Decanato de Ingeniería e Informática
Escuela de Informática

"Análisis de modelo de enseñanza multilenguaje en línea de la empresa SOTO DOMINICANA en la Ciudad de Santo Domingo, 2014."

Sustentantes:

José Jail Soto	**2006-0218**
Ramón Castillo	**2007-1328**
Jhosuamel Serrata	**2009-1631**

Asesor:
Ing. Santo Rafael Navarro

Monografía para Optar por el Título de:
Ingeniero en Sistemas de Computación

Distrito Nacional, República Dominicana
Agosto, 2014

“Análisis de modelo de enseñanza multilenguaje en línea de la empresa SOTO DOMINICANA en la Ciudad de Santo Domingo, 2014.”

ÍNDICE GENERAL

CAPÍTULO 4

CAPITULO 5

CAPÍTULO 6

CAPÍTULO 7

AGRADECIMIENTOS

Gracia a Dios Todo Poderoso, por darme la bendición de poder culminar este gran capítulo en mi vida, por darme la Fe y Esperanza que he tenido, por iluminar mi mente y camino para poder completar esta gran meta: concluir mis estudios universitarios. Gracias Dios.

Agradecer enormemente a mi Padre **José Gregorio Soto** siempre estuviste ahí para brindarme tu apoyo en todas las etapas de mi vida. Tu Fe en mí me dio las fuerzas necesarias para abrirme paso en la vida y enseñarme que lo que se empieza se debe terminar. Gracias por enseñarme a como caminar en esta vida.

A mi madre, **Saudí Beatriz Peña** porque que siempre sentí ese apoyo maternal para seguir adelante con este proyecto de vida, supiste mantener tu esperanza y Fe en mí y me diste fuerzas para terminar mis estudios universitarios. Eres unos de los pilares en mi vida que siempre me apoyo en mis momentos difíciles de carrera para no darme por vencido.

Debo de agradecer a **todos Mis familiares** por apoyarme siempre en las cosas necesarias para poder lograr mis objetivos universitarios.

A mis compañeros de Monográfico, **Ramón Castillo y Jhosuamel Serrata** por todo su apoyo y colaboración para culminar este maravilloso proyecto que hoy nos coloca como profesionales ante la sociedad.

José Jail Soto

DEDICATORIAS

Dedicatoria

A la **Universidad APEC** por permitirme ser parte de su familia y a través de su excelente equipo de maestros y a todos aquellos que en algún momento perdieron la fe en mí.

A mi asesor **Ing. Santos Navarro**, por su apoyo y colaboración en todo el trayecto de nuestra tesis.

José Jail Soto

AGRADECIMIENTOS

Gracia a Dios Todo Poderoso, por darme la bendición de poder culminar este gran capítulo en mi vida, por darme la Fe y Esperanza que he tenido, por iluminar mi mente y camino para poder completar esta gran meta: concluir mis estudios universitarios. Gracias Dios.

Agradecer enormemente a mi Padre **José A. Serrata** siempre estuviste ahí para brindarme tu apoyo en todas las etapas de mi vida. Tu Fe en mí me dio las fuerzas necesarias para abrirme paso en la vida y enseñarme que lo que se empieza se debe terminar. Gracias por enseñarme a como caminar en esta vida.

A mi madre, **Emelinda M. Ramos** porque que siempre sentí ese apoyo maternal para seguir adelante con este proyecto de vida, supiste mantener tu esperanza y Fe en mí y me diste fuerzas para terminar mis estudios universitarios. Eres unos de los pilares en mi vida que siempre me apoyo en mis momentos difíciles de carrera para no darme por vencido.

Debo de agradecer a **todos Mis familiares** por apoyarme siempre en las cosas necesarias para poder lograr mis objetivos universitarios.

A mis compañeros de Monográfico, **Ramón Castillo y José Jail Soto** por todo su apoyo y colaboración para culminar este maravilloso proyecto que hoy nos coloca como profesionales ante la sociedad.

DEDICATORIAS

Dedicatoria

A la **Universidad APEC** por permitirme ser parte de su familia y a través de su excelente equipo de maestros, adquirir todos los conocimientos necesarios para mi formación universitaria.

A mi asesor **Ing. Santos Navarro**, por su apoyo y colaboración en todo el trayecto de nuestra tesis.

AGRADECIMIENTOS

Primero DIOS por darme la vida, por ayudarme y permitir lograr mis sueños, porque sin el nada hubiese sido posible.

A mis padres Ramón **Dilone y Brígida Chery** por su apoyo, tanto moral como económico, gracias a ello pude seguir día a día luchando por alcanzar mis metas. Esto es más de ustedes que mío ya que al igual que yo esta era una de sus metas.

A mis hermanos, porque a pesar de que no siempre estamos de acuerdo en un sin número de ocasiones puedo decir que siempre me han apoyado incondicionalmente en todas mis fases.

A mi hija **Tiffany Marie** que es mi motivación principal, la que hace que todos los días sea una mejor persona y de lo mejor de mí en todo lo que haga, a ti mi reina que eres más que mis pensamientos te lo dedico todo.

A mis compañeros de estudia **Jhosuamel Serrata y José Jail Soto** quienes desde el primer día han sido de gran motivación y ayuda para mí. Gracias muchachos…

Ramón Antonio Castillo

DEDICATORIA

A mi Madre por siempre apoyarme, por guiarme y aconsejarme. Te dedico esto porque desde el primer día haz estado apoyándome en todo los aspectos de mis estudios y mi vida.

A mi Padre por siempre estar disponible para mí, no importa las circunstancias, por tu apoyo y motivación además de económico. Sin ti no fuera posible esto ya que siempre me motivaste a seguir adelante.

A mi Hija, tu que eres mi mayor motivación, te dedico no solo esto sino todo lo que haga en mi vida, Te amo.

Ramón Antonio Castillo

RESUMEN EJECUTIVO

Debido al aumento constante de la tecnología la educación ha evolucionado y la necesidad de realizar capacitaciones a distancia ha crecido con el tiempo, Presentamos una solución que permite romper las barreras del idioma de las capacitaciones en líneas utilizando un sistema de traducción en tiempo real en video conferencias que pueda ser utilizado en cualquier dispositivo.

Esta investigación tiene como alcance el análisis de la remodelación del data center de la empresa SOTO DOMINICANA. Este análisis cuenta con un levantamiento de requerimientos que exigen un data center, dentro de un marco temporal comprendido de mayo a agosto del año 2014. Dejando fuera de rango el desarrollo y la implementación de la solución planteada.

La solución que presentamos para el problemático mundo de las capacitaciones online y la incertidumbre que produce no saber idiomas está comprendida por un conjunto de elementos que operan en un data center servidores, sistema de enfriamiento, base de datos en SQL Server, aplicación web y soluciones móviles para Android, Windows Phone y IOS, todos estos optimizados para trabajar con un sistema de traducción en línea en tiempo real. Por último un conjunto de herramientas de inteligencia de negocio para poder percibir los resultados que brinda nuestra solución, tanto operativa como financieramente.

El principal objetivo es conseguir romper las barreras del idioma en el aprendizaje a distancia, proporcionar una herramienta útil para la sociedad y apoyar el desarrollo de la educación proyectar la mejora continua del sistema a través de la satisfacción de los estudiantes.

INTRODUCCIÓN

SOTO DOMINICANA es una empresa dedicada a impartir clases mediante tecnológicos enfocada en facilitar al estudiante al momento de impartir un curso, comprobar la disponibilidad y cantidad de los cursos disponibles.

En los grandes avances tecnológicos de los últimos años, la tecnología ha jugado un papel muy importante en la forma de implementar cursos en líneas para los estudiantes. Dentro de algunas de las ventajas de la tecnología están la ventaja competitiva, la tecnología como herramienta, una mejor gestión de los datos y una mayor seguridad garantizando confidencialidad, integridad y una alta disponibilidad de la información.

La capacitación en línea no es más que un concepto tecnológico que se basa en que el software y el hardware no están en el PC o equipos del usuario, sino que están ubicado en un centro de datos que permite a los usuarios poder acceder a las aplicaciones y servicios disponibles a través de Internet de una forma sencilla y cómoda sin tener que depender de servidores para almacenar la información.

Esta investigación tendrá como objetivo general: la implementación de un traductor en línea para romper las barreras del idioma al momento de ofrecer un curso en línea en la Ciudad de Santo Domingo, 2014.

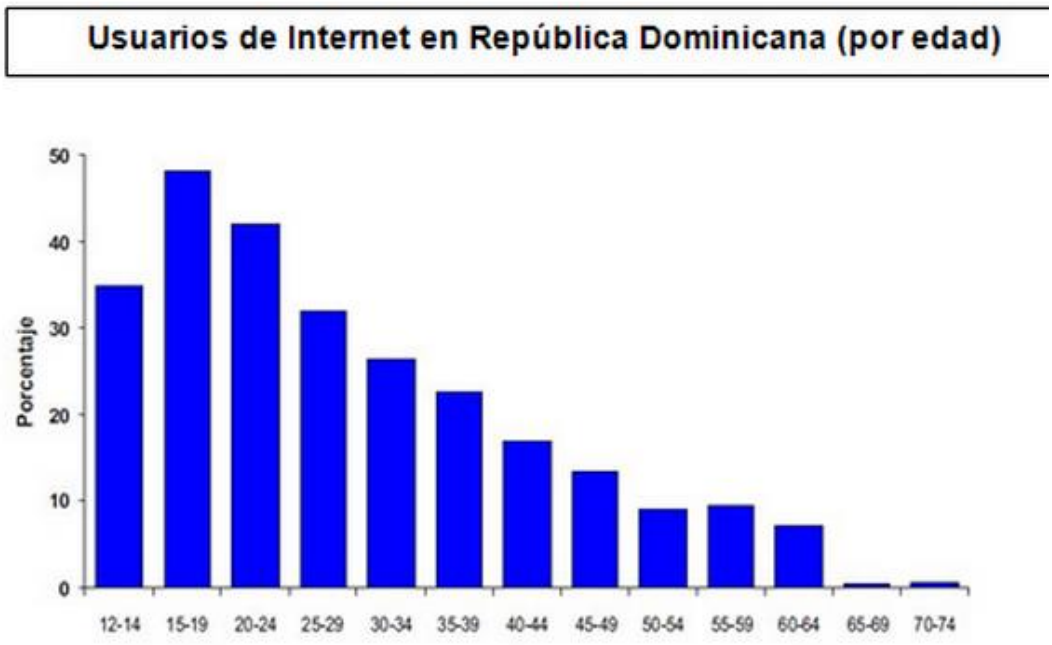
Este será alcanzado mediante los siguientes objetivos específicos: Detallar los servicios que ofrece el Centro De Capacitación. Describir el funcionamiento del modelo Web. Implementar sistemas de seguridad aplicada, tanto en la web Como dentro de la empresa. Implementar inteligencia de negocio en la web a través de la empresa. Diseñar modelo de plantilla basado en estructura y contenido de datos. Identificar el modelo de base de datos. Describir la estructura, funcionamiento y servicio de la Empresa SOTO DOMINICANA.

PLANTEAMIENTO DEL PROBLEMA

La empresa SOTO DOMINICANA, tiene por mandato de ley la responsabilidad de impulsar el desarrollo de los Recursos Humanos que laboran en el área financiera del Estado. Para cumplir con su misión la empresa SOTO DOMINICANA ha desarrollado diversas capacitaciones en materia fiscal a nivel nacional, sin embargo, por razones presupuestaria no ha podido extender su presencia en todo el país.

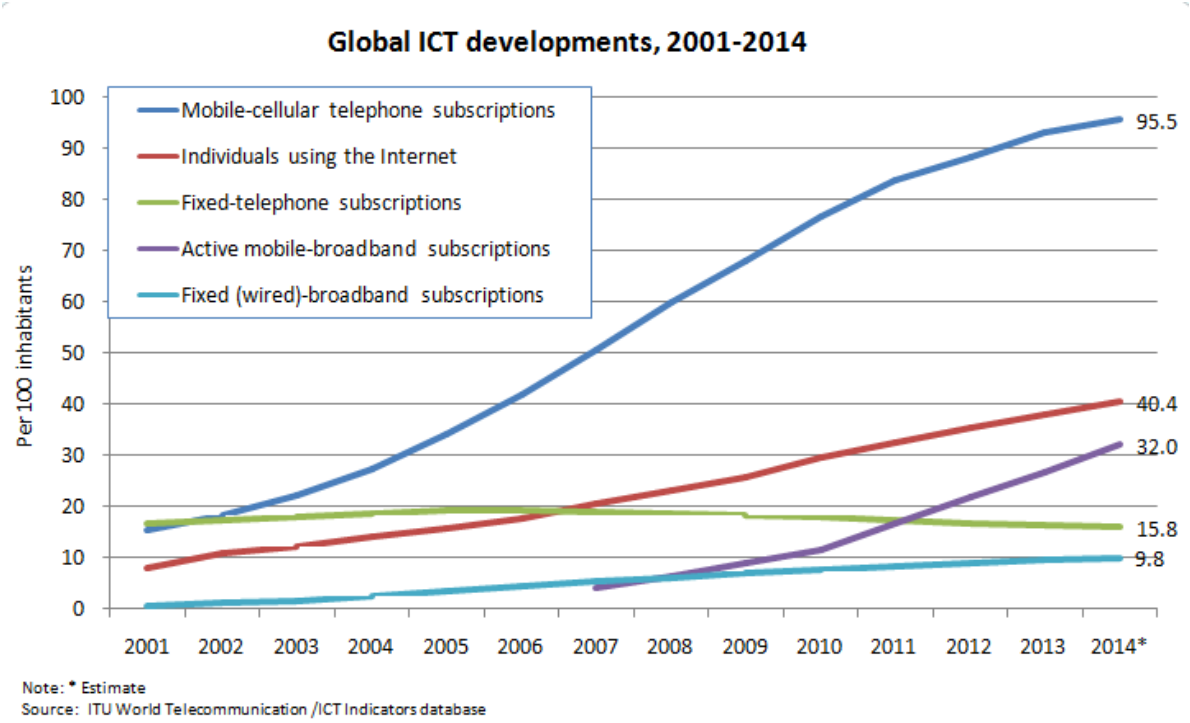
Un estudio demuestra que todo el que estudió en una **universidad en la República Dominicana** entre el 2004 y 2005, aproximadamente, conoció y vivió de mala manera el proceso tortuoso de ir en horas de la madrugada para obtener el registro de las asignaturas a estudiar en un determinado cuatrimestre, pues los procesos de selección de materias, aunque se utilizaban computadoras en muchos casos, había que hacerlo de manera presencial. Sin embargo, en las principales **universidades dominicanas,** los estudiantes universitarios ya se inscriben a través de internet, revisan sus notas y también reciben las actualizaciones y correos electrónicos para enviar las informaciones por esta vía y que no tengan que estar haciendo largas filas para procesos cotidianos.

Otro estudio realizado en nuestro país en el año 2007 demuestran que el listado nominal de votantes de 18 y 29 años que utilizan internet es de 1, 154,256 usuarios.



Fuente: Oficina Nacional de Estadísticas. Encuesta Nacional de Hogares de Propósitos Múltiples (ENHOGAR)2007

En el mismo orden se muestran estadísticas sobre disponibilidad y uso de tecnologías de Información y Comunicación. En las Américas, casi dos de cada tres personas utilizará Internet a finales de 2014, lo que representa la segunda mayor tasa de penetración después de Europa. En Europa, la penetración de Internet alcanzará el 75 por ciento (es decir, tres de cada cuatro personas) a finales de 2014 y será la más alta a nivel mundial. Un tercio de la población de Asia y el Pacífico estará en línea a finales de 2014 y cerca del 45 por ciento de los usuarios de Internet totales procederán de esta región.



Fuentes: ITU Statistics (http://www.itu.int/ict/statistics) Global ICT developments, 2001-2014

A raíz de lo anterior, una de las grandes problemáticas es la convergencia de los dispositivos de los clientes para tener acceso a la plataforma en línea, ya que hasta ahora solo está enfocado para trabajar con PC, dejando un lavo la revolución de los dispositivos móvil. Otro aspecto fundamental es el mal diseño a nivel de infraestructura de las bases de datos. No obstante la seguridad juega un papel importante y en el levantamiento información que obtuvimos de la entrevista al departamento de TI de la empresa Soto Dominicana, nos dimos cuenta que no poseen una dmz (Zona Desmilitarizada) para publicar los servicios web teniendo altas vulnerabilidades a nivel de seguridad.

Una limitante de la capacitación en línea es la barrera del idioma, que impide que las formaciones ofrecidas por la empresa Soto Dominicana puedan expandirse sin

ninguna frontera, tenemos un caso de estudiantes que pertenecen Haití donde manejan el idioma inglés y francés más que el español, siendo esto una debilidad del sistema de capacitación actual que no posee traducciones en tiempo real para satisfacer la demanda de estos sectores.

Por otro lado, los sistemas de información y equipos informáticos tienen sistema operativo descontinuados por los fabricantes como el caso de windowsxp, altos problemas de seguridad por una mala planificación en la infraestructura tecnológica, descentralización de los procesos internos entre departamentos que tienen flujos de trabajo compartidos.

OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

- Implementar un sistema basado en un nuevo método de enseñanza en línea, que incorpore un traductor en tiempo real para permitir a los clientes tomar curso a distancias sin importar el idioma.

- Implementar un método de enseñanza mediante un sistema multilenguaje en línea que Permita al usuario tomar entrenamientos y capacitaciones sin importar las barreras que se presenten a nivel de idiomas

OBJETIVOS ESPECÍFICOS

- Implementar un nuevo sistema de traducción en tiempo real para la capacitación en línea.

- Describir la arquitectura para el diseño del ambiente de virtualización de servidores y escritorios.
- Centralizar todo los sistemas virtualizados y datos de la empresa.
- Segmentar el tráfico en VLANs (Virtual LAN Área Network) para dividir el acceso de la red corporativa y la red de estudiante.
- Aprovechar los recursos de hardware para minimizar el impacto del consumo eléctrico.
- Utilizar la inteligencia de negocio (BI) para la administración y análisis de los datos existente de la empresa.
- Ofrecer nuevas alternativas tecnológicas con virtualización de escritorio para remodelar los laboratorios con tecnología de punta.
- Ahorrar espacio y energía eléctrica en el data center, centralizar la administración de los servidores, contar con una imagen del sistema que pueda ser recuperada ante cualquier cambio que se haga en los servidores.
- Mantener la encriptación e integridad en la comunicación cliente-servidor
- Realizar replicación de los servicios críticos de la empresa para continuidad del negocio en caso de falla.
- Realizar copias de seguridad tantos en cintas como en la nube para salvaguardar la información fuera de la empresa garantizando que en caso de cualquier desastre en la empresa la data está segura.
- Mantener las bases de datos de la plataforma virtual siempre en línea aplicando modelos de alta disponibilidad y tolerancia a fallos.
- Brindar al cliente el acceso a los servicios y capacitaciones de la empresa tomando en cuenta la revolución de los dispositivos móviles.

Capítulo 1

Define la Empresa y a que está dedicada. Explica la misión de la misma en el mercado y a quién va dirigida. Explica también la visión de la empresa, hacia donde quiere llegar y conseguir la total satisfacción de los clientes. Además de los objetivos.

1.1 Historia de la Empresa SOTO DOMINICANA

La Empresa SOTO DOMINICANA tiene la responsabilidad de impulsar el perfeccionamiento de los recursos humanos que participen en los procesos de política y gestión fiscal en todo ámbito del Sector Público, apoyando las reformas emprendidas por el Gobierno con el fin de dotar a la Administración Pública de una acción más eficaz y oportuna en la dirección de la gestión financiera, a través de un alto nivel de especialización.

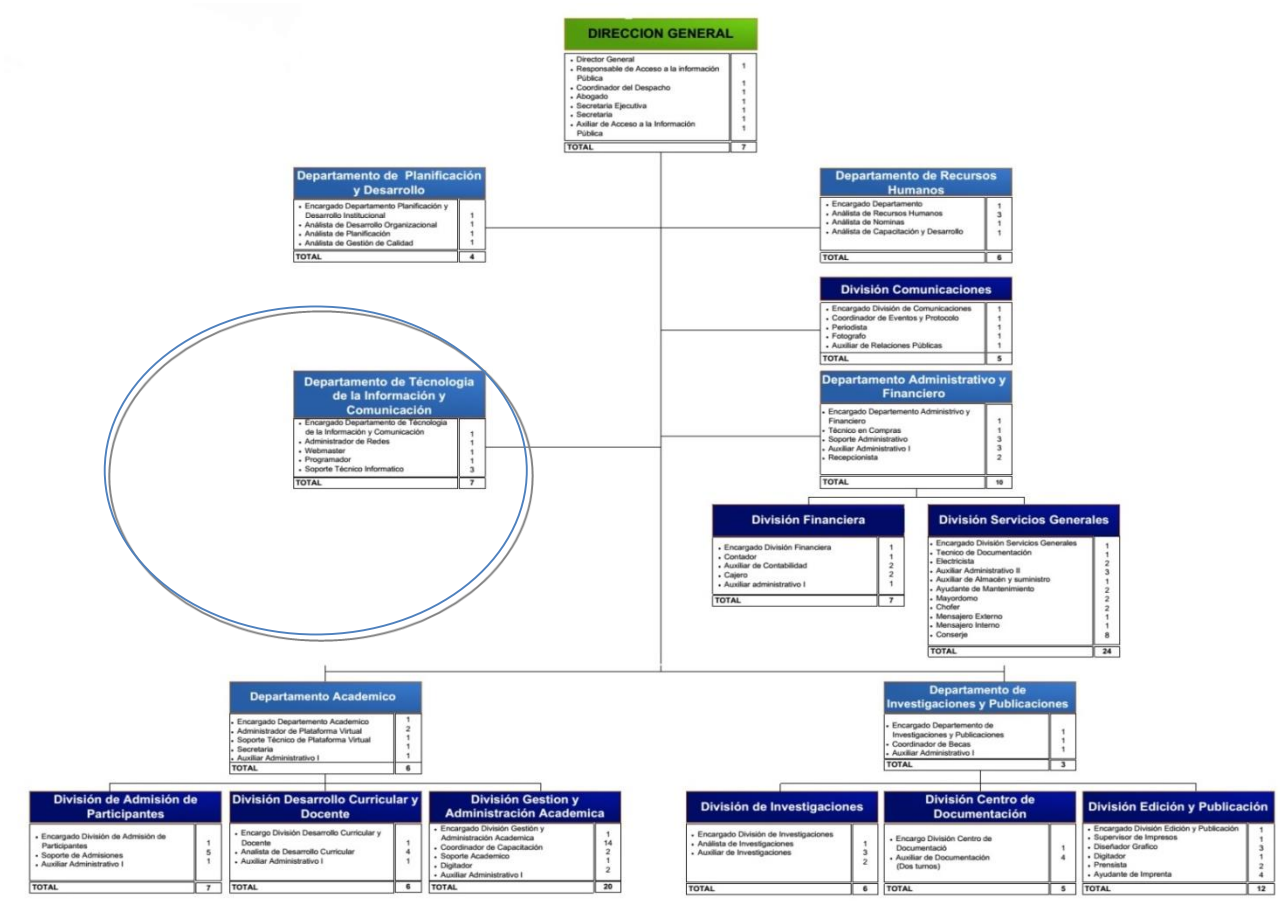


Figura 1 Organigrama de la Empresa

Fuente: (Soto, 2014)

1.2 Misión

Capacitar y adiestrar los recursos humanos que participan en los procesos de política y gestión fiscal a fin de garantizar su desempeño para que contribuyan con el fortalecimiento y modernización de la Administración Financiera del Estado y ofrecer a los contribuyentes y público en general orientación sobre la materia fiscal.

