 obtiene el Título de Ingeniera en Sistemas en la Universidad Técnica de Babahoyo, Facultad de Administración Finanzas e Informática, Comienza su vida profesional en el sector público en la Ilustre Municipalidad de Babahoyo, durante 7 años 8 meses, poniendo en práctica sus conocimientos adquiridos. Además, continuando con sus aspiraciones siguió ampliando sus conocimientos mediante capacitaciones continuas; y es así donde en el año 2012, se inscribe en el Masterado de Administración de Empresas, obteniendo su título de Magíster en el año 2014, y en el año Marzo del 2015, aplica como Docente de la Universidad Técnica de Babahoyo–Facultad de Ciencias de la Salud, y en la actualidad está cursando un Doctorado en Ciencias Informáticas en la Universidad Nacional de la Plata- Argentina.

JOFFRE VICENTE LEÓN ACURIO

PhD candidato en la Universidad Nacional de la Plata, Argentina, Magíster en Informática Empresarial, Especialista en Redes de Comunicación de Datos, Diplomado Superior en Sistemas de Información Empresarial (Universidad Regional Autónoma de Los Andes). Ingeniero en Sistemas (Universidad Técnica de Babahoyo), Docente especializado en el área de Seguridad Informática y responsable de la asignatura de Auditoría en Sistemas, Certificación de Auditor Interno ISO 27001. Consultor de Tecnologías de la Información, Coaching Profesional en temas relacionados en Seguridad Informática, Docente Titular Agregado de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, Editor en Jefe del Centro de Investigación y Desarrollo Profesional y CIDEPRO EDITORIAL, Editor en Jefe de la Revista Pro Sciences: Revista de Producción, Ciencias e Investigación, ha participado en congresos nacionales e internacionales y publicado artículos de alto impacto relacionados a la seguridad informática.

REFERENCIAS BIBLIOGRÁFICAS

- ACISSI, 2011, “Seguridad Informática”, Ediciones ENI, Primera edición, Barcelona – España.
- ACISSI, 2011, “Seguridad Informática”, Ediciones ENI, Primera edición, Barcelona – España.
- ALDEGANI, Gustavo, 2003 “Seguridad Informática.” MP Ediciones. Argentina.
- AREITIO Javier, 2008, “Seguridad de la información”, Editorial Paraninfo, Primera Edición, Madrid-España.
- ATELIN Philippe, 2006, “Redes Informáticas”, ediciones ENI, Primera Edición, Barcelona-España.
- ATELIN Philippe, 2006, “Redes Informáticas”, ediciones ENI, Primera Edición, Barcelona-España.
- BAETA Jesús, “Seguridad Informática en línea”, http://es.scribd.com/doc/95069532/Seguridad-Informatica.
- BARCELÓ José, 2008, “Protocolos y Aplicaciones de Internet”, Editorial UOC, Primera edición, Barcelona – España.
- CABEZAS Luis, GOZALES Francisco “Redes Inalambricas”, Editorial Anaya Interactiva, Madrid-España, Segunda edición, 2009.
- CALDER Alan, 2009, “Implementig information Security Based on ISO 27001/ISO 270002” Tercera Edición, Ontario-Canada.
- CARBALLAR José, 2010, “Wi-Fi, lo que se necesita conocer”, Editorial Alfaomega, México-México, Primera edición.

- DERFLER Frank, “Redes Wan & Lan”,Prentice-Hall, Madrid-España, Segunda Edición, 2008.
- Eduardo Jorge Arnoletto “La Gestión Organizacional en los Gobiernos Locales” http://www.eumed.net/libros/2010d/777/gestion%20operativa%20o%20gestion%20hacia%20abajo.htm
- Eduardo Jorge Arnoletto y Ana Carolina “UN APORTE A LA GESTIÓNPUBLICA” http://www.eumed.net/libros/2009b/550/La%20gestion%20operativa.htm
- GARCÍA Alberto, “Redes Wi-Fi”, Editorial Anaya Multimedia, Madrid-España, Segunda edición, 2008.
- HAYES Jim, ROSENBERG Paul, 2009, “Cableado de redes para voz, video y datos. Planificación y construcción”, Editorial CENGAGE Learning, Buenos Aires, Tercera edición.
- MILLAN Joseph, “Domine las redes P2P”, Editorial Alfao, México - México, 2007
- MOLINA Francisco, “Redes Locales”, Editorial Microinformatica, Madrid-España, Segunda Edición, 2009.
- RAYA José, RAYA Elena, (2006), “Redes Locales”, Editorial Alfaomega Ra-Ma, Madrid-España, Tercera edición.
- TANENBAU Andrews, (2004), “Redes de Computadoras”, Prentice-Hall, Madrid-España.
- TERÁN David, (2010), “Redes Convergentes”, Editorial Alfaomega, Madrid-España, Primera edición.

Centro de Investigación y Desarrollo Profesional
Generador de Conocimientos...

ISBN: 978-9942-792-89-1

CIDE Editorial