1.3 Visión

Constituirse en un órgano rector de la capacitación en el área fiscal que contribuya al desarrollo del país, a través de la capacitación, promoción de la investigación, profesionalización y participación comprometida con la modernización del estado.

1.4 Valores

- ✓ Calidad
- ✓ Trabajo en equipo
- ✓ Compromiso
- ✓ Ética profesional
- ✓ Innovación
- ✓ Alianzas estratégicas

CAPÍTULO 2

Se desarrolla una investigación de los tipos de enlaces privados, su historia y evolución al pasar de los años.

LOS ENLACES PRIVADOS ANTES DE LA APARICIÓN DE LAS REDES PRIVADAS VIRTUALES.

2.1 INTRODUCCIÓN

Desde el principio de los tiempos, la humanidad ha tenido la necesidad de comunicarse. Paralelamente también ha existido la necesidad de hacerlo de manera privada, es decir que el mensaje sólo le llegue a determinados receptores. En las redes de comunicaciones pasa exactamente lo mismo. En especial el sector corporativo siempre ha requerido la implementación de enlaces privados para transportar de forma segura toda su información confidencial.

2.2 ENLACES PRIVADOS

Los enlaces privados se caracterizan por brindar seguridad en la transmisión de datos de extremo a extremo. Se valen siempre de una red de transmisión (en algunos casos también existe una red de conmutación) para conectar las partes. Estos enlaces pueden ir desde los 9600bps (en el caso de una conexión conmutada usando un modem análogo de 9600bps) hasta el orden de los Gigabps (usando redes ópticas, con equipos de transporte de última generación o multiplexores DWDM).

2.3. TIPOS DE ENLACES PRIVADOS

Las redes de computadores se han valido de los enlaces privados para interconectarse a través de grandes distancias geográficas. Antes de la aparición de las VPN habían existido sólo dos tecnologías de enlaces WAN, los enlaces

dedicados, y los enlaces conmutados. Dentro de los enlaces dedicados caben topologías tales como Clear Channel, FrameRelay y ATM. Aunque se sabe que FrameRelay usa conmutación de paquetes y ATM usa conmutación de celdas, en este trabajo se clasifican como enlaces dedicados, porque en últimas para el usuario la conmutación es transparente. Dentro de los enlaces conmutados están los análogos que van desde 2400bit/s hasta los 56 kbit/s y los digitales RDSI de 64 kbit/s y 128 kbit/s.

2.3.1. ENLACES DEDICADOS

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) o de transporte y conmutación (Capa 1 y 2). Los primeros son comúnmente llamados enlaces Clear Channel y los segundos son enlaces FrameRelay o ATM.

2.3.1.1. CLEAR CHANNEL

Son enlaces donde sólo interviene la red de transporte del proveedor de servicios. Para el mercado corporativo comúnmente van desde los 64 kbit/s hasta los 2048 kbit/s. Los enlaces Clear Channel ofrecen un rendimiento efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo. Por lo general, la compañía (o cliente en general) debe tener un puerto disponible DTE que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el

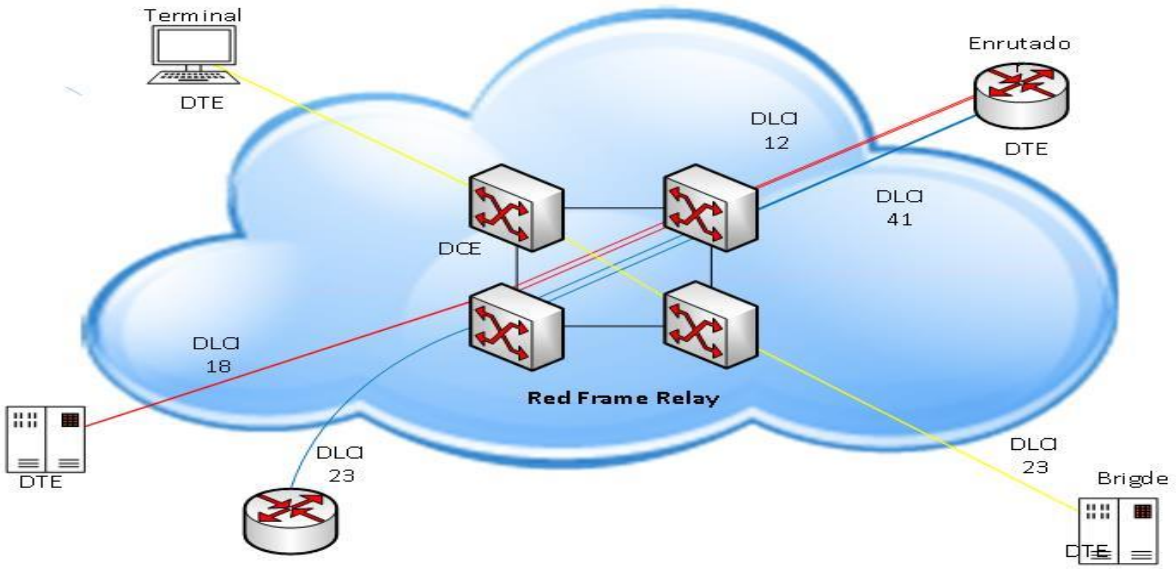
proveedor. Típicamente la mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente son enrutadores o switches de nivel 3. Y son estos, los que se encargan de manejar los niveles 2 y 3. Vale la pena aclarar, que los enlaces Clear Channel fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz PCM de los distintos operadores de telefonía locales, nacionales e internacionales. Como era de esperarse, por provenir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente.

2.3.1.2. FRAME RELAY

FrameRelay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo de referencia OSI. FrameRelay fue diseñado originalmente para trabajar con redes ISDN. FrameRelay es una tecnología de conmutación de paquetes, que permite compartir dinámicamente el medio y por ende el ancho de banda disponible. La longitud de los paquetes es variable para hacer más eficiente y flexible las transferencias de datos. Estos paquetes son conmutados por varios segmentos de la red hasta que llegan hasta el destino final. Todo el acceso al medio en una red de conmutación de paquetes es controlado usando técnicas de multiplexación estadística, por medio de las cuales se minimizan la cantidad de demoras y/o colisiones para acceder al medio.

Ethernet y Token Ring son los protocolos de redes LAN más usados. Todas las ventajas que ofrecen los medios de hoy día, han posibilitado a FrameRelay ofrecer un alto desempeño y una gran eficiencia de transmisión. Los equipos que

se usan en una red FrameRelay se pueden dividir en dos categorías: Equipos Terminales de Datos (DTEs) y Equipos Terminales de Circuitos de Datos (DCEs).



Ejemplo de asignación de valores DLCI en una red frame Relay

Fuente: (Soto, 2014)

Figura 2. Ejemplo de Asignación de valores DLCI en un Red Frame Relay.

La figura 1 ilustra la ubicación de los DTEs y los DCEs en un red Frame Relay. Los DTEs son generalmente considerados equipos terminales de una red específica y típicamente son enrutadores, computadores personales, terminales o bridges. Estos equipos se localizan en las premisas del cliente y en la mayoría de los casos son propiedad de los mismos. Los DCEs son dispositivos normalmente propiedad del carrier. El propósito de los equipos DCEs es proveer o generar

señales de reloj y conmutar los paquetes de la red. Por lo general, son llamados packet switchs o conmutadores de paquetes.

2.3.1.3. ATM (ASYNCHRONOUS TRANSFER MODE)

El Modo de Transferencia Asíncrono (ATM) es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, tales como voz, video y datos usando técnicas de conmutación de celdas pequeñas de tamaño fijo. Las redes ATM son, al igual que las redes FrameRelay, orientadas a conexión.

ATM es una tecnología de multiplexación y de conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos megabits por segundo hasta cientos de gigabits por segundo. Su naturaleza asíncrona, hace de ATM una tecnología más eficiente que las síncronas tales como TDM. En TDM a los usuarios se les asigna un timeslot, y ningún otro cliente puede transmitir en ese timeslot así el propietario no esté transmitiendo. Esto hace que la red no sea muy eficiente.

Una red ATM está compuesta de dos tipos de dispositivos: los switches ATM y los terminadores ATM. Un switch ATM es el encargado de recibir las celdas entrantes provenientes de otro switch ATM, leer y actualizar las cabeceras de cada celda y de direccionar la celda hasta que llegue a su destino final. Los terminadores ATM

(o sistemas finales) son dispositivos que están provistos de un adaptador de interfaz de red ATM, por lo general están en las premisas del cliente

El Modo de Transferencia Asíncrono (ATM) es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, tales como voz, video y datos usando técnicas de conmutación de celdas pequeñas de tamaño fijo. Las redes ATM son, al igual que las redes FrameRelay, orientadas a conexión.

ATM es una tecnología de multiplexación y de conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos megabits por segundo hasta cientos de gigabits por segundo. Su naturaleza asíncrona, hace de ATM una tecnología más eficiente que las síncronas tales como TDM. En TDM a los usuarios se les asigna un timeslot, y ningún otro cliente puede transmitir en ese timeslot así el propietario no esté transmitiendo. Esto hace que la red no sea muy eficiente. Una red ATM está compuesta de dos tipos de dispositivos: los switches ATM y los terminadores ATM. Un switch ATM es el encargado de recibir las celdas entrantes provenientes de otro switch ATM, leer y actualizar las cabeceras de cada celda y de direccionar la celda hasta que llegue a su destino final. Los terminadores ATM (o sistemas finales) son dispositivos que están provistos de un adaptador de interfaz de red ATM, por lo general están en las premisas del cliente.

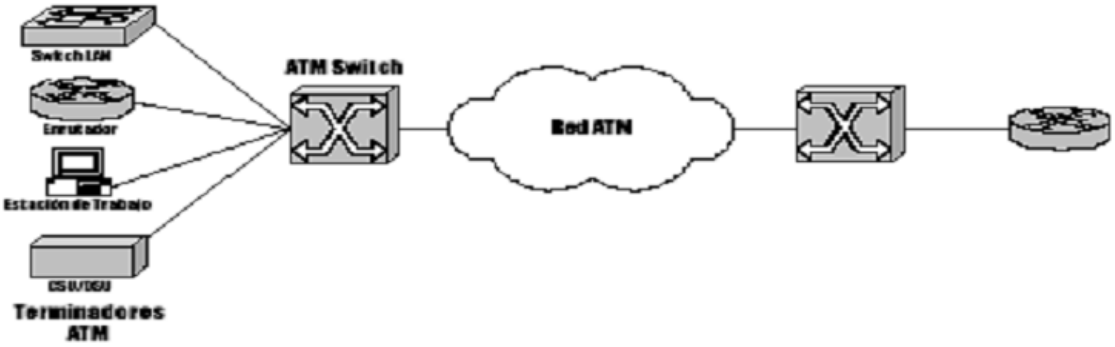


Figura 3. Dispositivos que intervienen en una red ATH

Ejemplos de terminadores ATM, como los que aparecen en la figura 1.6 son estaciones de trabajo, enrutadores, switches LAN, video CODECs (coder - decoders). En ATM se distingue dos tipos de interfaces: la UNI (User - Network Interface) que conecta un terminador con un switchATM y la NNI (Network - Node Interface) que conecta dos switches ATM.

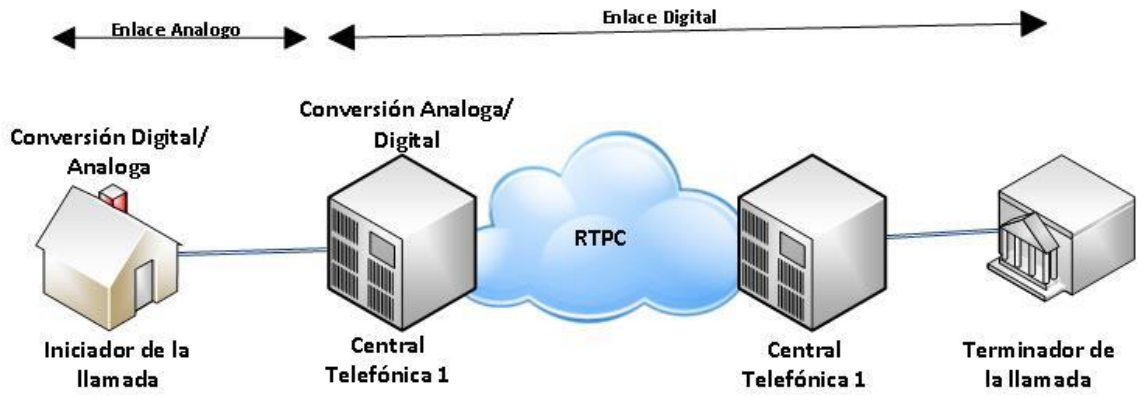
2.3.2. ENLACES CONMUTADOS

Los enlaces conmutados se dividen en dos tipos: los análogos y los digitales. Los primeros llegan hasta velocidades de 53 kbit/s para el downlink y hasta de 48 kbit/s para el uplink, los segundos transmiten y reciben a 64 kbit/s o 128 kbit/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de Red Digital de Servicios Integrados.

2.3.2.1. ENLACES CONMUTADOS ANALÓGICOS

Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la Red de Telefonía Pública Conmutada –RTPC (PSTN, en inglés), dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha prestado ha sido comunicación de voz, y sólo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos. El rango de frecuencia de la voz humana va desde los 20Hz hasta los 20Khz, pero casi toda la energía espectral se encuentra entre los 300Hz y 3.4Khz, por ende, la ITU ha definido un canal de voz (speechchannel) para telefonía en esta banda. En un enlace conmutado de datos, intervienen varios equipos desde el usuario inicial hasta el punto o equipo destino.

La figura 2 muestra los componentes de un enlace típico de datos sobre la red telefónica pública, se puede notar la necesidad de realizar una conversión A/D y otra D/A. La inercia que resulta de todo este proceso electrónico es la que en últimas limita a 56 kbit/s una comunicación analógica, que incluso puede llegar a 33.6 kbit/s cuando aparece una tercera y cuarta conversión entre la Central Telefónica 2 y el terminador de la llamada.

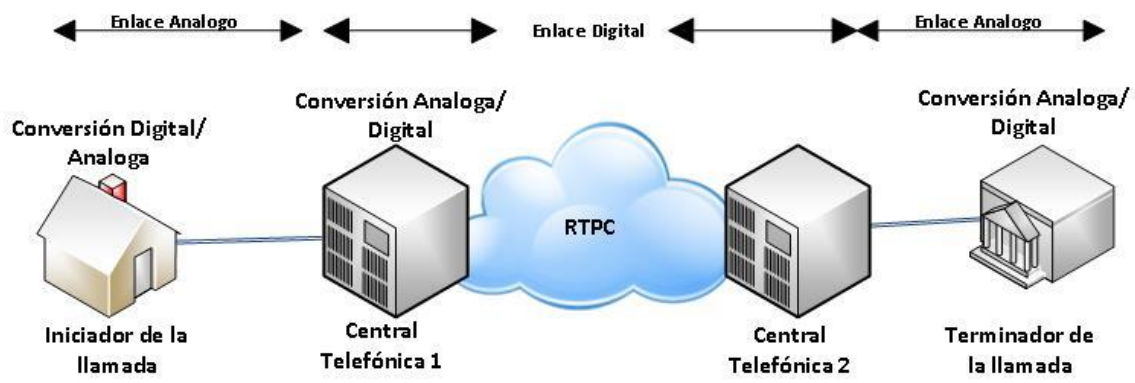


Ejemplo de conexión análoga de datos sobre la RTPC

Fuente: (Soto, 2014)

Figura 4. Conexión análoga de datos sobre RTCP

Se puede notar que la conexión entre el iniciador de la llamada y la central telefónica es análoga, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un modem análogo. Mientras que en el lado del sitio remoto la conexión es digital, y para esto se usan enlaces RDSI PRI o BRI. Por lo general los equipos que intervienen en este lado son servidores de acceso remoto (Remote Access Server – RAS). Cuando este enlace es también análogo, entonces se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos A/D y dos D/A, esto hace que la velocidad de transmisión y de recepción máximas sean apenas de 33.6 kbit/s. La figura 3 ilustra este escenario.



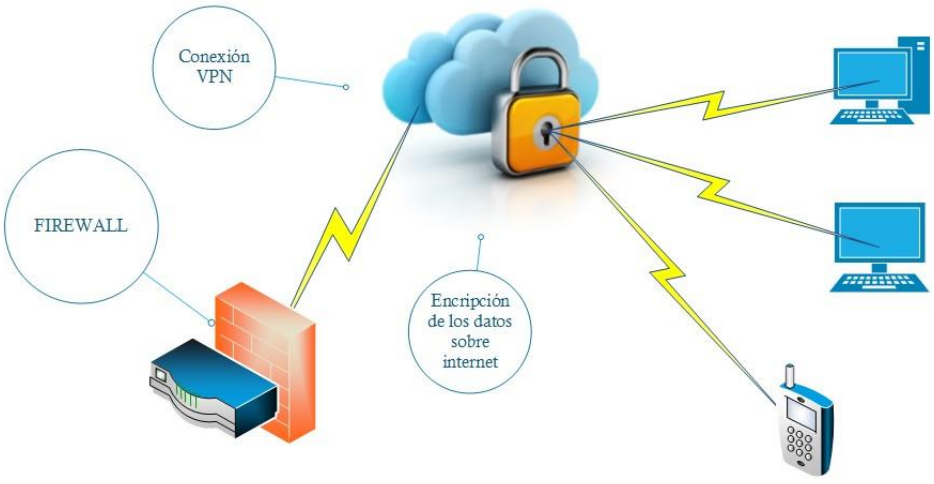
Fuente: (Soto, 2014)

Figura 5. Proceso total de la conexión con sus conversiones.

2.3.2.2. ENLACES CONMUTADOS DIGITALES – RDSI

RDSI o Red Digital de Servicios Integrados es un sistema de telefonía digital. Este sistema permite transmitir voz y datos simultáneamente a nivel global usando 100% conectividad digital. En RDSI, la voz y los datos son transportados sobre canales B (del inglés Bearer) que poseen una velocidad de transmisión de datos de 64 kbit/s, aunque algunos switches ISDN limitan esta capacidad a solo 56 kbit/s. Los canales D (o canales de datos) se usan para señalización y tienen velocidades de 16 kbit/s o 64 kbit/s dependiendo del tipo de servicio. Los dos tipos básicos de servicio RDSI son: BRI (del inglés Basic Rate Interface) y PRI (delinglés Primary Rate Interface). Un enlace BRI consiste de dos canales B de 64 kbit/s y un canal D de 16 kbit/s para un total de 144 kbit/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales.

Un enlace PRI está orientado a usuarios que requieren un mayor ancho de banda. Para accesar a un servicio BRI, es necesario tener una línea RDSI. Si sólo se desean comunicaciones de voz es necesario tener teléfonos digitales RDSI, y para transmitir datos es necesario contar con un adaptador de Terminal – TA (del inglés Terminal Adapter) o un enrutador RDSI. A diferencia de las conexiones conmutadas analógicas en una conexión RDSI el camino es 100% digital desde la central hasta el sitio del abonado, por lo cual no existe ningún tipo de conversiones A/D o viceversa, lo que facilita la obtención de velocidades de 64 kbit/s o 128 kbit/s, lo cual se logra convirtiendo los dos canales B de 64 kbit/s o en un canal lógico de 128 kbit/s. Esta característica es usada sólo en transmisión de datos y depende de la facilidad que tenga el equipo terminal de realizar esto. Típicamente esta característica tiene el nombre de Multilink.



Fuente: (Soto, 2014)

Figura: 6. Conexión de Redes Privadas Utilizando VPN

REDES PRIVADAS VIRTUALES – VPNs

2.2. INTRODUCCIÓN

Es comúnmente aceptado el hecho que las tecnologías de información en Internet han cambiado la forma como las compañías se mantienen comunicadas con sus clientes, socios de negocios, empleados y proveedores. Inicialmente las compañías eran conservadoras con la información que publicaban en Internet, tal como, productos, disponibilidad de los mismos u otros ítems comerciales. Pero recientemente, con el auge que ha tenido Internet, por el cada vez menor costo que la gente tiene que pagar para acceder a esta gran red y con el significado que esta ha adquirido como el principal medio mundial de comunicación, las redes privadas virtuales han hecho su aparición con más fuerza que nunca y se han ganado un espacio dentro del tan cambiante mundo de las redes de información.

Tradicionalmente, un enlace privado se ha hecho por medio de tecnologías WAN como X.25, FrameRelay, ATM, enlaces Clear Channel o enlaces conmutados (todas estas tecnologías WAN). Ahora con el gran crecimiento de Internet, es posible usar un protocolo como IP, sin importar la tecnología WAN que lo soporte, para disfrutar de los servicios y ventajas que ofrecen las redes privadas. Y mientras que las tradicionales redes privadas se han hecho fuertes en las conexiones LAN – to - LAN, no han sido capaces de atacar el mercado de los usuarios individuales o pequeñas oficinas sucursales, y es aquí principalmente donde han surgido con fuerza las soluciones basadas en VPNs sobre IP, pues su implementación resulta sencilla y bastante económica. Además el hecho que las

VPNs se construyan sobre infraestructuras públicas ya creadas ha hecho que las empresas ahorren más del 50% del costo que antes tenían que pagar en llamadas de larga distancia y en equipos físicos de acceso remoto o en alquiler de enlaces privados o dedicados.

2.3. QUÉ SON LAS REDES PRIVADAS VIRTUALES – VPNs

Para poder habilitar redes privadas distribuidas para comunicar de forma segura cada uno de los nodos de una red pública hay una necesidad de evitar que los datos sean interceptados. Una VPN es una conexión que tiene la apariencia y muchas de las ventajas de un enlace dedicado pero trabaja sobre una red pública. Para este propósito usa una técnica llamada entunelamiento (tunneling), los paquetes de datos son enrutados por la red pública, tal como Internet o alguna otra red comercial, en un túnel privado que simula una conexión punto a punto.

VPN

Una VPN (RED PRIVADA VIRTUAL) es una conexión virtual que utiliza algoritmos de seguridad como AES (Estándar de Encripción Avanzado) para cifrar la comunicación que pasa sobre internet. **(Soto, 2014)**

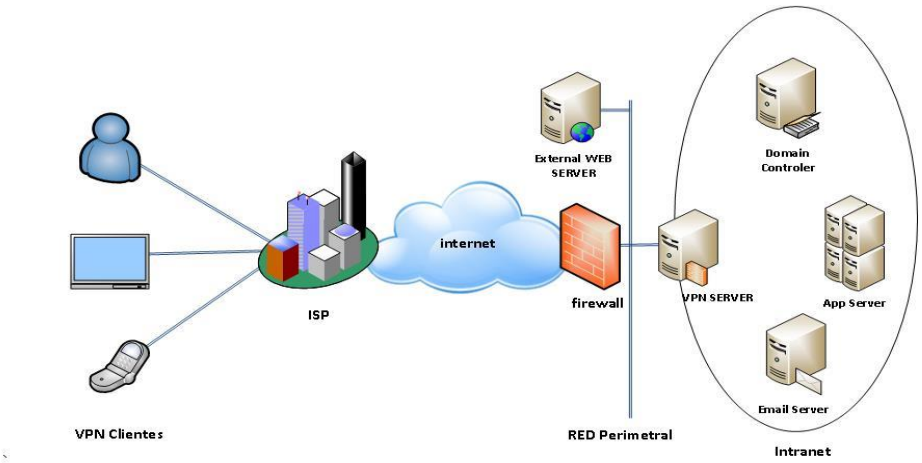
Otra Definición Según Wikipedia

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de

gestión de una red privada.1 Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.[1]

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.

La figura 1.0.07 muestra los distintos escenarios que se pueden manejar con la tecnología de Redes Privadas Virtuales (Dial - Up, Intranet VPN y Extranet VPN). Significativamente, decrece el coste de las comunicaciones porque el acceso a Internet es generalmente local y mucho más barato que las conexiones mediante Acceso Remoto a Servidores.



Fuente:(Soto, 2014)
Figura: 7. **Esquema de conexión de una VPN.**

[1] http://es.wikipedia.org/wiki/Red_privada_virtual

El objetivo final de una VPN es brindarle una conexión al usuario remoto como si este estuviera disfrutando directamente de su red privada y de los beneficios y servicios que dentro de ella dispone, aunque esta conexión se realice sobre una infraestructura pública.

2.4. ¿POR QUÉ VPN?

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red. Esta tecnología proporciona un medio para aprovechar un canal público de Internet como un canal privado o propio para comunicar datos que son privados. Más aún, con un método de codificación y encapsulamiento, una VPN básica, crea un camino privado a través de Internet.

Esto reduce el trabajo y riesgo en una gestión de red. Las VPNs son una gran solución a distintos problemas, pero sólo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Perú, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque sólo se hace uso de Internet que es un conjunto de redes conectadas entre sí.

2.4.1. COSTE

La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en líneas analógicas (dial-up) como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos: En el caso de accesos remotos, llamadas locales a los ISP (Internet ServiceProvider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización. O también mediante servicios de banda ancha.

Otras Ventajas

• **Usuario Móviles:** Una vez que la empresa cuenta con una VPN puede utilizarla para otros servicios sin gastos adicionales, reduciendo así sus costos operativos. Por ejemplo: es muy sencillo canalizar todas las llamadas telefónicas (locales o larga distancia) entre las sucursales a través de la VPN sin incrementar costos.

• **Escalabilidad y Flexibilidad:** Es posible integrar nuevos puntos a la VPN a demanda, sólo se debe agregar equipos y contratar conexiones a Internet.

•La disponibilidad, la seguridad, la eficiencia en el manejo del ancho de banda y la amplia cobertura que ha logrado Internet.

2.5. MEDIOS

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

• **Autenticación y autorización:** ¿Quién está del otro lado?, usuario / equipo y qué nivel de acceso debe tener.

• **Integridad:** La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los MessageDigest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

• **Confidencialidad:** Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y AdvancedEncryption Standard (AES).

• **No repudio:** Es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

• **Administración de dirección:** La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.

•**Encriptación de datos:** Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

2.6 TECNOLOGÍAS DE TUNELAMIENTO VPN

Existen varios tipos de arquitectura para las VPN, pero en esta ocasión se tratarán sólo algunas de ellas.

2.6.1 INTRANET VPN LAN – TO - LAN

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

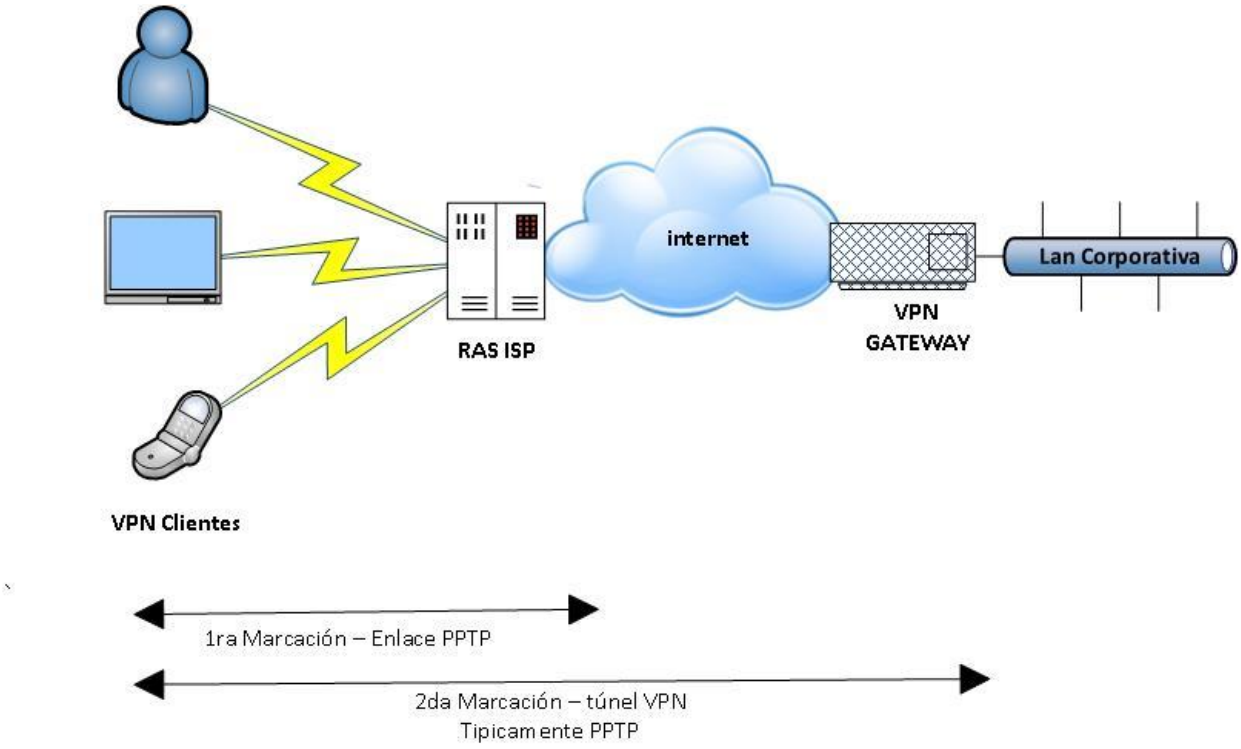
Una arquitectura Intranet VPN (o LAN – to - LAN VPN) se puede lograr el mismo objetivo de interconectar dos o más sitios de una red corporativa y a un costo mucho menor. La economía se ve reflejada tanto en equipos que se tienen que adquirir o arrendar para el montaje inicial de la topología, como en cargos fijos que se tienen que pagar mes a mes.

2.6.2. ACCESO REMOTO VPN

Fue la primera aplicación que se le dio a la emergente tecnología de las VPNs. Consiste en usar cualquier RAS que preste servicio de conexión a Internet como punto de acceso a una red corporativa también conectada a Internet por medio de un gateway VPN. Esta solución nació de la necesidad de poder acceder a la red corporativa desde cualquier ubicación, incluso a nivel mundial. Con el Acceso Remoto VPN, los RAS (Remote Access Service) corporativos quedaron olvidados, pues su mantenimiento era costoso y además las conexiones que tenían que hacer los trabajadores de planta externa, como vendedores y personal de soporte

técnico, cuando viajaban fuera de la ciudad, y más aun, a otros países eran demasiado costosas. El acceso remoto VPN se vio claramente impulsado por el auge de la Internet que ha hecho que prácticamente en todas partes del mundo se obtenga fácil acceso a la misma. Con el acceso remoto VPN un trabajador que se haya desplazado a otro país, por ejemplo, y que quiere acceder a la base de datos de su compañía, o al correo interno, o a cualquier otro recurso de su red corporativa, sólo tiene que conectarse a Internet con una simple llamada local a la ISP de la ciudad en la que se encuentre, y ejecutar su cliente de marcación VPN. A partir de la versión Windows 98, Microsoft incluyó un cliente de marcación VPN que funciona con el protocolo de entunelamiento PPTP.7 Todos los gateways VPN vienen con software VPN clientes para ser instalados en los distintos sistemas operativos presentes en el mercado.

La figura 1.0.09 muestra la creación de un túnel conmutado VPN usando un cliente PPTP instalado en el computador del trabajador remoto. Nótese que se realizan dos conexiones, una PPP a la ISP, y una PPTP al gateway VPN de la compañía que se encuentra conectado a Internet. La conexión PPP puede ser analógica o digital RDSI



Fuente: (Soto, 2014)

La figura 8. Creación de un túnel conmutado VPN usando un cliente PPTP

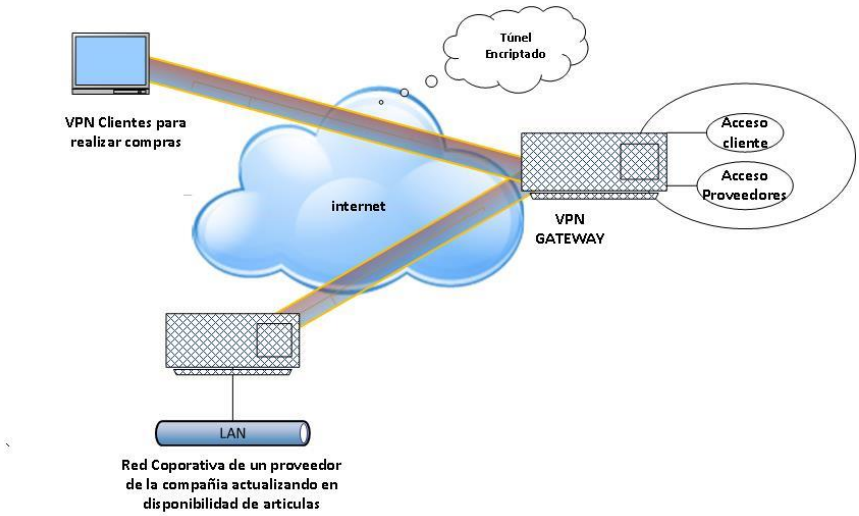
2.6.3. EXTRANET VPN

Las empresas necesitan intercambiar información y realizar transacciones no solamente entre sitios de su misma organización sino también con otras compañías. Por ejemplo, una empresa manufacturera quisiera permitirle a los computadores de sus distribuidores acceder a su sistema de control de inventarios. También dicha empresa quisiera poder acceder a la base de datos de sus proveedores y poder ordenar fácil y automáticamente cuando ellos necesiten materia prima. Hoy en día todas las empresas están haciendo presencia en la Internet y esto hace casi imperativo la comunicación con las otras empresas por

este medio. Ciertamente con una arquitectura de Extranet VPNs cada empresa tiene que controlar muy meticulosamente el acceso a los recursos de su red corporativa y a los datos que van a intercambiar con sus socios de negocios.

Implementar una topología Extranet VPN implica incrementar la complejidad de los sistemas de control de acceso y de autenticación. Adicionalmente la tendencia de los mercados hace que un cambio en la topología se pueda realizar fácilmente, para esto una Extranet VPN debe poder adicionar y eliminar dinámicamente acceso seguro a otras compañías. Tal reconfiguración dinámica es difícil cuando se cuenta con circuitos cerrados dedicados. La presencia de una compañía en Internet y el uso de la arquitectura de Extranet VPN, hace

posible crear conexiones dinámicas seguras a otras redes sin necesidad de cambiar la infraestructura física. Ejemplos de conexiones dinámicas seguras y que son conocidos como Extranet VPNs se muestran en la figura 1.0.10.



Fuente :(Soto, 2014)

Figura: 9. Conexiones Dinámicas Seguras VPN

Al igual que en una arquitectura LAN to LAN VPN es necesario un Gateway VPN que se instala en la frontera de la red corporativa. Los túneles son creados a través de Internet entre este gateway y el gateway VPN situado en la red de la otra empresa. De otro modo un cliente VPN en un computador independiente podría accesar a la red corporativa como un cliente usando cualquier acceso remoto.

En la actualidad la mayoría de los gateways VPN pueden establecer múltiples túneles seguros a múltiples empresas. Sin embargo, es importante que una empresa no sea capaz de obtener acceso a la información de otra compañía que está accediendo por medio de Extranet VPNs. Un nivel más de seguridad puede ser adicionado ubicando recursos exclusivos a cada una de las compañías que va a acceder a la red de interés en diferentes servidores.

2.6.4. MODELOS DE ENTUNELAMIENTO

Internet se construyó desde un principio como un medio inseguro. Muchos de los protocolos utilizados hoy en día para transferir datos de una máquina a otra a través de la red carecen de algún tipo de cifrado o medio de seguridad que evite que nuestras comunicaciones puedan ser interceptadas y espiadas. HTTP, FTP, POP3 y otros muchos protocolos ampliamente usados, utilizan comunicaciones que viajan en claro a través de la red. Esto supone un grave problema, en todas aquellas situaciones en las que queremos transferir entre máquinas información sensible, como pueda ser una cuenta de usuario (nombre de usuario y contraseña), y no tengamos un control absoluto sobre la red, a fin de evitar que

alguien pueda interceptar nuestra comunicación por medio de la técnica del hombre en el medio (man in themiddle), como es el caso de la Red de redes.

El problema de los protocolos que envían sus datos en claro, es decir, sin cifrarlos, es que cualquier persona que tenga acceso físico a la red en la que se sitúan las máquinas puede ver dichos datos. De este modo, alguien que conecte su máquina a una red y utilice un sniffer recibirá y podrá analizar por tanto todos los paquetes que circulen por dicha red. Si alguno de esos paquetes pertenece a un protocolo que envía sus comunicaciones en claro, y contiene información sensible, dicha información se verá comprometida. Si por el contrario, se cifran las comunicaciones con un sistema que permita entenderse sólo a las dos máquinas que son partícipes de la comunicación, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos, al no poder descifrar los datos.

Una forma de evitar este problema, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, es usar una técnica llamada tunneling. Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (SecureSHell), a través de las cuales se realizarán las transferencias inseguras, que pasarán de este modo a ser seguras. De esta analogía viene el nombre de la técnica, siendo la conexión segura (en este caso de SSH) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma

imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar.

2.6.5. VPN INTERNA WLAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi). Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

2.7 IMPLEMENTACIONES VPNS

2.7.1. SISTEMAS BASADOS EN HARDWARE

Los sistemas basados en hardware son routers que encriptan. Son seguros y fáciles de usar, simplemente hay que conectarlos. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación. Algunos de los productos en el mercado son por ejemplo:

2.7.2. SISTEMAS BASADOS EN CORTAFUEGOS

Estos se implementan con software de cortafuegos (firewall). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte. Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos de serie, y les provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

2.7.3. SISTEMAS BASADOS EN SOFTWARE

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPNs ofrecen el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico es enrutado por el túnel. Se puede hacer un enrutamiento inteligente de una manera mucho más fácil.

2.8 TECNOLOGÍAS DE TÚNELES Y CIFRADO DE DATOS

Para que se establezca un túnel tanto el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel. La tecnologíade túnel se puede basar

ya sea en el protocolo del túnel de Nivel 2 ó de Nivel 3. Estos niveles corresponden al Modelo de referencia de interconexión de sistemas abiertos (OSI). Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP y L2TP y el envío de nivel 2 (L2F) son protocolos de túnel de Nivel 2; ambos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP) que se enviará a través de la red. Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes. IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3. Estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

2.8.1 PROTOCOLO DE PUNTO A PUNTO (PPP)

Debido a que los protocolos de Nivel 2 dependen principalmente de las funciones originalmente especificadas para PPP, vale la pena examinar este protocolo más de cerca. PPP se diseñó para enviar datos a través de conexiones de marcación o de punto a punto dedicadas. PPP encapsula paquetes de IP, IPX y NetBEUI dentro de las tramas del PPP y luego transmite los paquetes encapsulados del PPP a través de un enlace punto a punto. El PPP se utiliza entre un cliente de marcación y un NAS.

Existen cuatro fases distintivas de negociación en una sesión de marcación del PPP. Cada una de estas cuatro fases debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del usuario:

Fase1: Establecer el enlace del PPP: Utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física.

Fase 2: Autenticar al usuario: La PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Un esquema seguro de autenticación proporciona protección contra ataques de reproducción y personificación de clientes remotos. Un ataque de reproducción ocurre cuando un tercero monitorea una conexión exitosa y utiliza paquetes capturados para reproducir la respuesta del cliente remoto, de tal manera que pueda lograr una conexión autenticada. La personificación del cliente remoto ocurre cuando un tercero se apropia de una conexión autenticada. La mayoría de las implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de Autenticación de Saludo Challenge (CHAP) y Microsoft ChallengeHandshakeAuthenticationProtocol (MSCHAP).

Fase 3: Control de rellamado del PPP: La implementación de Microsoft del PPP incluye una Fase opcional de control de rellamado. Esta fase utiliza el Protocolo de control de rellamado (CBCP) inmediatamente después de la fase de autenticación. Si se configura para rellamado, después de la autenticación, se desconectan tanto el cliente remoto como el NAS.

Fase 4: Invocar los protocolos a nivel de red: Una vez que se hayan terminado las fases previas, PPP invoca los distintos Protocolos de Control de Red (NCPs) que se seleccionaron durante la de establecimiento de enlace (Fase1) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el

Protocolo de Control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación. Fase de transferencia de datos: Una vez que se han terminado las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitido se envuelve en un encabezado del PPP el cual quita el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 4, los datos se comprimirán antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos, los datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

2.8.2 PPTP (POINT – TO - POINT TUNNELING PROTOCOL)

Protocolo de túnel de punto a punto (PPTP): El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas del IP para transmisión sobre una red IP, como la de Internet. El PPTP se documenta en el RFC preliminar, “Protocolo de túnel de punto a punto” (pptp-draft-ietf -ppext-pptp-02.txt). Este proyecto se presentó ante el IETF en junio de 1996 por parte de las compañías miembros del Foro PPTP incluyendo Microsoft Corporation, AscendCommunications, 3Com/Primary Access, ECI Telematics y US Robotics (ahora 3Com). PPTP agrega un nuevo nivel de seguridad mejorada y comunicaciones multiprotocolo a través de Internet. Si se utiliza el nuevo Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) con métodos de autenticación seguros como los certificados, la transferencia de datos a través de una conexión VPN con PPTP es tan segura como en una LAN de un sitio corporativo.

Protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP para mantenimiento del túnel y tramas del PPP encapsuladas de Encapsulación de Enrutamiento Genérico (GRE) para datos de túnel (puerto 1723). Se pueden encriptar y/o comprimir las cargas útiles de las tramas del PPP encapsulado. La Figura 5.1. muestra la forma en que se ensambla el paquete del PPTP antes de la transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño de la trama final muestra la encapsulación para un cliente de marcación (controlador de dispositivo PPP).

Está especialmente diseñado para las aplicaciones de acceso remoto de VPN, pero también soporta las otras aplicaciones de VPN. PPTP soporta encriptación de datos y la compresión de estos paquetes. Además usa una forma de GRE (General Routing Encapsulation, Protocolo Genérico de Encapsulación). En el entorno de un acceso remoto VPN usando PPTP a través de Internet, los túneles VPN son creados en dos pasos:

1. El cliente PPTP conecta a su ISP usando PPP dial - up (mediante modem tradicional o ISDN).

2. Por medio del dispositivo intermedio ya mencionado, PPTP crea una conexión de control TCP entre el cliente VPN y el servidor VPN para establecer un túnel (PPTP usa el puerto 1723 para estas conexiones).

Por otro lado, PPTP soporta conexiones VPN a través de una LAN, por lo que no es necesario conectar a un ISP. Los túneles son creados directamente. Una vez que el túnel VPN está establecido, PPTP soporta dos tipos de flujo de información:

1. Mensajes de control para manejar y/o eliminar la conexión VPN. Este tipo de mensajes pasan directamente entre el cliente VPN y el servidor.

2. Paquetes de datos que pasan a través del túnel, hacia o desde el cliente VPN. Volviendo al tema del control de conexión en PPTP, una vez que la conexión TCP está establecida, PPTP utiliza una serie de mensajes de control para mantener la conexión VPN.

Algunos de estos mensajes son los siguientes:

1. Start Control Connection Request: Inicia la configuración de la sesión VPN; puede ser enviado tanto por el cliente como por el servidor.

2. Start Control Connection Reply: Enviado en respuesta a (1). Contiene información que indica el éxito o el fracaso de la operación de configuración y del número de versión del protocolo.

3. Stop Control Connection Request: Petición de cerrar la conexión de control. En cuanto a la seguridad en PPTP, soporta autenticación (usa para ello protocolos basados en PPP, tales como EAP, CHAP y PAP), encriptación y filtrado de paquetes. PPTP depende de la funcionalidad de PPP para autentificar a los usuarios y mantener la conexión remota dial up y para encapsular y encriptar los paquetes IP, IPX o NeTBEUI pero se encarga directamente del mantenimiento del túnel VPN y de transmitir los datos a través del túnel. PPTP además tiene algunas características adicionales de seguridad aparte de la que provee PPP. La popularidad de PPTP se debe en gran parte a Microsoft, ya que los clientes PPTP están disponibles en Windows.

VENTAJAS

Coste y Escalabilidad: Como ya se ha comentado, tienen un bajo coste ya que no hacen uso de líneas dedicadas de larga distancia y sólo se hace necesario una conexión dedicada a un proveedor de servicios. Esta conexión podría ser a través de una línea dedicada de corta distancia (mucho más barata que las de larga distancia) o simplemente una conexión de banda ancha como por ejemplo DSL. Otra forma de reducir costes con VPN se da en la opción de acceso remoto; en este caso y por norma general, el cliente VPN no tiene que hacer una llamada de larga distancia al punto de acceso del proveedor de servicios, con una llamada local bastaría. Por otro lado, el coste es bajo ya que son los proveedores del servicio los que cargan con el coste de acceso y no las compañías. A medida que una compañía crece, si utilizase líneas dedicadas el número de estas se vería incrementado al mismo tiempo (según las necesidades de la compañía) con el consiguiente aumento de los gastos. Con VPN, y utilizando Internet, se solucionaría este problema ya que se usa la red ya disponible pudiendo acceder con ella, además, a puntos donde las líneas dedicadas no podrían llegar.

DESVENTAJAS

Incompatibilidad: Este protocolo suele utilizar más de un estándar para la autenticación y la encriptación, por lo que, por ejemplo, dos clientes PPTP pueden ser incompatibles entre ellos si encriptan los datos de manera diferente.

Vulnerabilidad: La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de

VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo. Aunque tengan estos puntos en contra se puede implementar PPTP con EAP-TLS para soportar certificados de seguridad.

ACTUALIZACIÓN DE PPTP

La actualización de PPTP para las plataformas Microsoft viene por parte de L2TP o IPSec. Su adopción es lenta porque PPTP es fácil de configurar, mientras L2TP requiere certificados de clave pública, e IPSec es complejo y poco soportado por plataformas antiguas como Windows 98 y Windows Me

2.8.3. TÚNELES

PPTP permite a los usuarios y a las ISPs crear varios tipos de túneles, basados en la capacidad del computador del usuario final y en el soporte del ISP para implementar PPTP. Los túneles se pueden dividir en dos clases, voluntarios y permanentes. Túneles voluntarios son creados por requerimiento de un usuario y para un uso específico. Los túneles permanentes son creados automáticamente sin la acción del usuario y no se le permite escoger ningún tipo de privilegio. En los túneles voluntarios, la configuración del mismo depende del usuario final; cuando se usan túneles de este tipo, el usuario puede simultáneamente acceder a Internet y abrir un túnel seguro hacia el servidor PPTP. En este caso el cliente PPTP reside en el computador del usuario. Los túneles voluntarios proveen más privacidad e integridad de los datos que un túnel permanente.

Túneles permanentes son creados sin el consentimiento del usuario, por lo tanto, son transparentes para el mismo. El cliente PPTP reside en el servidor de acceso remoto del ISP al que se conectan los usuarios finales. Todo el tráfico originado desde el computador del usuario final es reenviado por el RAS sobre el túnel PPTP. En este caso la conexión del usuario se limita sólo a la utilización del túnel PPTP, no hay acceso a la red pública (Internet) sobre la cual se establece el túnel. Un túnel permanente PPTP permite que múltiples conexiones sean transportadas sobre el mismo túnel.

2.9. L2TP (LAYER 2 TUNNELING PROTOCOL)

L2TP [REF5.4] fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte de la IETF. Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de este último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accediendo vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por el ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo. Todas las anteriores características

de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM. Dado que L2TP es un protocolo de capa 2, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI.

Puesto que L2TP usa PPTP en enlaces conmutados, incluye mecanismos de autenticación nativos de PPP como PAP y CHAP. Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.

El L2TP sobre las redes IP utiliza UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. La Figura 5.2 muestra la forma en que se ensambla un paquete L2TP antes de su transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

2.10. IPSEC (Internet Protocol Security / Protocolo Seguridad de Internet)

Es un conjunto de protocolo que se utiliza para aplicar algoritmos de seguridad para asegurar la confidencialidad y autenticidad del protocolo de internet.

(Soto, 2014)

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos. IPSec [REF5.5] es un conjunto de protocolos diseñados para proveer seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6.

Entre los servicios de seguridad definidos en IPSec se encuentran, control de acceso, integridad de datos, autenticación del origen de los datos, protección anti - repetición y confidencialidad en los datos. Entre las ventajas de IPSec están la modularidad del protocolo, ya que no depende de un algoritmo criptográfico específico.

2.10.1. COMPONENTES DE IPSEC

IPSec está compuesto por tres componentes básicos: los protocolos de seguridad (AH y ESP), las asociaciones de seguridad (SAs) y las bases de datos de seguridad; cada uno de los cuales, trabaja de la mano con los demás y ninguno le resta importancia al otro.

2.10.1.1. PROTOCOLOS DE SEGURIDAD

IPSec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el Authentication Header (AH) [REF5.6] y el Encapsulating Security Payload (ESP) [REF5.7], y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (Internet Key Exchange Protocol) [REF5.8].

El éxito de una implementación IPSec depende en gran medida de una adecuada elección del protocolo de seguridad y de la forma como se intercambian las llaves criptográficas. AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir ataques de repetición. Este protocolo es apropiado cuando se requiere autenticación en vez de confidencialidad.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo. IKE es un protocolo que permite a dos entidades IPSec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma.

2.10.2. AUTHENTICATION HEADER (AH)

El protocolo de cabecera de autenticación AH es usado para propósitos de autenticación de la carga útil IP a nivel de paquete por paquete, esto es autenticación de la integridad de los datos y de la fuente de los mismos. Como el

término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP son auténticos, es decir, que han arribado a su destino sin ninguna modificación. AH también provee de un mecanismo de protección opcional anti - repetición de paquetes IP. Sin embargo, AH no protege la confidencialidad de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos. El protocolo AH define como un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda autenticación.

2.12. CONCEPTOS DE LAS VPN DINÁMICAS

Internet no fue diseñada, originalmente, para el ámbito de los negocios. Carece de la tecnología necesaria para la seguridad en las transacciones y comunicaciones que se producen en los negocios. Entonces, ¿cómo establecer y mantener la confianza en un entorno el cual fue diseñado desde el comienzo para permitir un acceso libre a la información?, es decir, ¿cómo conseguir seguridad en una intranet sin chocar con los principios básicos de Internet sobre la flexibilidad, interoperatibilidad y facilidad de uso?.

La respuesta apropiada se encuentra en la utilización de VPNs Dinámicas. A diferencia de una VPN tradicional, una VPN Dinámica proporciona, además de un alto nivel de seguridad a ambos extremos, una flexibilidad necesaria para acoplarse dinámicamente a la información que necesitan los distintos grupos de usuarios. Las VPNs Dinámicas pueden ofrecer esta flexibilidad ya que están basadas en una única arquitectura. Además, una VPN Dinámica proporciona más

recursos y servicios a una Intranet, para hacer mayor uso de los recursos de la información. Alguna de las características que se proporciona son las siguientes:

- Proporciona una seguridad importante para la empresa.
- Se ajusta dinámicamente al colectivo dispar de usuarios.
- Permite la posibilidad de intercambio de información en diversos formatos.
- El ajuste que hace para cada usuario lo consigue gracias a los diferentes navegadores, aplicaciones, sistemas operativos, etc.
- Permite a los usuarios unirse a distintos grupos, así como a los administradores asignar identidades en un entorno simple pero controlado.
- Mantiene la integridad total, independientemente del volumen administrativo, cambios en la tecnología o complejidad del sistema de información corporativo.

2.13. FUNCIONAMIENTO DE LAS VPN DINÁMICAS

Las VPNs Dinámicas constan de una plataforma de seguridad de red y un conjunto de aplicaciones para usar en la plataforma de seguridad.

Siguiendo los pasos ilustrados en la figura anterior, un usuario realiza una petición de información a un servidor, por ejemplo, pulsando con su ratón en un hipervínculo. Los pasos seguidos se pueden describir en los siguientes puntos:

Un usuario solicita información usando una aplicación tal como un navegador de Internet, desde un ordenador de sobremesa: El intercambio de información comienza cuando un usuario envía información a otro usuario o solicita información al servidor. En el supuesto de que un usuario haya accedido a un hipervínculo desde dentro de algún documento Web, dicho hipervínculo será seguro y solamente podrá ser accedido por usuarios autorizados.

La aplicación envía y asegura el mensaje: Cuando un cliente y un servidor detectan que se necesita seguridad para transmitir la petición y para ver el nuevo documento, ellos se interconectan en un mutuo protocolo de autentificación.

Este paso verifica la identidad de ambas partes antes de llevar a cabo cualquier acción. Una vez que se produce la autentificación se asegura el mensaje encriptándolo. Adicionalmente, se puede atribuir un certificado o firma electrónica al usuario.

El mensaje se transmite a través de Internet: Para que la petición alcance el servidor debe dejar la LAN y viajar a través de Internet, lo cual le permitirá alcanzar el servidor en algún punto de la misma. Durante este viaje, puede darse el caso de que atraviese uno o más firewalls antes de alcanzar su objetivo. Una vez atravesado el firewall, la petición circula a lo largo del pasillo Internet hasta alcanzar el destino.

El mensaje recibido debe pasar controles de seguridad: El mensaje se transfiere al servidor. El servidor conoce la identidad del usuario cliente cuando recibe la petición. Durante la petición, se verifican los derechos de acceso de los usuarios:

En una VPN dinámica, el sistema debe poder restringir qué usuarios pueden y no pueden acceder a la misma. El servidor debe determinar si el usuario tiene derechos para realizar la petición de información. Esto lo hace usando mecanismos de control, alojados en el Servidor de Control de Acceso. De este modo, incluso si un usuario presenta un certificado válido, puede ser que se le deniegue el acceso basándose en otros criterios.

La petición de información es devuelta por Internet, previamente asegurada: El servidor de información encripta la información y opcionalmente la certifica. Las claves establecidas durante los pasos de autentificación mutua se usan para encriptar y desencriptar el mensaje. De esta forma, un usuario tiene su documento asegurado.

Las redes VPN proporcionan principalmente dos ventajas:

• **Bajo coste de una VPN:** Una forma de reducir coste en las VPN es eliminando la necesidad de largas líneas de coste elevado. Con las VPN, una organización sólo necesita una conexión relativamente pequeña al proveedor del servicio. Otra forma de reducir costes es disminuir la carga de teléfono para accesos remotos. Los clientes VPN sólo necesitan llamar al proveedor del servicio más cercano, que en la mayoría de los casos será una llamada local.

• **Escalabilidad de las VPNs:** Las redes VPN evitan el problema que existía en el pasado al aumentar las redes de una determinada compañía, gracias a Internet. Internet simplemente deriva en accesos distribuidos geográficamente.

Hay dos aplicaciones principales para las redes VPN:

• **Teletrabajo:** Es la solución ideal, por su efectividad y sus bajos costes, para aquellas organizaciones que necesiten que sus empleados accedan a la red corporativa, independientemente de su ubicación geográfica.

• **VPN Empresa:** Solución de conectividad entre sucursales de la empresa o entre la empresa y sus socios, proveedores, etc. Gracias a su flexibilidad se adapta al tamaño y necesidades de la organización.

Las redes VPN presentan cuatro inconvenientes:

•Las redes VPN requieren un conocimiento en profundidad de la seguridad en las redes públicas y tomar precauciones en su desarrollo.

•Las redes VPN dependen de un área externa a la organización, Internet en particular, y por lo tanto dependen de factores externos al control de la organización.

•Las diferentes tecnologías de VPN podrían no trabajar bien juntas.

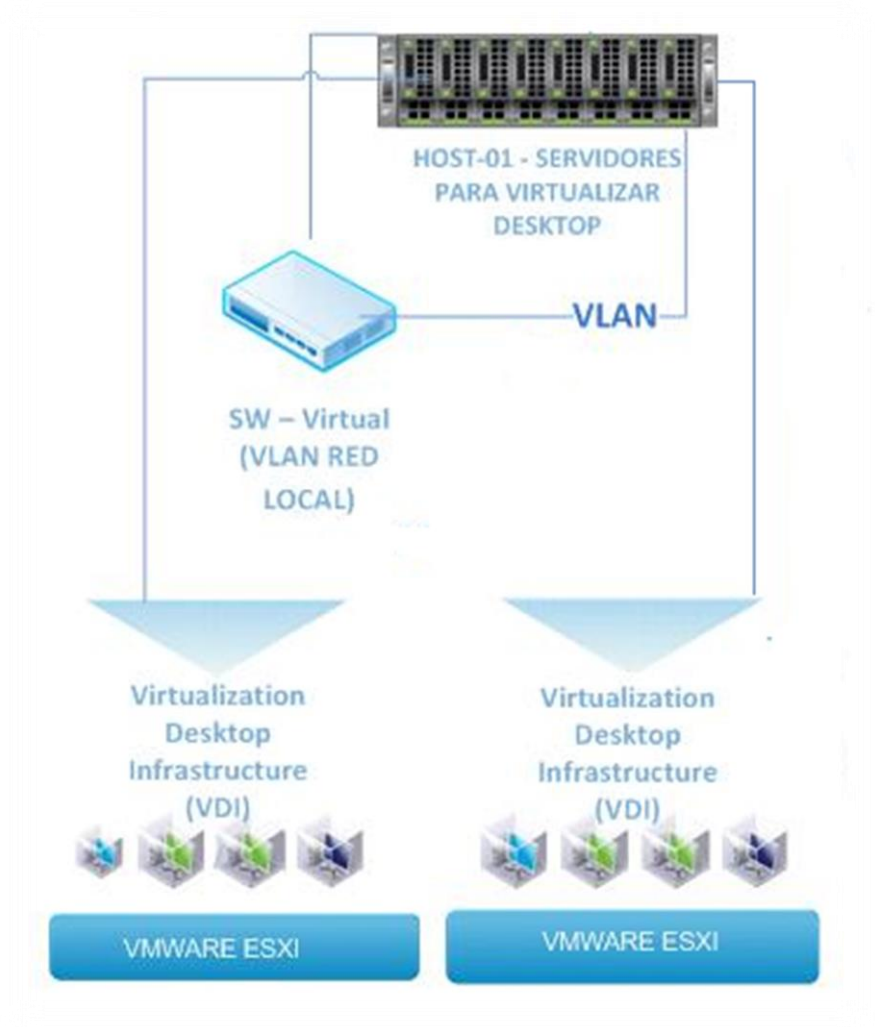
•Las redes VPN necesitan diferentes protocolos que los de IP.

Se estima que una solución VPN para una determinada empresa puede reducir sus costes entre un 30% y un 50% comparada con las conexiones punto a punto.

CAPÍTULO 3

VIRTUALIZACION

Se inicia con la historia de la virtualización, un nuevo concepto de virtualización de escritorio, cual es la demanda que existe hoy día de este nuevo concepto. Se dan la Estimaciones, estadísticas y las ventajas que posee al ser implementada en compañías.



3.1 Virtualización

Virtualización es el proceso que ayuda a reducir los gastos de capital por medio de la consolidación de servidores, también permite disminuir los gastos operacionales mediante la automatización. ***(Soto, 2014)***

3.1.1 Historia de la Virtualización

Fue International Business Machines (IBM**) quien inicio con la implementación de la Virtualización, hace más de 30 años como una forma de hacer particiones de ordenadores de los llamados** Mainframes en máquinas virtuales

que fueran independientes. Estas particiones permitían a los computadores realizar múltiples tareas y procesos al mismo tiempo.

La Virtualización experimento cambios en los 80s y los 90s, cuando se vio un cambio en aplicaciones tipo cliente-servidor y los servidores llamados x86 y algunas computadoras de escritorio económicas establecieron el modelo de distribución de la informática. La extensa aplicación de Windows y la ocurrencia de Linux como un sistema operativo en los 80s convirtieron a los servidores x86 en el modelo del sector. De la manera en que incrementaron los servidores x86 y los computadores de escritorio generaron problemas operacionales y de infraestructura de TI. De algunos de estos problemas se mencionan los siguientes:

Poca utilización de infraestructura. Estas implementaciones lograron un promedio entre un 10 y un 15% de su capacidad total, según señala International Data Corporation (IDC) una empresa del tipo estudios de mercado. Habitualmente, las instituciones hacen una sola aplicación por cada servidor para evitar que las debilidades de una aplicación afecten a la disponibilidad de otra en el mismo servidor en el cual se implementó.

Incremento de los precios de infraestructura. Los precios de los operantes, los cuales proveen soporte al incremento de las infraestructuras han aumentado a un ritmo acelerado. La gran mayoría de estas infraestructuras deben permanecer operando en todo momento, esto trae como consecuencia un gasto en el consumo

energético, lo que implica refrigeración y que algunas instalaciones no varían con el uso que se les da.

De manera que los ambientes se hacen más complicados, aumenta el nivel de determinación de la experiencia que debe tener el personal que gestiona estas estructuras, y así mismo, aumentan los precios asociados con dicho personal. Las organizaciones derrochan cantidades exageradas de dinero y recursos en tareas manuales que son ligadas al mantenimiento de los servidores y esto trae consigo el aumento del personal que la realiza.

Insuficiente protección ante desastres y fallas. Con el paso del tiempo las aplicaciones se ven afectadas por las interrupciones del servicio de aplicaciones de servidor críticas y la falta de acceso a escritorios de usuario final fundamentales. Los desastres naturales, amenaza de ataques a la seguridad, enfermedades y terrorismo han hecho énfasis en que se planifique la continuidad del negocio, tanto en computadores de escritorios como en servidores.

Escritorios de usuario final de mantenimiento elevado. El trabajo y la seguridad de los escritorios empresariales planean cuantiosos retos. Intervenir un ambiente de escritorios clasificados y así mismo aplicar políticas de gestión, acceso y seguridad sin inquietar la capacidad que posee el usuario de trabajar con eficacia y eficiencia, ya que si no fuera así sería complejo y costoso. Se tienen que aplicar continuamente muchos parches y actualizaciones en el entorno del escritorio para eliminar los riesgos de seguridad.

Virtualización

La virtualización consiste en la capacidad de separar el software del hardware en el que están instalados. Esta característica aplicada al Cloud Computing se materializa en que el usuario no tiene que preocuparse por la implementación concreta de los servicios de la nube ni tener en cuenta el hardware asociado a ellos.

La virtualización posibilita una optimización respecto al aprovechamiento de los recursos comunes, ya que permite que las aplicaciones sean independientes del hardware en el que se ejecutan.

Hypervisor

Un hypervisor es el software encargado de mediar el hardware físico con el hardware de las máquinas virtuales. Existen hypervisores de 2 tipos, tipo 1 o bar-metal y tipo 2 o hosted. El hypervisorbare-metal no funciona bajo un sistema operativo instalado sino que tiene acceso directo sobre los recursos hardware, en este tipo de tecnología de virtualización el hardware soportado es más limitado ya que normalmente es construido con un conjunto limitado de drivers.

Un hypervisorhosted requiere que instales primero un sistema operativo sobre el cual se instalará el software de virtualización, de igual modo a como se instala cualquier aplicación. Esta tecnología presenta una compatibilidad mayor con el hardware que la bare-metal, debido a que es el propio sistema operativo el que se encarga de gestionar los drivers.

Fuente: Propia

Figura 10. Tipos Virtualización de Servidores

3.1.2 Virtualización a Nivel Operativo

Este tipo de tecnología de virtualización de servidores es la que trabaja a nivel de sistema operativo. El servidor físico y una única instancia del sistema operativo son virtualizadas en múltiples particiones aisladas, donde cada partición duplica un servidor real. Elkernel se ejecutará en un único sistema operativo y proveerá esa funcionalidad del sistema operativo para cada una de las particiones. Esta virtualización no debe ser confundida con la virtualización de sistema operativo (ALEGSA, 1998-2013).

3.1.3 Paravirtualización

La Paravirtualización es una técnica de programación informática que permite virtualizar por software los sistemas operativos. El programa paravirtualizador presenta una interfaz de manejo de máquinas virtuales. Cada máquina virtual se

comporta como un computador independiente, por lo que permite usar un sistema operativo o varios por computador emulado.

La intención de la interfaz modificada es reducir la porción del tiempo de ejecución del usuario, empleado en operaciones que son sustancialmente más difíciles de ejecutar en un entorno virtual, comparado con un entorno no virtualizado.

La paravirtualización provee filtros especialmente definidos para permitir a los invitados y al anfitrión hacer peticiones y conocer estas tareas, que de otro modo serían ejecutadas en el dominio virtual (donde el rendimiento de la ejecución es peor.) Por lo tanto, una plataforma de paravirtualización exitosa puede permitir que el monitor de la máquina virtual (VMM) sea más simple (por traslado de la ejecución de tareas críticas desde el dominio virtual al anfitrión de dominio), y/o que reduzca la degradación del rendimiento global de la ejecución de la máquina dentro del anfitrión virtual.

La paravirtualización requiere que el sistema operativo invitado sea portado de manera explícita para la API. Una distribución de un sistema operativo convencional que no soporte paravirtualización no puede ser ejecutada ni visualizada en un monitor de máquina virtual VMM (IBM, 2007).

3.1.4 Virtualización Completa

La Virtualización completa es similar a la paravirtualizacion, pero difiere en que no requiere que los sistemas operativos auxilien con el hypervisor. En algunas plataformas, tales como la x86 existen algunos inconvenientes para lograr que la Virtualización completa sea llevada a cabo. Esto método es muy semejante a la

paravirtualizacion, con el agregado de que no necesita modificaciones para los guest. La única condición es que estos deben soportar la arquitectura de hardware que utiliza.

Según Turban, E; King, D; Lee, J; Viehland, D. (2008), en Informática, la Virtualización es crear a través de un software una versión virtual de algún recurso de tecnología, pudiendo ser una plataforma de algún hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

La Virtualización es el cambio de recursos físicos por recursos virtuales. La misma implica menos costos en equipos, más rapidez del trabajo, menos consumo de energía y un sinnúmero de ventajas más. **(Jhacdira Valdez, 2014)**

Definiéndolo de otra manera, se asemeja con la abstracción de los recursos de una computadora, llamada Hypervisor o por sus siglas en ingles VMM (Virtual Machine Monitor) el cual crea una capa abstracta entre el hardware de la máquina física o host y el sistema operativo de la máquina virtual (virtual machine, guest), dividiéndose el recurso en uno o más entornos de ejecución.

Esta capa de software (VMM) gestiona y maneja los cuatro recursos principales de una computadora (CPU, Memoria, Periféricos de entrada y salida y Conexiones de Red) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en la computadora central. Esto hace que se puedan poseer diferentes ordenadores virtuales ejecutándose en el mismo ordenador físico.

Tal término es antiguo; y se viene utilizando desde 1960, y ha sido aplicado a disparejos aspectos y ambientes diferentes de la informática, desde sistemas computacionales completos, hasta capacidades o componentes individuales (Brodkin, 2009) (Microsoft C. , 2011).

La Virtualización es la encargada de implantar una interfaz externa que encapsula una implementación subyacente mediante la composición de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control.

Un avanzado desarrollo de nuevas plataformas y tecnologías de virtualización ha hecho que en los últimos años se haya vuelto a prestar atención a este concepto.

La máquina virtual en general simula una plataforma de hardware autónoma incluyendo un sistema operativo completo que se ejecuta como si estuviera instalado. Típicamente varias máquinas virtuales operan en un computador central. Para que el sistema operativo “guest” funcione, la simulación debe ser lo suficientemente grande (siempre dependiendo del tipo de virtualización).

La Virtualización es la creación de un entorno virtual donde puedes ejecutar otros programas de manera independiente. Esos programas serán los mismos que ejecutas normalmente en tu ordenador, pero funcionarán, por así decirlo, en una réplica de un sistema operativo. **(Alexandra Hernández, 2014)**

Existen diferentes formas de Virtualización: es posible virtualizar el hardware de servidor, el software de servidor, virtualizar sesiones de usuario, virtualizar

aplicaciones y también se pueden crear máquinas virtuales en una computadora de escritorio (Microsoft, 2011).

Entre los principales proveedores de software que han desarrollado tecnologías de virtualización completas (que abarcan todas las instancias: servidor, aplicaciones, escritorio) se encuentran, por ejemplo VMware y Microsoft. Estas compañías han diseñado soluciones específicas para virtualización, como VMware Server y Windows Server 2008 Hyper-V para la virtualización de servidores. Si bien la virtualización no es un invento reciente, con la consolidación del modelo de la Computación en la nube, la virtualización ha pasado a ser uno de los componentes fundamentales, especialmente en lo que se denomina infraestructura de nube privada.

Cloud Computing (Computación en la Nube)

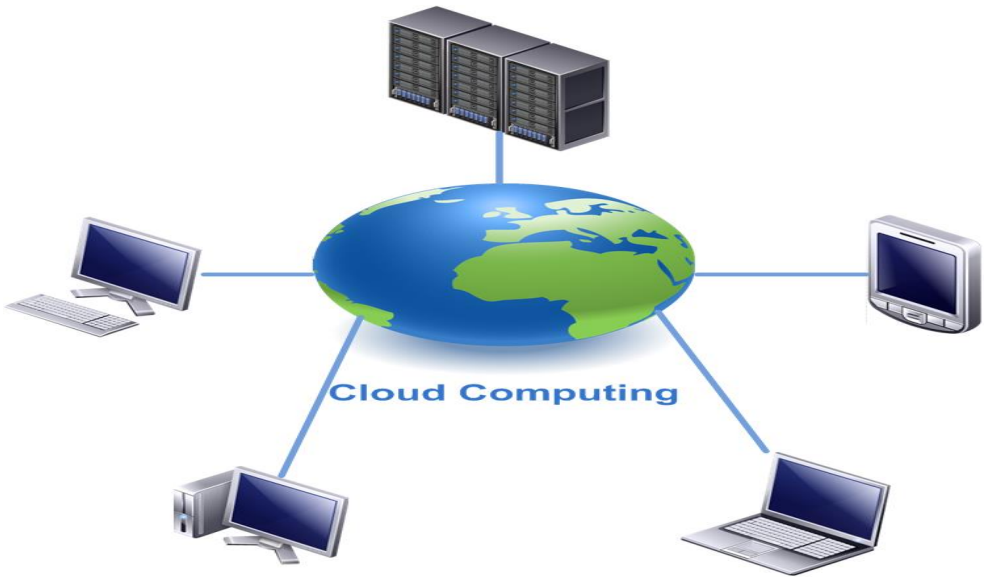


Figura 11. Cloud Computing

Fuente: Propia

Se define como una tecnología que ofrece servicios a través de la plataforma de internet. Los usuarios de este servicio tienen acceso de forma gratuita o de pago, todo depende del servicio que se necesite usar.[2]

La computación en la nube, consiste en la gestión y suministro de aplicaciones, información y datos como un servicio. Estos servicios se proporcionan a través de la "nube", a menudo basado en un "modelo basado en el consumo".[3]

Cloud Computing

Conceptos básicos de Cloud Computing

El Cloud Computing puede definirse como grupos de ordenadores distribuidos (generalmente centros de datos y granjas de servidores) que proporcionan recursos y servicios bajo demanda a través de una red (generalmente Internet).

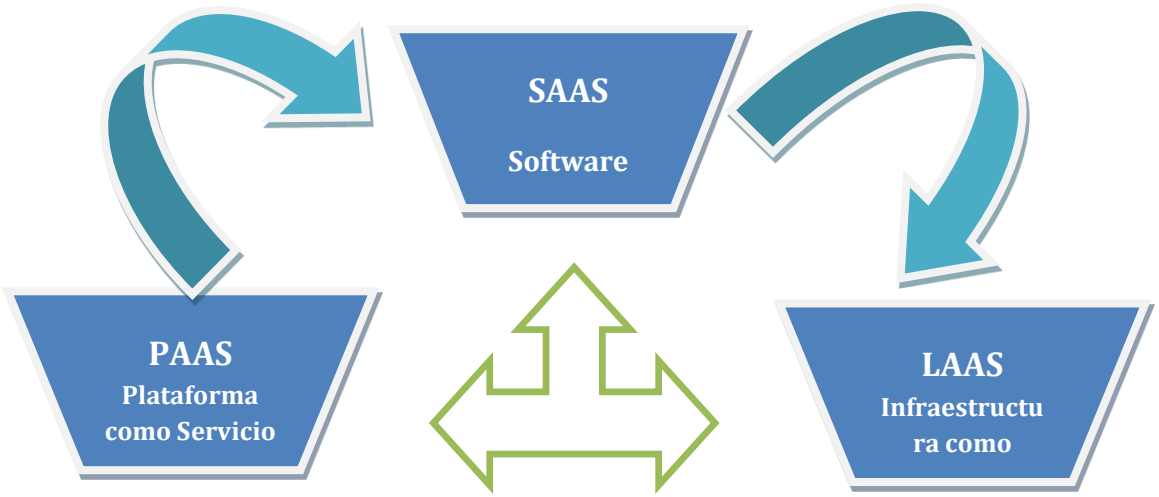
Pueden definirse tres tipos básicos de modalidades de servicio:

[2] Aroche, S. F. (s.f.). Maestros del web. Recuperado el 8 de abril de 2011, de http://www.maestrosdelweb.com/editorial/cloud-computing-nueva-era-de-desarrollo/

[3] Junta de castilla y León. (2010). Observatorio Regional de la Sociedad de la Información. Recuperado el 03 de 11 de 2011, de La tecnología como servicio: http://issuu.com/orsicyl/docs/cloud_computing?mode=a_p

Tipos de servicios

La computación en nube ha evolucionado en una variedad de servicios que incluyen recursos compartidos, software y plataformas “a demanda”. Se dará a conocer una breve introducción a cada uno de estos tipos: SaaS (Software as a Service), PaaS (Plataform as a Service), IaaS (Infrastructure as a Service).[4]



Fuente: (Soto, 2014)

Figura 12. Tipos de Servicios

Software as a Service (SaaS)

Software as a Service (Software como servicio) es un término utilizado para describir el software desplegado en Internet y se caracteriza por que el proveedor licencia la aplicación al suscriptor en un modelo de "servicio por demanda". Los principales segmentos de mercado del modelo SaaS se encuentran en tópicos como: administración de contenido, colaboración y Customer Relationship Management (CRM).

[4] http://www.denoe.es/test/wp-content/uploads/estructura-cloud-computing.png

Platform as a Service (PaaS)

Distribución de herramientas y software necesarios para el desarrollo de aplicaciones en equipos distribuidos.

Platform as a Service (Plataforma como Servicio) se refiere a un modelo que no sólo ofrece la plataforma de despliegue y adicionalmente una plataforma de desarrollo de aplicaciones completa. Mientras que en el modelo SaaS se ofrecen aplicaciones listas para utilizarse, el modelo PaaS brinda la opción de construir una aplicación personalizada utilizando la plataforma de desarrollo ofrecida. Los proveedores PaaS ofrecen por medio de sus plataformas soporte para los lenguajes de programación más comunes como Java o .NET reduciendo la dependencia de plataformas SaaS, que usualmente casan los usuarios y organizaciones con su plataforma.

3.2 Infrastructure as a Service (IaaS)

Consiste en la externalización de las máquinas de proceso de datos (servidores, dispositivos de almacenamiento, enrutadores, etc.). Gracias a la virtualización (separación física entre la infraestructura y el lugar donde transcurren las operaciones) se puede pagar por el consumo de recursos.

Infrastructure as a Service (Infraestructura como servicio) es el tercer modelo de implementación de Cloud Computing y hace referencia a plataformas que ofrecen infraestructura de cómputo y usualmente se encuentran desplegadas

sobre un entorno de virtualización. La plataforma brinda la alternativa de escalar la infraestructura de manera vertical (subir y bajar los recursos de cómputo) a demanda y se paga por los recursos consumidos. Este modelo ofrece el más alto grado de flexibilidad, así como el menor grado de dependencia con la plataforma permitiendo a los usuarios migrar las aplicaciones de un proveedor a otro. Por otro lado una implementación sobre IaaS requiere instalación, configuración y mantenimiento adicionales.[5]

Software como servicio (SaaS): distribución de aplicaciones a través de Internet mediante un navegador web, pagando en base al consumo. La información, el proceso de datos y los resultados están alojados en la empresa proveedora TIC. Finalmente, existen otras modalidades de servicio Cloud Computingmucho menos extendidas, como por ejemplo el modelo PraaS (Process as a Service), una variante del SaaS, que se basa en la gestión externa y operada en Internet de un proceso de negocio completo.

3.3 Algunas de las características tecnológicas del Cloud Computing

son las siguientes: dispone de un alto grado de automatización, el acceso y la administración se realizan por medio de una red (infraestructura colad), las actividades son gestionadas desde ubicaciones centrales, en lugar de ser realizadas en la sede de cada cliente permitiendo a los clientes el acceso remoto a las aplicaciones mediante la web, emplea una virtualización avanzada y

[5] Cloudcomputingla. (10 de 08 de 2010). Cloudcomputingla.com/. Recuperado el 10 de 02 de 2011, de http://www.cloudcomputingla.com/

se integra en una red de mayor ámbito con mayor software de comunicación.

A la hora de implantar la tecnología Cloud Computing (CC) en las empresas se deben realizar una serie de etapas que comienzan con el estudio de viabilidad técnica y de rentabilidad económica que incluya el análisis y previsión de las cargas de trabajo. Esta información ayudará a determinar si la tecnología CC es interesante (viable) para una empresa. La siguiente etapa determina el tipo de Cloud a utilizar: Cloud pública, privada o híbrida. Las nubes públicas son propiedad, y están operadas por un proveedor externo que proporciona acceso a varios clientes bajo suscripción. Esta modalidad es adecuada para acceder a herramientas de colaboración, ofimáticas o almacenamiento.

Las nubes privadas son propiedad de la empresa que demanda el servicio y pueden estar gestionadas por la propia empresa o por un tercero. Esta opción asegura mayores niveles de privacidad y control interno.

Las nubes híbridas resultan de la combinación de dos o más nubes de diferentes tipos. Por ejemplo, cuando una empresa tiene servicios dispuestos en su red privada pero también utiliza una nube pública.

Una recomendación general sería que las empresas comiencen con un despliegue de servicios sencillos en la modalidad de Cloud Computing en la modalidad de nube pública, incorporando progresivamente servicios más sensibles y complejos con una orientación de Cloud privada.

3.4 Beneficios del uso del Cloud Computing

Los beneficios que puede aportar el Cloud Computing a las empresas que lo adopten pueden clasificarse en tres grupos:

Económicos, Tecnológicos y Organizativos.

Económicos.

El Cloud Computing permite reducir los costes de mantenimiento, soporte y ahorro de energía de los sistemas de información existentes, junto con un ahorro en el despliegue de nuevas infraestructuras. Además, no es necesario el pago de licencias o las actualizaciones de versiones (incluso hay servicios gratuitos).

Reducción de la complejidad y enfoque estratégico: aumentar el nivel de concentración en el negocio principal (corebusiness).

Flexibilidad: (Reacción más rápida ante los cambios en las condiciones del mercado), incorporando servicios adicionales cuando sea necesario por parte del proveedor de Cloud.

Los beneficios económicos son especialmente importantes para las pymes y las empresas que no disponen de suficientes recursos facilitándoles ser competitivas al proporcionarles la oportunidad de adoptar nuevos desarrollos de Tecnologías de la Información (TI)con costes razonables al adoptar el modelo de pago por consumo y los costes de mantenimiento.

Tecnológicos.

Facilita el despliegue en la implantación, no es necesario infraestructura (hardware, software y comunicaciones) aunque también depende de la especificidad y complejidad de los servicios. solicitados. Asimismo se simplifican las tareas de actualizaciones, mantenimiento y soporte.

Los aspectos de seguridad de la información se ven facilitados al realizar una gestión centralizada que permite que el proveedor de servicios TI proporcione accesos seguros que garanticen la privacidad y confidencialidad de la información (encriptación de datos, htpps, Kerberos, etc.) y una completa protección antivirus. Además debe garantizarse el funcionamiento y la estabilidad del sistema en un marco 24/7 por medio de la utilización de infraestructuras a prueba de fallos y líneas replicadas y disponiendo de alternativas para proporcionar el servicio por otros medios y en otras ubicaciones en el menor tiempo posible. Se proporciona de esta forma una mejora en la capacidad de adaptación y de recuperación de desastres así como una reducción de los tiempos de inactividad.

Se dispone de una capacidad externa que permite hacer frente a aumentos de las cargas de los sistemas de información (así como disminuciones) provocados por variaciones en la actividad de áreas funcionales y procesos de negocio, con el menor coste posible.

La responsabilidad en el desarrollo y operación de los sistemas de información puede transferirse parcialmente a la empresa suministradora de Cloud. Se suprime también la complejidad en los procesos de actualización en las versiones.

Mayor respeto por el medio ambiente, dado que al centralizar los servicios se produce un menor consumo de energía (partida importante de los costes de la infraestructura de TI) y una reducción en el impacto medioambiental.

Finalmente hay que citar la conveniencia de utilizar herramientas estandarizadas y generales así como una mayor facilidad en la integración con el resto de las aplicaciones empresariales.

Organizativos.

Disminuye la dimensión y la orientación del departamento de TI así como la necesidad de disponer de personal formado. Se aumentan también las posibilidades de comunicación, colaboración y registro de la información dado que se puede acceder a toda la información desde cualquier lugar, momento o dispositivo. En la actualidad, en modalidad Cloud Computing se pueden aprovechar una nueva generación de aplicaciones sociales que fomentan la colaboración dentro de la organización pero también con proveedores o clientes, que sería complicado desplegar con los recursos propios de la organización.

El Cloud Computing ofrece también una oportunidad de cambio: plantearse hacer las cosas de forma distinta, identificando costes ocultos e inercias

organizativas y provocado por el creciente número de aplicaciones web disponibles que son un acicate para el planteamiento de nuevos procesos o el rediseño de los ya existentes.

Debido a la estandarización y factores relacionados con la difusión de la tecnología y el empleo de interfaces amigables las aplicaciones y servicios web disponibles son fáciles de utilizar, disminuyendo, de esta forma, la curva de aprendizaje: el usuario no tiene que estar familiarizado con los aspectos tecnológicos que hay detrás, accediendo de forma directa a través de la red sin la interacción de un tercero. Además, la disminución en el uso fraudulento del software y la piratería tienen un impacto beneficioso tanto en la cultura organizativa de la empresa como en el riesgo de

sufrir sanciones.

En definitiva el Cloud Computing facilita el acceso a un catálogo de servicios estandarizados que pueden responder a las necesidades de los negocios de forma flexible, adaptándose a las variables necesidades de la empresa y a las condiciones del mercado y pagando únicamente por el consumo efectuado.

3.5 Desventajas del uso del Cloud Computing

La adopción del Cloud Computing se enfrenta a una serie de obstáculos y resistencias que las empresas, de una forma más o menos objetiva, tienen. Existe una preocupación sobre el cómo adoptar este modelo, puede afectar a la disponibilidad de los servicios TI y también a su impacto sobre la seguridad de la información. De forma similar al planteamiento seguido para

los beneficios, las desventajas pueden clasificarse en aspectos tecnológicos y aspectos organizativos.

3.6 Aspectos tecnológicos

La seguridad es un aspecto importante para la mayoría de las empresas. Se entiende que se va a estar expuesto a un número mayor de riesgos y vulnerabilidades al producirse un traslado de información de una red protegida a una red pública, pudiendo sufrir ataques o una merma de la confidencialidad. Los temores surgen porque las empresas creen que pierden el control de la información y que al compartir infraestructura aumentan los posibles riesgos a la seguridad debido a accesos no autorizados. Una alternativa que mejora la seguridad es el empleo de nubes privadas. En cualquier caso, es importante conocer con claridad las garantías con las que se ofrece un servicio Cloud.

También se presentan temores respecto a las siguientes circunstancias:

Falta de privacidad. Ante la ausencia de una suficiente cobertura legal (o incluso con ella). Los datos de una organización podrían ser comercializados y adquiridos por terceros; incluso por empresas de la competencia, logrando información ventajosa sobre productos o cuentas de clientes. No obstante, Hay que preguntarse en qué se diferencian los datos alojados en la nube de los que maneja una entidad financiera o la información asociada a una operación en línea realizada mediante una tarjeta de crédito. En estos casos, los datos

“viajan” y no es objetivo pensar que están más seguros en un servidor propio que en el de un reputado proveedor externo.

- Integridad de la información ante incidentes informáticos de diversa índole sobre los que no se tiene ningún tipo de control. Este concepto está relacionado con la fiabilidad del servicio suministrado, al considerar que se trata de un sistema que no está convenientemente probado.

- Situación de “cautividad” respecto de los proveedores de servicios Cloud por varias razones: falta de estandarización, poca (o nula) interoperabilidad de los servicios existentes, acuerdos de nivel de servicio (SLA) mal definidos y con requerimientos insuficientes, etc.

- Se considera que la inercia al cambio puede ser también un obstáculo que impida la adopción de la perspectiva Cloud, especialmente en empresas maduras y con sistemas de información consolidados y que pueden estar funcionando de forma satisfactoria.

- Disponibilidad y continuidad del servicio. Por falta de calidad de las comunicaciones, interrupciones. Dado que si Internet no está disponible el usuario no tendrá acceso al programa. Podría producirse interrupción en el servicio por razones achacables al propio proveedor, como no disponer de una capacidad suficiente.

- Disminución de la libertad y creatividad para introducir mejoras y personalizaciones en las distintas capas de los sistemas de información. No se dispone de métricas que permitan evaluar los parámetros de

calidad de servicio y que fundamenten una queja razonada ante una pérdida de calidad.

- No se dispone de métricas que permitan evaluar los parámetros de calidad de servicio y que fundamenten una queja razonada ante una pérdida de calidad.

3.7 Aspectos organizativos

En este bloque se consideran aquellos inconvenientes en el ámbito organizativo que son percibidos por las empresas. Entre ellos cabe citar: la dependencia del proveedor originada por la centralización de las aplicaciones y el almacenamiento de los datos. Esta dependencia origina una sensación de cautividad: no resultará fácil migrar a otro servicio y tendrá asociados una serie de costes económicos y riesgos para los procesos de negocio de la organización. Este temor aparece fortalecido si se considera la aparición de planteamientos monopolísticos por parte de las empresas proveedoras de servicios. Asociada al obstáculo percibido de la dependencia y la cautividad se encuentra la percepción falta de cobertura legal o el empleo de legislación extranjera que permita definir unos acuerdos de niveles de servicio SLA (Service Level Agreement) adecuados. Una circunstancia que debe ser tenida en cuenta es la falta de una comprensión de las implicaciones reales de utilizar este tipo de servicio.

En resumen, quizá las empresas estarán más dispuestas a adoptar de forma amplia el Cloud Computing cuando pueda asegurarse el

cumplimiento de normativas relativas a la seguridad (protección de datos) a través de toda la empresa, la integración de la información crítica para el negocio y los procesos empresariales o la gestión completa del ciclo de vida de la aplicación, con independencia del mecanismo de descarga. A todo esto hay que unir unas garantías de calidad de servicio, alta fiabilidad, seguridad y alta disponibilidad.[6]

3.8 Características del Cloud Computing

Auto Reparable: En caso de fallo, el último Backup de la aplicación pasa a ser automáticamente la copia primaria y se genera uno nuevo.

Escalable: Todo el sistema/arquitectura es predecible y eficiente. Si un servidor maneja 1000 transacciones, 2 servidores manejaran 2000 transacciones.

SLA: Regidos por un Acuerdo de Nivel de Servicio (SLA) que define varias políticas como cuáles son los tiempos esperados de rendimiento y en caso de pico, debe crear más instancias.

Virtualizado: las aplicaciones son independientes del hardware en el que corran, incluso varias aplicaciones pueden corren en una misma máquina o una aplicación puede usar varias máquinas a la vez.[7]

[6] http://blog.stikom.edu/vivine/files/2010/11/Identification-of-a-companys-suitability-for-the-adoption-of-cloud.pdf

[7] Aroche, S. F. (s.f.). Maestros del web. Recuperado el 8 de abril de 2011, de http://www.maestrosdelweb.com/editorial/cloud-computing-nueva-era-de-desarrollo/

3.9 Futuro de la virtualización.

La virtualización es un tema que hoy tiene mucho auge en los grandes centros de datos pero hace tan solo una década solo IBM tenía conocimiento de los beneficios de la virtualización con su sistema operativo VM. Si del lanzamiento de la tecnología de VMware a su dominio en los grandes centros de da tos en 2009 solo han trascurrido diez años, es razonable suponer que la virtualización es una tecnología que no es moda pasajera. Es un producto en constante evolución que necesariamente debe dar el salto de los grandes centros de datos a los escritorios de la computación hogareña, para lograr la penetración en masa tan necesaria para permanecer en el mercado.

Respecto de la virtualización, el usuario casero difícilmente requiere de tener varios equipos virtuales corriendo en su domicilio. Esto se puede ejemplificar con otra tecnología virtual, Java, a pesar de que su teléfono, reproductor de video, refrigerador o consola de juegos alojen una máquina virtual en su firmware, esto es totalmente transparente para él. Por esta razón WMware encuentra su nicho de mercado en la solución de problemas de integración y alta disponibilidad, no en convencer al usuario final de las bondades de la virtualización, de la misma forma que SUN no necesitó convencer al usuario final para que fuera incluida su tecnología en un dispositivo del hogar.

En la conferencia dictada por Stephen Alan Herrod [9], se exponen algunas de las tendencias más importantes desde la óptica del Vicepresidente de Tecnología de VMware: las tendencias tecnológicas de la virtualización, su presencia en

los centros de datos, la forma en que la virtualización permitirá la creación de dispositivos integrados todo en uno mediante máquinas virtuales y la estrategia de recuperación de desastres mediante virtualización. Todos estos esfuerzos comparten la característica de estar enfocados en los centros de datos.

En la estrategia a futuro de VMware s e aprecia una esperanza obtener participación del mercado masivo, en la reflexión sobre el nuevo modelo de distribución del software. Herrod plantea un modelo para empaquetar software en máquinas virtuales e instalar el hypervisor en las máquinas destino. Aplicando este 14 modelo no será necesario un proceso previo de carga de software liberando a las empresas de esta labor, por supuesto con el pago de la respectiva licencia a VMware. Ya sea como un componente importante del centro de datos del futuro o como un medio para la distribución masiva de software, lo cierto es que la tecnología tiene mucho que innovar y conquistar en el cambiante mercado de las tecnologías de la información. Hasta el momento ha logrado mantenerse como un producto que tiene mucho que ofrecer a sus compradores y no solo como una moda que con el paso del tiempo desaparecerá.

3.10 Aplicaciones de la virtualización.

La virtualización tiene un amplio potencial de utilización. Sus aplicaciones se pueden clasificar en dos grandes áreas, aquellas aplicaciones que están ampliamente probadas, que tradicionalmente los fabricantes y proveedores las usan como argumentos para la toma de decisiones sobre la adopción

de la virtualización. La otra área, más amplia pero menos difundida, se enfoca en los usos experimentales y académicos de la virtualización. En este caso la difusión de estas aplicaciones solo puede hacerse mediante la consulta de archivos como documentos técnicos (whitepapers), reportes de investigación.

En ambos casos la virtualización es una tecnología que logra despertar un fuerte interés en aquellos que se atreven a profundizar en sus aplicaciones, debido a que los usos de la virtualización solo se encuentran limitados por el propio usuario. La capacidad de crear equipos virtuales e instalar en ellos un sistema, así como la replicación de este sistema con la facilidad de copiar y pegar archivos, permite crear, modificar o destruir equipos y ambientes virtuales en horas. Esta facilidad y versatilidad son muy difíciles de lograr en el mundo real.

Existen también un cierto número de aplicaciones de la virtualización que recientemente se han puesto al descubierto, por citar alguno de ellos se puede mencionar los planes de recuperación. Estos pueden ser de dos tipos de continuidad del negocio o planes de recuperación ante desastres (BCP y DRP respectivamente por sus siglas en inglés).

Este tema comenzará revisando las aplicaciones de la virtualización en los negocios, para cerrar con un análisis de los usos académicos que se le dan. Aunque el tema está pensado para ser amplio y completo en su alcance,

muchas de las aplicaciones de la virtualización, aún se están gestando en las áreas de soporte técnico de las empresas, en las aulas de las escuelas o incluso en la computadora de un desvelado estudiante que está desarrollando una nueva e interesante forma de aprovechar el poder que nos brinda la virtualización. De esta forma se intenta resaltar que las aplicaciones de la virtualización están en constante desarrollo y crecen de manera acelerada, considerarlas todas es una labor que escapa a los alcances de este trabajo.

CAPÍTULO 4

Este capítulo tratará sobre la disponibilidad en los centro de datos, Según lo establecido por el estándar TIA-942, de la Asociación para la Industria de las Telecomunicaciones (TIA, por sus siglas en inglés).

En esta parte se va a profundizar sobre la disponibilidad en los centro de datos, Según lo establecido por el estándar TIA-942, esta propiedad es muy importante en el mundo de la infraestructura tecnológica por ende se deben conservar para mantener y asegurar la continuidad del negocio.

4.1 Estándar TIA 942

El estándar TIA 942 nos brinda una serie recomendaciones además de directrices detalladas para el diseño e instalación de un centro de datos. El mismo se categoriza como tiers y trae un concepto nuevo en pleno auge en América Latina, por así decirlo ofrecen de manera racional la formulación de las necesidades de la infraestructura a la par con las de la disponibilidad del negocio.

4.2 Historia

La Telecomunication Industry Association publica su estándar TIA-942, En abril de 2005 buscando unificar diferentes conceptos en el diseño de la infraestructura tecnológica. Dicho estándar que en principio se basaba en una serie de características para las comunicaciones y cableado estructurado, se desarrolla con avances de mejoras en subsistemas de infraestructura generando los lineamientos que deben seguir para clasificar los mismos en función de los distintos grados de disponibilidad que se pretende alcanzar.

Gracias a este estándar se puede obtener grandes ventajas que son fundamentales:

- Nomenclatura estándar.

- Funcionamiento a prueba de fallos.
- Aumento de la protección frente a agentes externos.
- Fiabilidad a largo plazo
- Mayores capacidades de expansión y escalabilidad.

4.3 Estándar TIA-942 y La Infraestructura

El estándar TIA-942 especifica que los centros de datos están diseñados para manejar los requerimientos de grandes cantidades de equipos informáticos y telecomunicaciones. Por lo tanto, las telecomunicaciones y los profesionales de la tecnología de información deberían participar en el diseño del centro de datos desde su inicio.

Según el estándar TIA-942, la infraestructura de datos está compuesta por cuatro subsistemas:

- Telecomunicaciones:
    - Cableado de armarios y horizontal
    - Accesos redundantes
    - Cuarto de entrada / Cuarto de Comunicaciones
    - Área de distribución
    - Troncal
    - Elementos activos y alimentación redundantes,
    - Patchpanels y latiguillos
    - Documentación

- Arquitectura:
    - Selección de ubicación
    - Tipo de construcción
    - Protección ignífuga y requerimientos NFPA 75(Sistemas de protección contra el fuego para información),
    - Barreras de vapor
    - Techos y pisos
    - Áreas de oficina
    - Salas de UPS y baterías
    - Sala de generador
    - Control de acceso, CCTV, NOC (Network Operations Center – Centro operativo)
- Sistema eléctrico:
    - Número de accesos
    - Puntos de fallo
    - Cargas críticas
    - Redundancia de UPS y topología de UPS
    - Puesta a tierra
    - EPO (Emergency Power Off- sistemas de corte de emergencia)
    - Baterías
    - Monitorización
    - Generadores
    - Sistemas de transferencia.

- Sistema mecánico:
    - Climatización
    - Presión positiva
    - Tuberías y drenajes
    - condensadores
    - Control de HVAC (High Ventilating Air Conditionning)
    - Detección de incendios
    - Extinción por agente limpio (NFPA 2001)
    - Detección por aspiración (ASD)
    - Detección de líquidos.

Los equipos que aquí se encuentran consisten esencialmente de computadoras, redes de comunicaciones y demás servicios internos o externos a la red de una empresa.

Por ejemplo, un banco guardará todos los datos de sus clientes, depósitos en el extranjero, etc., en su centro de datos.

Un centro de datos es un caso típico de una instalación donde, debido a la extrema importancia de la información allí contenida y a la continuidad de los servicios que se le exige, la energía suministrada debe estar siempre disponible. Debido a esta importancia, a estos equipos se les suele llamar “equipos críticos”, haciendo alusión a que su mal funcionamiento, o desperfecto, sería “crítico” para los intereses de una empresa.

Por supuesto que la importancia de estos equipos críticos es relativa al servicio que brindan. Un desperfecto momentáneo puede ocasionar una pérdida de competitividad.

- Como en el caso que una terminal de venta al público de boletos de avión de una determinada empresa no pueda acceder al centro de datos para saber el saldo de los boletos para un determinado vuelo, o puede ocasionar una pérdida importante de ingresos a la empresa.
- Como sería el caso que el centro de datos de una tarjeta de crédito internacional no respondiera a las solicitudes de crédito durante 1 hora, o hasta la total desaparición de la misma.
- Como sería el caso que el centro de datos de un banco pierda los datos de sus depósitos.

Debido a esta criticidad es que desde hace años se estudian distintas topologías, o formas de realizar la instalación eléctrica en estos sitios, de forma que las fallas y mal funcionamientos comunes no afecten el servicio del Centro de Datos. En otras palabras, se han analizado las fallas comunes en una instalación eléctrica (cortocircuitos, cortes de energía desde la red, la falla o demora de encendido de un grupo electrógeno, la falla de un interruptor termomagnético, etc.) así como las tareas habituales que deben hacerse sobre la misma (ampliar un tablero de distribución, agregar un interruptor en un tablero general, sustitución de una línea de potencia, sustitución de un interruptor, etc.) y cómo evitar que estas tareas afecten el servicio de los equipos críticos (Centro de Datos).

Esto hizo que los proyectistas de instalaciones eléctricas para un centro de datos tuvieran que crear arquitecturas cada vez más complejas para considerar todo tipo de circunstancias adversas que pudieran afectar el servicio de energía de los equipos críticos. Por supuesto, esto tiene un límite en la experiencia y subjetividad personal de cada proyectista.

4.4 TIERS, estándar ANSI/TIA-942

Este estándar incluye cuatro niveles relacionados con diversos puntos de disponibilidad de la infraestructura de centro de datos. Las calificaciones de nivel corresponden a los de la industria, clasificación en las filas del centro de datos definidos por el Instituto Uptime, pero las definiciones de cada nivel se han ampliado en la presente Norma. Los niveles más altos no sólo corresponden a una mayor disponibilidad, también conducen a mayores costos de construcción. En todos los casos, los niveles de mayor categoría incluyen los requisitos de menor nivel a menos que se especifique lo contrario.

Un centro de datos puede contener calificaciones de diferentes niveles para algunos puntos de su infraestructura. Por ejemplo, un centro de datos puede ser clasificado de nivel 3 para eléctrica, pero el nivel 2 a mecánica. Sin embargo, el centro de datos en su valoración global de nivel es igual a la calificación más baja en todas partes de su infraestructura. Por lo tanto, un centro de datos que está clasificado de nivel 4 para todas las partes de su infraestructura, exceptuando la eléctrica, donde tiene el nivel 2, tiene el nivel 2 en general. La valoración global para el centro de datos se basa en su componente más débil.

Se debe tener cuidado para mantener la capacidad del sistema mecánico y eléctrico para el nivel correcto cuando la carga del centro de datos aumenta con el tiempo. Un centro de datos puede ser degradado desde el nivel 3 o nivel 4 al nivel 1 o nivel 2, como la capacidad de redundancia se utiliza para apoyar los nuevos equipos informáticos y de telecomunicaciones.

Un centro de datos debe cumplir con los requisitos especificados en esta Norma para ser clasificado en cualquier nivel de este método. Si bien el concepto de niveles es útil para estratificar los niveles de redundancia dentro de varios sistemas del centro de datos, es muy posible que las circunstancias pudieran exigir algunos sistemas como niveles más altos que otros. Por ejemplo, un centro de datos ubicado en el suministro eléctrico es menos fiable que el promedio podría ser diseñado con un sistema eléctrico de nivel 3 pero sólo tier 2 sistemas mecánicos. Los sistemas mecánicos pueden ser mejorados con las piezas de recambio para ayudar a asegurar un MTTR (tiempo de reparación medio).

También hay que señalar que los factores humanos y los procedimientos de operación pueden ser muy importantes.

4.4.1 Niveles del Data Center

El instituto de Uptime define 4 niveles en centros de datos en su libro, “Industry Standard Tier Classifications Define SiteInfrastructure Performance” especificamos las mismas:

- Tier I del Centro de Datos: Básico

El Tier I del centro de datos es susceptible a las interrupciones tanto planificadas como una actividad no planeada. Cuenta con la distribución de energía del ordenador y la refrigeración, puede o no tener un piso elevado, UPS, o un generador de motor. Si no tiene UPS o generadores, que son sistemas de un solo módulo y tienen muchos puntos de fallo. La infraestructura debe estar completamente cerrada, se realiza el mantenimiento preventivo y reparación anual. Situaciones urgentes pueden requerir paradas más frecuentes. Errores de operación o fallas espontáneas de los componentes de infraestructura del lugar causarán una interrupción del centro de datos.

- Tier II Centro de Datos: Componentes Redundantes

Tier II instalaciones con componentes redundantes son ligeramente menos susceptibles a las interrupciones tanto planificada como actividad no planeada de un centro de datos básico. Tienen un piso elevado, UPS y generadores de motor, pero su diseño es la capacidad de "Componentes Redundantes" (N+1), que tiene una vía de distribución de un único subproceso en todo. Mantenimiento de la ruta crítica de potencia y otras partes de la infraestructura del lugar requerirá un cierre de procesamiento.

- Tier III del centro de datos: Al mismo tiempo Mantenible

Capacidad de nivel Tier III permite cualquier actividad de la infraestructura del lugar planeado sin interrumpir el funcionamiento del hardware informático de ninguna forma. Las actividades previstas incluyen el mantenimiento preventivo y programable, la reparación y sustitución de componentes, adición o eliminación de componentes de capacidad, pruebas de componentes, sistemas y más. Para

grandes lugares que utilizan agua fría, esto significa dos conjuntos independientes de las tuberías. La capacidad y la distribución, debe ser suficiente para llevar al mismo tiempo la carga en una ruta de acceso durante el mantenimiento o las pruebas por el otro camino. Actividades no planificadas, tales como errores en el funcionamiento o fallas espontáneas de los componentes de infraestructura instalados, aún causarán una interrupción del centro de datos. Sitios de nivel III son a menudo diseñados para ser ascendidos a Tier IV en caso de negocio del cliente justifica el costo de la protección adicional.

- Tier IV Centro de Datos: Tolerante a Fallos

Tier IV ofrece capacidades de la infraestructura del sitio además de permitir cualquier actividad planeada sin interrupciones a la carga crítica. Funcionalidad tolerante a fallos también proporciona la capacidad de la infraestructura de sitio para sostener al menos un peor caso de fallo o evento no planeado con ningún impacto carga crítica. Esto requiere de rutas de distribución simultáneamente activas, típicamente en una configuración System + System. Eléctricamente, esto significa dos sistemas UPS separados en los que cada sistema tiene redundancia N +1. A causa de incendios y códigos de seguridad eléctrica, todavía habrá tiempo de inactividad debido a la exposición a las alarmas de incendio o personas que inician un apagado de emergencia (EPO). Requiere que todos los equipos informáticos deben tener entradas de alimentación dual según la definición de Tolerancia a Fallos de alimentación Conformidad con las especificaciones del Instituto.

Infraestructuras sitio de Nivel IV son los más compatibles con los conceptos de TI de alta disponibilidad que emplean agrupación CPU, DASD RAID y comunicaciones redundantes para lograr confiabilidad, disponibilidad y capacidad de servicio.

4.4.2 Niveles, Comunicaciones

- Tier 1 (telecomunicaciones)

La infraestructura de telecomunicaciones debe cumplir con los requisitos de esta Norma para ser calificados como mínimo con el nivel 1. La misma tendrá un espacio de mantenimiento propiedad del cliente y una vía de entrada a la instalación. Los servicios del proveedor de acceso se darán por terminado en un plazo de un cuarto de entrada / Cuarto de Comunicaciones. La infraestructura de comunicaciones se distribuirá de la sala de entrada de la distribución principal y áreas de distribución horizontal en todo el centro de datos a través de una única vía. Aunque la redundancia lógica puede ser incorporada en la topología de la red, no habría ninguna redundancia física o diversificación establecida dentro de una instalación de nivel 1.

Etiquete todos los paneles de conexión, enchufes y cables como se describe en ANSI/TIA/EIA-606-A y anexo B de la presente Norma. Además etiquetar todos los armarios y bastidores con su identificador en la parte delantera y trasera.

Algunos puntos únicos de fallo potenciales de una instalación de nivel 1 son los siguientes:

- Fallo del equipo proveedor de acceso;

- Router o fallo del interruptor, si no son redundantes;
- Cualquier evento catastrófico en la sala de entrada, área de distribución principal, o el espacio de mantenimiento que pueda interrumpir todos los servicios de telecomunicaciones en el centro de datos;
- Los daños a la columna vertebral o el cableado horizontal.

- Tier 2 (telecomunicaciones)

La infraestructura de telecomunicaciones debe cumplir con los requisitos de nivel 1.

Equipos de telecomunicaciones críticos, acceso proveedor a equipos de aprovisionamiento y producción, routers, switches, LAN y SAN, deben tener componentes redundantes (fuentes de alimentación, procesadores, etc.).

Configuraciones lógicas son posibles y pueden estar en una topología de anillo o malla superpuesta a la configuración en estrella física.

Una instalación de nivel 2 se ocupa de la vulnerabilidad de los servicios de telecomunicaciones que entran al edificio.

Una instalación de nivel 2 debería tener dos lapsos de mantenimiento para la propiedad del cliente y las vías de entrada a la instalación. Las dos vías de acceso redundantes se terminarán dentro de una sala de entrada. Se recomienda la separación física de las vías de los orificios de mantenimiento redundantes a la sala de entrada a ser de un mínimo de 20 m (66 pies) a lo largo de toda la ruta. Se

recomiendan las vías de acceso para entrar en los extremos opuestos de la sala de entrada. No se recomienda que las vías de acceso redundantes que entran a la instalación en la misma zona que estos nos vayan a proporcionar, la separación recomendada a lo largo de toda la ruta.

Todos los cables de conexión y los puentes deben estar etiquetados en ambos extremos del este con el nombre de la conexión en ambos extremos del mismo para clasificar el centro de datos de nivel 2.

Algunos puntos únicos de fallo potenciales de una instalación de nivel 2 son:

- Equipos de proveedor de acceso se encuentran en la sala de entrada conectados a misma distribución eléctrica y el apoyo de los componentes o sistemas de climatización individuales;
- Enrutamiento redundante y hardware núcleo de conmutación situado en la zona de distribución principal conectado a misma distribución eléctrica y el apoyo de componentes o sistemas de HVAC individuales;
- El hardware de conmutación de distribución redundante situado en el área de distribución horizontal conectado a la misma distribución eléctrica y el apoyo de componentes o sistemas de HVAC individuales;
- Cualquier evento catastrófico en la sala de entrada o área de distribución principal puede interrumpir todos los servicios de telecomunicaciones en el centro de datos.

- Nivel 3 (telecomunicaciones)

La infraestructura de telecomunicaciones debe cumplir los requisitos del nivel 2.

El centro de datos se debe contener por lo menos dos proveedores de acceso. El mantenimiento deberá ser realizado a partir de al menos dos oficinas centrales de proveedores de acceso diferentes o puntos de presencias. Proveedor de acceso cableado desde sus oficinas centrales o puntos de presencia debe estar separado por lo menos 20 m (66 pies) a lo largo de toda su ruta para las rutas que deben ser considerados diversamente enrutado.

El centro de datos debería tener dos salas de ingreso preferentemente en los extremos opuestos del centro de datos, pero un mínimo de 20 m (66 pies) de separación física entre las dos habitaciones. No comparta el acceso a equipos proveedor de aprovisionamiento, las zonas de protección contra incendios, unidades de distribución de energía y equipos de aire acondicionado entre las dos salas de ingreso. El equipo de aprovisionamiento de proveedor de acceso en cada sala de entrada debe ser capaz de seguir operando si el equipo en el otro cuarto de entrada / Cuarto de Comunicaciones falla.

El centro de datos debe tener vías troncales redundantes entre las salas de entrada, área de distribución principal y áreas de distribución horizontal.

Centro de datos Intra LAN y SAN cableado troncal de los interruptores en las áreas de distribución horizontal a conmutadores de red troncal en el área principal de distribución deben tener pares de fibras o hilos redundantes dentro de la configuración general de la estrella. Las conexiones redundantes deben estar en fundas de cable diversamente enrutados.

No debe haber una copia de seguridad "en caliente" de espera para todos los equipos de telecomunicaciones críticos, acceso equipamiento proveedor de aprovisionamiento, los routers de producción de capa base y capa de la base de producción de LAN / SAN switches.

Todos los cables, las conexiones cruzadas y los cables de conexión deben documentarse utilizando hojas de cálculo, bases de datos o programas diseñados para realizar la administración de cables. La documentación del sistema de cableado es un requisito para un centro de datos para ser clasificado de nivel 3.

Algunos puntos únicos de fallo potenciales de una instalación de nivel 3 son:

- Cualquier evento catastrófico en la zona principal de distribución puede interrumpir todos los servicios de telecomunicaciones en el centro de datos;
- Cualquier evento catastrófico dentro de un área de distribución horizontal puede interrumpir todos los servicios a los servidores el área de TI.

- Nivel 4 (telecomunicaciones)

La infraestructura de telecomunicaciones debe cumplir con los requisitos de nivel 3.

El cableado troncal del centro de datos debe ser redundante. El cableado entre dos espacios debe seguir físicamente rutas separadas, con caminos comunes sólo dentro de los dos espacios finales. El cableado Troncal debe ser protegido por el encaminamiento a través del conducto o mediante el uso de cables con armadura de enclavamiento.

Debe haber copias de seguridad automáticas de todos los equipos de telecomunicaciones críticos, acceso equipamiento proveedor de aprovisionamiento, los routers de producción de capa base y capa de la base de producción de LAN / SAN switches. Sesiones / conexiones deben cambiar automáticamente a los equipos de copia de seguridad.

El centro de datos debe tener un área de distribución principal y el área de distribución secundaria, preferiblemente en extremos opuestos del centro de datos, pero un mínimo de 20 m (66 pies) de separación física entre los dos espacios. No comparta las zonas de protección contra incendios, unidades de distribución de energía y equipos de aire acondicionado entre el área de distribución principal y el área de distribución secundaria. El área de distribución secundaria es opcional, si la sala de ordenadores es un único espacio continuo, probablemente hay poco que ganar mediante la implementación de un área de distribución secundaria.

El área de distribución principal y el área de distribución secundaria tendrán cada uno un camino a cada sala de entrada. También debe existir la vía entre el área de distribución principal y el área de distribución secundaria.

Los routers de distribución redundantes e interruptores deben ser distribuidos entre la zona de distribución principal y el área de distribución secundaria de tal manera que las redes de centros de datos pueden continuar la operación si el área de distribución principal, área de distribución secundaria, o una de las habitaciones de entrada tiene un fallo total.

Cada una de las áreas de distribución horizontal debería disponer de conectividad tanto a la zona de distribución principal y el área de distribución secundaria.

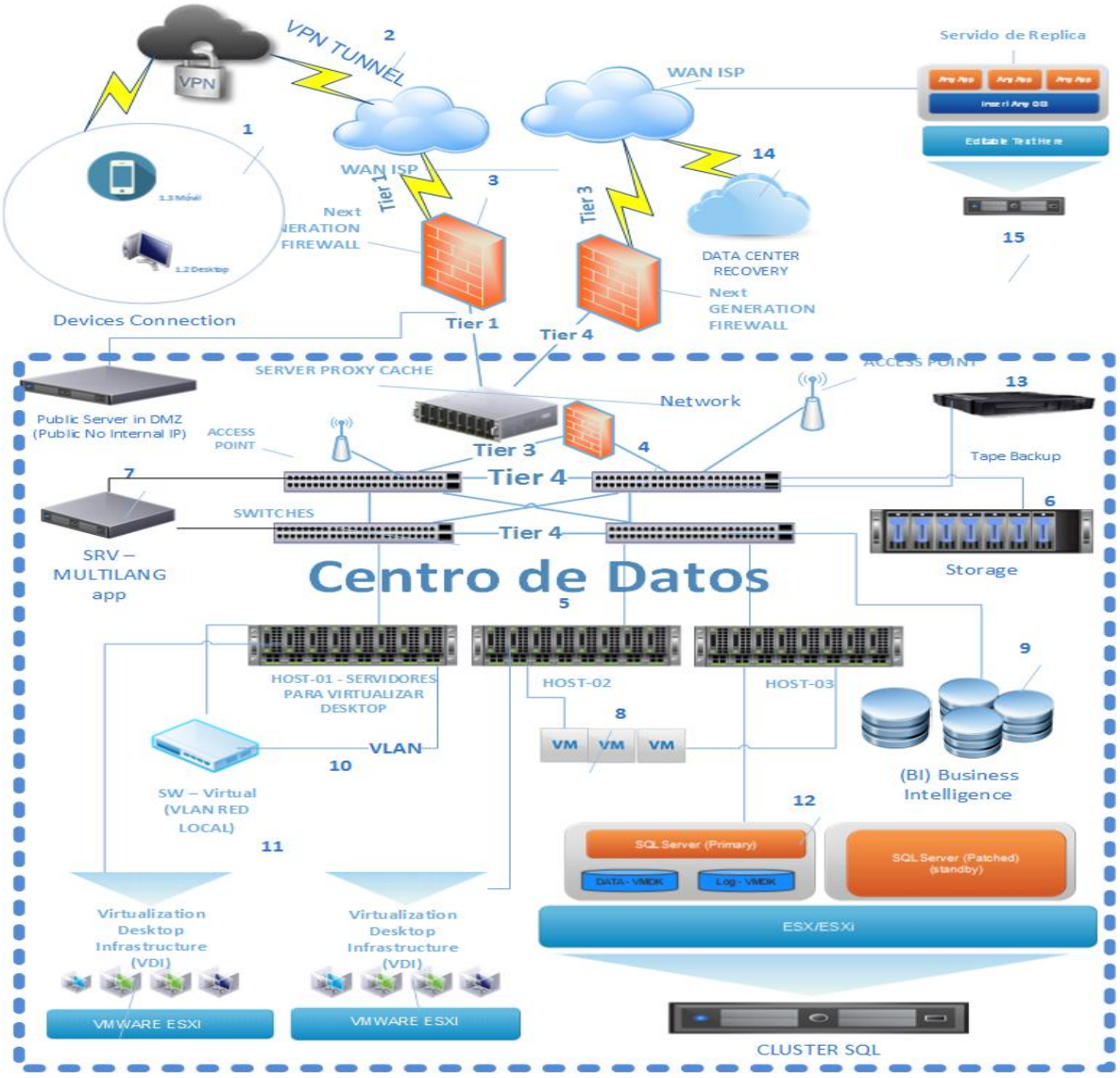
Los sistemas críticos deben tener cableado horizontal a dos áreas de distribución horizontal. Cableado horizontal redundante es opcional, incluso para niveles 4 de instalación.

Algunos puntos únicos de fallo potenciales de una instalación de nivel 4 son:

- El área de distribución principal (si no se implementa el área de distribución secundaria);
- En el área de distribución horizontal y el cableado horizontal (si el cableado horizontal redundante no está instalado).

Según la norma ANSI/ TIA 942, Un centro de datos es un espacio o edificio cuya objetivo primordial contener un cuarto de cómputo y sus áreas de soporte. También busca centralizar la infraestructura tecnológica (Servidores, Comunicaciones, Computadoras, etc.) para garantizar la disponibilidad y optimizar su gestión.

Esta norma ayuda a través de técnicas específicas a como diseñar la infraestructura de un centro de datos cubriendo áreas como distribución de espacio, del cableado y consideraciones ambiente adecuado, además de establecer recomendaciones para construirlo, y un conjunto de directrices para centros de datos de aplicación.



Fuente: Propia

Grafico Antroyecto. Distribución y Redundancia Según Estándar TIA-942

Como se observa en el grafico se aplica la norma TIA-942 a la infraestructura, con las Tiers correspondientes y sus enlaces troncales y horizontales.

CAPITULO 5 -

Sistema de continuidad basado en la nube.

En esta parte vamos a mostrar ampliamente la evaluación de las normas, recomendaciones y estándares internacionales actuales, para garantizar el diseño de infraestructura tecnológica que permita alta disponibilidad en la gestión y administración de datos.

Fuente: Propia

Figura 13. Sistema de Continuidad y Administración Centro de Datos

En esta parte vamos a tomar en cuenta la evaluación de las normas, recomendaciones y estándares internacionales actuales para garantizar alta disponibilidad. Con esto buscamos ofrecer una propuesta a la organización obteniendo así un marco de referencia, que sirva como base, para el soporte continuo de sus procesos de negocios, minimizando los riesgos existentes que pueden afectar la continuidad y competitividad de las mismas, logrando por consiguiente un óptimo desempeño en la gestión y administración de los datos que maneja la institución.

Existen estándares internacionales que ayudaran a enriquecer esta investigación, se listan a continuación:

- Estándares Internacionales TIA 942 Infraestructura de Telecomunicación.
- Estándares para centro de datos. ANSI/TIA/EIA-568 Cableado de telecomunicaciones para edificios comerciales.
- ANSI/TIA/EIA-569 Espacios y canalizaciones para telecomunicaciones en edificios comerciales.
- ANSI/TIA/EIA 607 Tierras y aterramientos para los sistemas de telecomunicaciones de edificios comerciales.
- ANSI/TIA/EIA-568-B: Cableado de Telecomunicaciones en Edificios Comerciales. (Cómo instalar el Cableado).
- TIA/EIA 568-B1 Requerimientos generales.
- TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.

5.1 Fases del Estudio

Para obtener una infraestructura tecnología de alta disponibilidad debemos hacer énfasis en tres fases que aportan grandes beneficios a la misma:

- Fase de Diagnóstico de la situación actual de la Infraestructura Tecnológica.
- Fase de Estudio de Factibilidad del proyecto desde el punto de vista operativo, técnico y económico.

- Fase de Diseño de una Infraestructura Tecnológica que permita alta disponibilidad. Este estudio se apoyará en la investigación monográfica documental y de campo.

5.1.1 FASE I – DIAGNÓSTICO

Se comprobó que el espacio que se está utilizando actualmente no es factible, de tal manera que se debe realizar un levantamiento del campo, localizar los puntos críticos y una mejor ubicación que contemplen los estándares internacionales para la infraestructura tecnológica.

Según Hernández, (2.003), "…la elección de los elementos no dependen de la probabilidad, sino de causas relacionadas con el investigador o la persona que hace la muestra".

- **Recolección de datos – Técnicas e instrumentos**

Unas de las herramientas más utilizadas fue la observación, gracias a la misma pudimos obtener información relevante del campo, ya que mediante la misma estudiamos las personas y su entorno en sus actividades cotidianas y además miembros de la institución.

Fernández (1995) "implica la observación directa de una situación específica, con un sistema predefinido de categorías clasificatorias…"

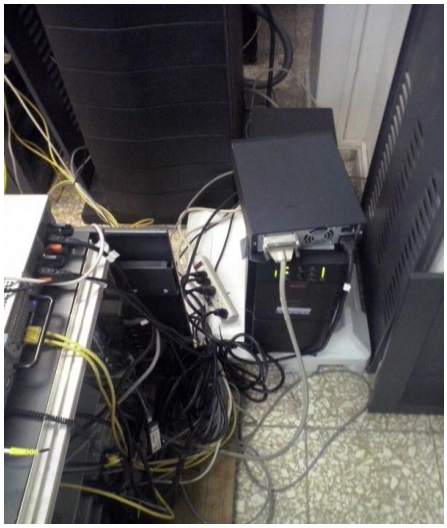
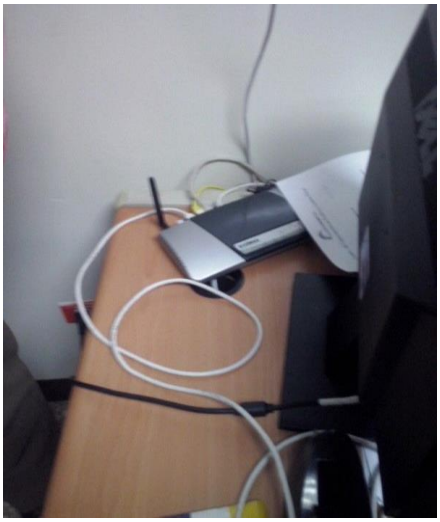
Analizamos como se realizan los procesos de productividad del día a día, quien los hace, cuando se llevan a cabo, cuánto tiempo se toman, donde los hacen, etc.

Utilizamos la técnica de la entrevista para obtener información, a través de preguntas cerradas (SI/NO) acerca de la institución.

Hernández (2003) de la siguiente manera: “En las entrevistas estructuradas, el entrevistador realiza su labor basándose en una guía de preguntas específicas y se sujeta exclusivamente a ésta.”

En tercer plano se utilizó la encuesta para recopilar datos importantes como son las necesidades y preferencias de los usuarios, además de los clientes.

- Observación Directa

5.1.2 FASE 2: ESTUDIO DE FACTIBILIDAD

Gracias a esta fase podremos comprobar y verificar el uso eficiente de los recursos tecnológicos así como comprobar los efectos de este proyecto en el área especificada en la fase de Diagnostico según el levamiento y los estándares internacionales.

Comprobaremos además cual es la factibilidad técnica, operativa y económica realizando un diseño eficiente de la infraestructura.

En esta fase acota Hernández, (2.003) "… es donde se establecen los criterios que permiten asegurar el uso óptimo de los recursos empleados así como los efectos del proyecto en el área o sector al que se destina".

- **Factibilidad Operativa**

En este sentido Scott (1.988) detalla tres (3) cuestionamientos:

1. Un nuevo sistema puede ser demasiado complejo para los usuarios de la organización o los operadores del sistema. En este caso, los usuarios pueden ignorarlo o usarlo de tal forma que cause errores.
2. Un nuevo sistema puede hacer que los usuarios se resistan a él, como consecuencia de una técnica de trabajo, miedo a ser desplazados, interés en el sistema antiguo u otras razones.
3. Un nuevo sistema puede introducir cambios demasiado rápido que impidan que el personal pueda adaptarse a él o aceptarlo.

- **Factibilidad Técnica**

Según Kendall (1.997) “una gran parte de la valoración de recursos tiene que ver con la factibilidad técnica, se debe encontrar si los recursos técnicos actuales pueden ser mejorados o añadidos, en forma tal que satisfagan la petición bajo consideración”.

De igual manera Kendall (ob.cit) menciona “si la respuesta sobre si una tecnología particular se encuentra disponible y es capaz de satisfacer las peticiones del usuario es “si”, entonces la pregunta se convierte en económica”.

- **Factibilidad Económica**

Según Kendall (1.997) los recursos básicos a considerar en cuanto a la factibilidad económica son: “el tiempo propio y el del equipo de sistemas, el costo del tiempo de los empleados del negocio, el costo estimado de hardware y el costo estimado de software y/o desarrollos de software”.

De esta manera conoceremos el estimado de la inversión que necesitamos para la ejecución de dicho proyecto, haciendo énfasis en los recursos materiales como en los humanos.

5.1.3 FASE 3: DISEÑO DEL PROYECTO

Ya en esta fase vamos a elaborar la propuesta del proyecto, de acuerdo con las normas y estándares internacionales ya mencionados, además identificaremos los beneficios y los actores claves.

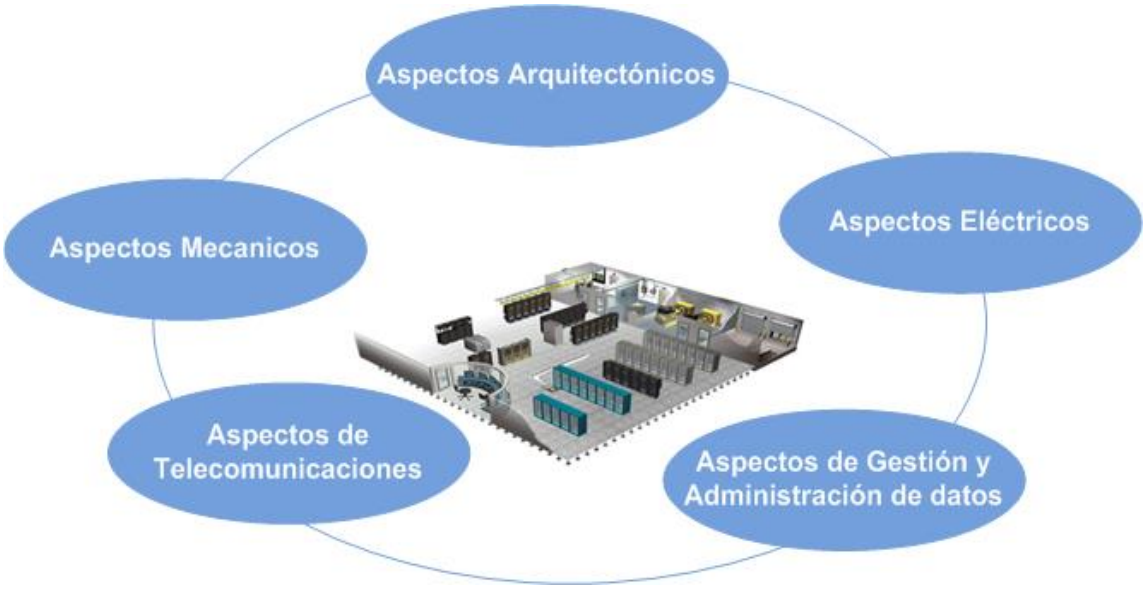
- Veremos cuales aspectos los aspectos contemplados en el estándar y las normas, para tomar en cuenta en el diseño de la infraestructura tecnológica, que permita una alta disponibilidad y una buena administración de datos de la institución.
- Observaremos cada sub-componente del modelo, a los cuales llamaremos sub-modelos, con las normas generales necesarias para el diseño de la infraestructura tecnológica, que permita una alta disponibilidad y una buena administración de datos de la institución.
- Aplicaremos cada sub-modelo, con las recomendaciones necesarias para el diseño de la infraestructura tecnológica, que permita una alta disponibilidad y una buena administración de datos de la institución.

5.1.3.1 Aspectos del Diseño

Desplegaremos algunos aspectos fundamentales para brindar un diseño de alta disponibilidad:

- Aspectos Arquitectónicos: Nos ayudara en todo el contorno del centro de datos, una correcta alimentación eléctrica, controles de acceso, prevenciones de incidentes ambientales, seguridad de cámaras, etc., todo lo que nos pueda afectar en la productividad de la organización para mantener la continuidad del negocio.
- Aspectos Eléctricos: Como su nombre lo indica, y de la manos de las normas y estándares internacionales nos ayudara a mantener una alta disponibilidad de nuestra infraestructura.

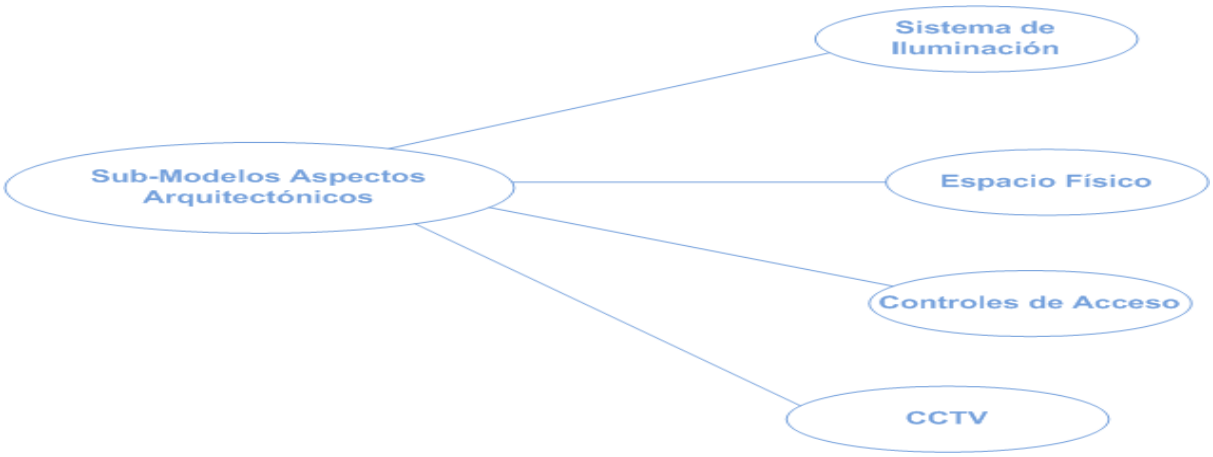
- Aspectos de Gestión y Administración de Datos: Nos aportara la ayuda necesaria tanto para el entorno físico y virtual de los equipos de la institución. El mismo es clave para mantener las operaciones de la institución de manera óptima.
- Aspectos de Telecomunicaciones: Se conjugan las mejores prácticas del mercado, según los estándares internaciones, además de recomendaciones y aportes a la comunicación de toda la infraestructura voz, data y video.
- Aspectos Mecánicos: Por último y no menos importante, veremos aquí los puntos importantes en cuanto a la ambientalización, prevenciones contra incendios, etc. Siempre de la mano de las normas.



Fuente: Propia

Figura 14. Aspectos del Diseño.

5.1.3.2 Aspectos Arquitectónicos



Fuente: Propia

Figura 15. Aspectos Arquitectónicos.

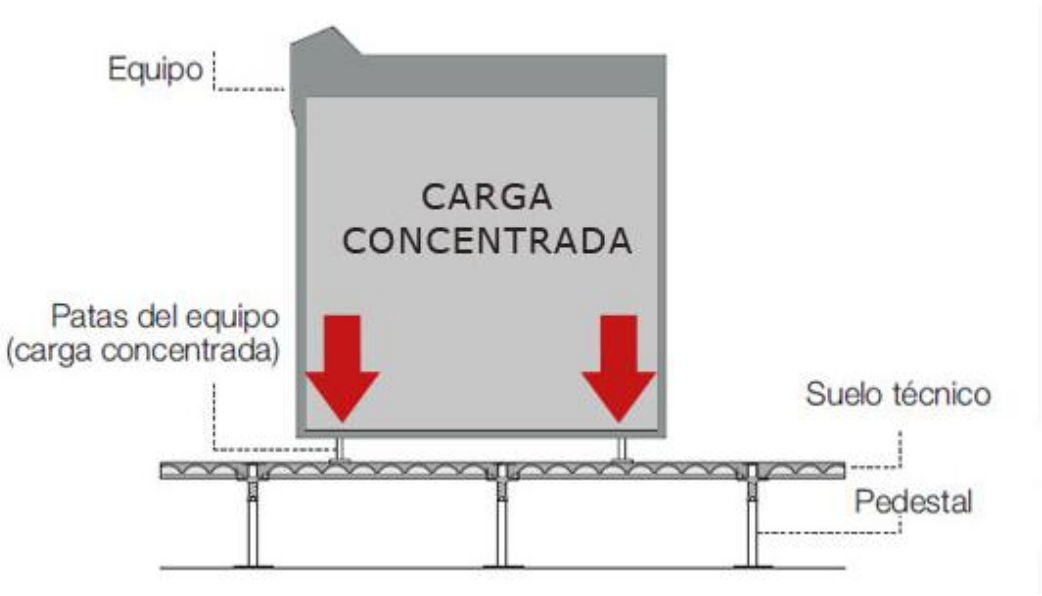
Este aspecto es uno de los más importantes ya que en el mismo definiremos cerramiento perimetral, dotación de suelo técnico sobre elevado de calidad sala informática, falso techo de placas de fibra de vidrio.

El centro de datos en general, deben pasar por las fases pertinentes para definir el área adecuada para tales fines, que cuenten con máxima medidas de seguridad, garantizando su funcionamiento, dentro de las normas que este tipo de locales exige.

Los mismos deben disponer de los siguientes componentes:

- **Pisos técnicos y Techos Falsos**

Estos deben ser apropiados para el uso en salas informáticas, con alturas suficientes para el paso de conductos y en el caso de los suelos en específico con capacidades de cargas máxima por metro cuadrado de 1000 kg como mínimo, deben ser de caucho, antideslizante, antiestático y anti polvo, con grosor de al menos 2 cm.



Fuente: olaretta.com

Figura 16. Concentración de Carga.

- Consideraciones para el Diseño del Piso Técnico:

Para efectos del diseño es importante tener en cuenta:

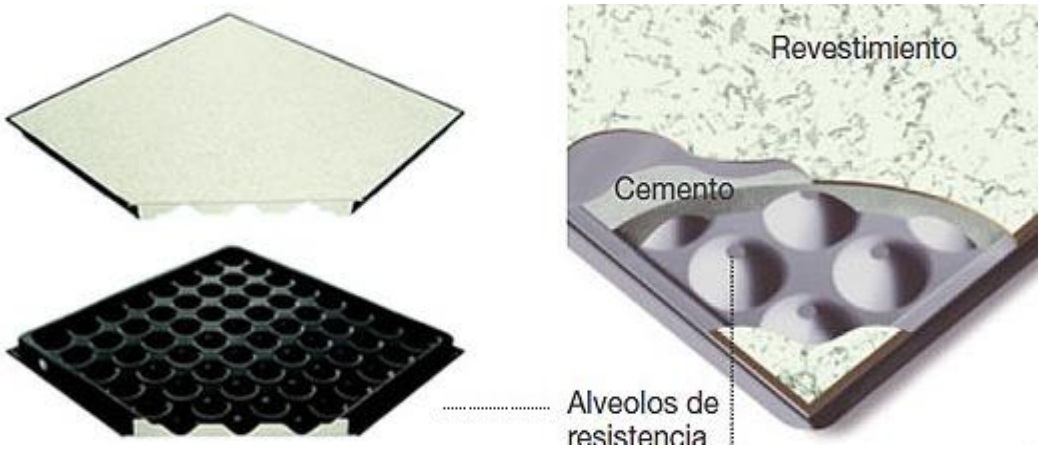
- El área que contará con el Piso Elevado.
- La altura, desde el nivel del suelo a la que será colocado.

- Escalón o escalerilla metálica, se debe indicar el número de pasos, así como el ancho de la misma.
- Opcionalmente podría ser necesario una rampa para facilitar el ingreso de equipos y muebles pesados, se deberá diseñar la mejor ubicación. También puede ser una alternativa a la escalerilla metálica.
- Herramienta para levantar las baldosas conocida como ventosa.

- Baldosa 600 mm. x 600 mm. x 35 mm:

  - La baldosa cuenta con una carcasa metálica electro-soldada estampada multiforme con relleno inyectado de argamasa homogénea de cemento, fibra de celulosa y agregados naturales en formato de medida de 600 x 600 x 35 mm con cubiertas de HPL (High Pressure Laminate) anti estática de 1.5 mm y protegidas con perfiles perimetrales de PVC.
  - La baldosa está diseñada para soportar cargas fijas y dinámicas, y es ofrecida en tres modelos, Mediano, Fuerte y Extra fuerte, según la capacidad de carga que se vaya a aplicar, ver tabla de datos.
  - La baldosa, tiene componentes completamente No Combustibles, en cumplimiento de la Norma ASTM E-136.

- Protección y Acabado de la baldosa en pintura electrostática en polvo Epóxica.
- Clase A para propagación de llama y desarrollo de humos (ASTM-E84-1998).
- Todo el sistema cumple con los requerimientos de MOB PF2 PS/SPU Platform Raised Access Floors Performance Specification (UK) para sus respectivas clasificaciones y CISCA (Theceiling& interior systemsconstructionassociation).
- Resistencia Eléctrica: 1×105 Ω~1×109 Ω según Norma NFPA 99.



Fuente: olaretta.com

Figura 17. Piso Falso.

Debemos de tener en cuenta que las paredes y el techo deben contener tonos claros para tener una mayor visibilidad y claridad en el mismo a partir de la iluminación.[8]

- Sistema de Iluminación

Aspecto importante con el que debe contar un centro de datos es con una buena iluminación en toda el área, esta facilitara en las operaciones de todos los equipos y aportaran ayuda en el mantenimiento de los mismos.

En el instituto se instalaran las estaciones de trabajo en orden paralelo, de esta forma los focos o lámparas colocaras en el techo o pared darán mejor enfoque en el trabajo que se esté realizando de esta forma evitamos inconvenientes como fatiga de la vista y mala visualización del entorno. Se pintaran las paredes con un color claro para mejorar la reflexión.

- Normas y Reglas

  - El sistema de iluminación debe ser eficiente para evitar reflejos en las pantallas del computador, la falta de luz en puntos estratégicos ayudara y evitara incidencia directa del sol sobre los equipos.
  - No debemos permitir que la iluminación dependa de una conexión donde también estén los equipos de cómputo.

[8] http://olaretta.com/index.php?option=com_content&view=article&id=62&Itemid=94&limitstart=3

- Del 100% de la iluminación, deberá distribuirse el 25% para la iluminación de emergencia y se conectará al sistema de fuerza continúa.
- Los reactores deben estar fuera, ya que generan campos magnéticos, o en su caso deben aislarse.
- En el área de computadoras debe mantenerse un promedio mínimo de 450 lúmenes midiendo a unos 70 cm del suelo.

- **Controles de Acceso**

Figura 5.1.3.4 Controles de Acceso

Fuente: tecnocomprascr

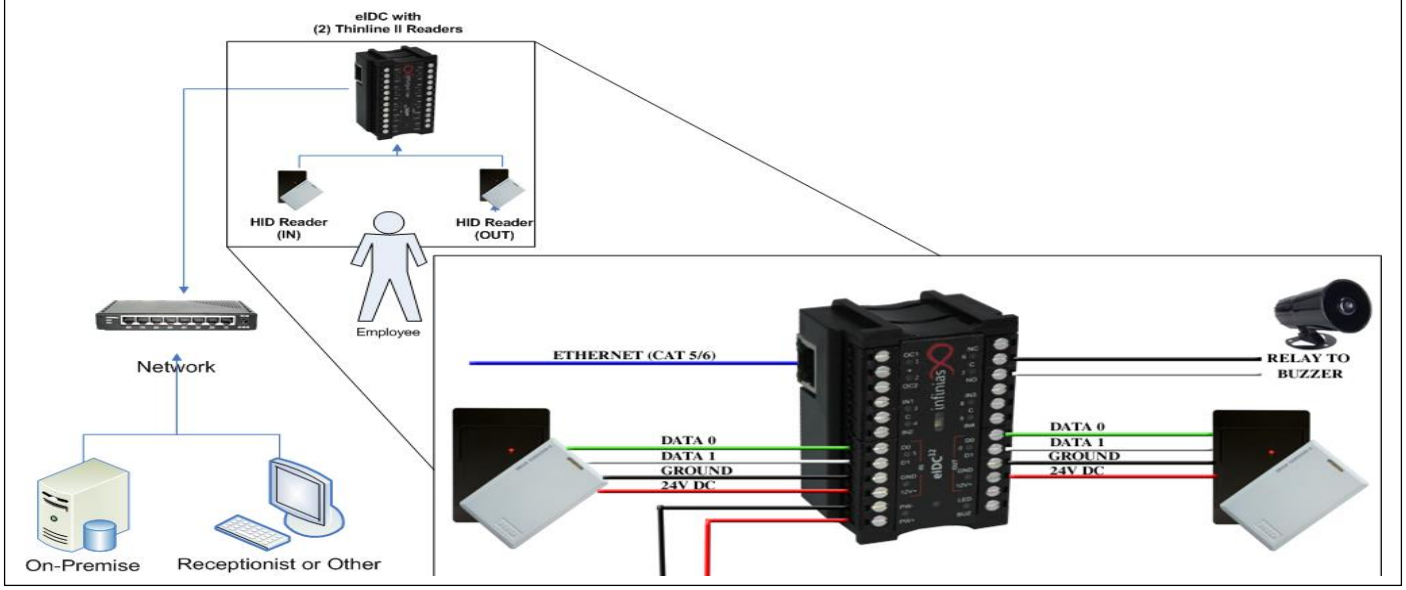


Figura 18. Control de Acceso

Fuente: tecnocomprascr.com

El centro de datos debe contar con dos puntos de control de acceso, verificación y registro de las personas que accedan al edificio.

- Sistema de Control de Acceso Biométrico

  Todos sabemos que un centro de datos es el lugar donde la seguridad debe ser más crítica, ya que en el mismo se registran o almacenan todas las informaciones y los datos importantes de la institución. Gracias a este sistema se podrá monitorear todas aquellas actividades que afecten la seguridad física del centro de datos.

- ¿Cómo funciona un lector Biométrico?

Con un sensor el lector biométrico escanea las huellas dactilares mediante un algoritmo propio, el mismo los transforma en parámetros numéricos para su lectura. El software es el motor del lector claro dependerá también de la capacidad en potencia y rapidez de hardware del dispositivo aportando la seguridad de almacenaje de huellas.

En el centro de datos de la organización serán instalados 2 puntos de accesos los cuales contaran con lectores biométricos, tarjeta magnética y escaneo facial. Además el mismo tendrá un monitoreo constante de las actividades en dicho lugar.

- **CCTV**

Figura 19. CCTV
Fuente: tecnocomprascr.com

- Como se conforma un CCTV?

  Debemos de armar el equipamiento partiendo de la premisa más básica y sencilla es decir sus componentes principales,

  - CAMARA
  - CABLE
  - MONITOR

  A partir de allí podremos diseñar nuestro sistema agregándole los accesorios que necesitaremos de acuerdo a los requerimientos del cliente y al criterio de seguridad utilizado, por ejemplo.

  - SECUENCIADORES
  - CUADRIPLICADORES DE PANTALLA
  - MULTIPLEXORES
  - LENTES
  - CONTROLADORES
  - UNIDADES DE PANEO O PANEO Y CABEZEO
  - PROTECTORES
  - VIDEOGRABADORAS
  - SISTEMAS DE TRANSMISION DE VIDEO (cable, inalámbrica, telefónica, etc.)

- ¿Para qué sirve el CCTV en seguridad?

  El CCTV nos debe permitir realizar identificaciones durante o después del suceso que está visualizando. Por eso es muy

importante definir qué función van a cumplir y donde serán colocadas las cámaras, estas deben permitir realizar tres tipos de identificaciones:

- Personal: esta se refiere a la capacidad del espectador de identificar personalmente alguien o algo (Caras, cajas, etc.).
- De acción: esta interactúa mucho con la anterior y debe permitir verificar que realmente sucedió un hecho (Movimientos).
- De escena: se debe poder identificar un lugar de otro similar por la ubicación.

- ¿Cómo se deben seleccionar las cámaras?

  Las cámaras deben seleccionarse de acuerdo a tres criterios

  1. Sensibilidad: se refiere a la cantidad real de luz visible o infrarroja necesaria para producir una imagen de calidad.
  2. Resolución: define la calidad de imagen a partir de un detalle o perspectiva de reproducción.
  3. Características: son ajustes extras que le dan ventaja sobre otras cámaras.

- ¿Cómo diseñar un sistema de CCTV?

  Se deben tomar en cuenta siete pasos para el correcto diseño:

1. Determinar el propósito del sistema de CCTV, y escribir un párrafo simple con el propósito de cada cámara en el sistema.
2. Definir las áreas que cada cámara visualizara.
3. Elegir el lente apropiado para cada cámara.
4. Determinar donde se localizara el monitor o monitores para visualizar el sistema.
5. Determinar el mejor método para transmitir la señal de vídeo de la cámara al monitor.
6. Diseñar el área de control.
7. Elegir el equipo con base en las notas del diseño del sistema.

En nuestro caso no disponemos de un sistema de cámaras y estamos vulnerables ante cualquier eventualidad por ende en este proyecto en específico se recomienda colocar las mismas tanto en el exterior como interior del centro de datos. En el interior debemos colocar 3 cámaras, una que vigile la puerta, otra que vigile el rack de comunicaciones y por ultimo una que vigile los servidores, storage, etc. En caso del Exterior debemos colocar una cámara dirigida a la puerta para verificar los accesos al centro de datos.

5.1.3.3 Aspectos Eléctricos

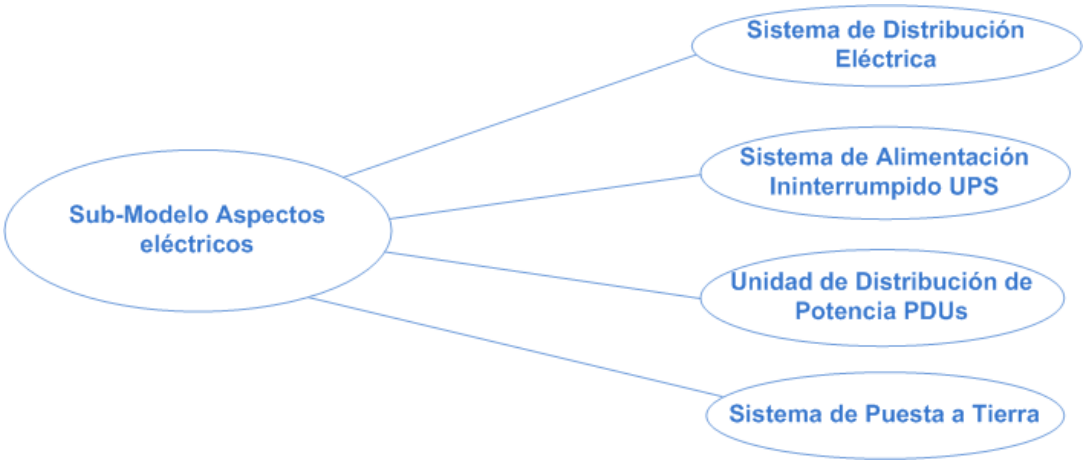


Figura 20. Aspectos Eléctricos

Fuente: Propia

Este es uno de los aspectos más importantes a la hora de diseñar un centro de datos, ya que si no disponemos de un estándar y normas que redactan como se efectúa un buen cálculo sobre la energía o carga a utilizar, podríamos tener consecuencias desastrosas además de pérdidas de datos.

- Requisitos eléctricos Generales (Entrada de servicios y utilidad de distribución primaria)

Se debe considerar a otros clientes de servicios públicos atendidos por el mismo alimentador de utilidad. Los hospitales son los preferidos, ya que suelen recibir gran prioridad durante los cortes. Los usuarios industriales que comparten suministros eléctricos entrantes no son preferidos debido a los transitorios y armónicos que a menudo imponen a los alimentadores.

Alimentadores de servicios públicos son preferibles a los alimentadores generales para reducir al mínimo la exposición a los rayos, los árboles, los accidentes de tráfico, y el vandalismo.

El interruptor principal debe estar diseñado para el crecimiento, el mantenimiento y la redundancia. Una configuración redundante doble extremo (principal-tie-principal) o aislado debe ser proporcionada. El bus de conmutación debe ser de gran tamaño ya que este sistema es el menos ampliable una vez que comiencen las operaciones. Breakers deben ser intercambiables en lo posible entre los espacios y alineaciones de aparamenta. El diseño debe permitir el mantenimiento de los interruptores, el autobús, y / o interruptores. El sistema debe permitir la flexibilidad de cambiar a satisfacer la mantenibilidad total. El transistor de supresión y sobretensión (TVSS) se debe instalar en cada nivel del sistema de distribución, y tener el tamaño apropiado para suprimir la energía transitoria que es probable que ocurra.

- Generación Standby

El sistema de generación de espera es el factor de resiliencia individual más importante y debe ser capaz de proporcionar un suministro de calidad razonable y la resistencia directamente a los equipos informáticos y de telecomunicaciones si hay un fallo de red.

Los generadores deben ser diseñados para suministrar la corriente armónica impuesta por el sistema UPS o cargas de equipo informático. Requerimientos de arranque del motor deben ser analizados para asegurar que el sistema generador

es capaz de suministrar corrientes de motor de partida requerido con una caída de tensión máxima de 15% en el motor. Las interacciones entre el UPS y el generador pueden causar problemas si no se ha especificado correctamente el generador; necesidades exactas deben ser coordinadas entre el generador y los vendedores de UPS. Una variedad de soluciones disponibles para hacer frente a estos requisitos, incluyendo filtros de armónicos, reactores de línea, generadores especialmente para heridas, el arranque del motor con retardo de tiempo, por etapas de transferencia, y el generador de-rating.

Cuando se disponga de un sistema generador de energía de reserva debe proporcionarse a todos los equipos de aire acondicionado para evitar la sobrecarga térmica y de apagado. Generadores proporcionan poco o ningún beneficio a la continuidad general de las operaciones si no son compatibles con los sistemas mecánicos.

Generadores en paralelo deben ser capaces de sincronización manual en caso de fallo de los controles de sincronización automática. Debería considerarse la posibilidad de bypass manual de cada generador para alimentar directamente cargas individuales en caso de avería o mantenimiento de las celdas en paralelo.

Supresores de sobretensión transitoria (TVSS) debe ser proporcionada por cada salida del generador.

Combustible para grupos electrógenos diesel debe ser para un arranque más rápido en lugar de gas natural. Así se evitará la dependencia de la compañía de gas y almacenamiento en el lugar de propano. Se debe considerar la cantidad de

almacenamiento de diesel en el lugar requerido, que puede ir de 4 horas a 60 días. Una monitorización remota de combustible y sistema de alarma deben ser proporcionados para todos los sistemas de almacenamiento de combustible. Dado que el crecimiento microbiano es el modo de falla más común de combustible diesel, se debe considerar a los sistemas de clarificación de combustibles portátiles o instalados de forma permanente. En climas más "frías", debe considerarse la posibilidad de calentar o de circulación del sistema de combustible para evitar la gelificación del combustible diesel. El tiempo de respuesta de los proveedores de combustible durante las situaciones de emergencia, deberían tenerse en cuenta al dimensionar el sistema de almacenamiento de combustible en el lugar.

Bancos de carga permanentes o adaptaciones para facilitar la conexión de bancos de carga portátiles son muy recomendables para cualquier sistema generador. Además de la prueba individual de los componentes, el sistema de generación de reserva, los sistemas UPS, y los interruptores de transferencia automática se deben probar en conjunto como un sistema. Como mínimo, las pruebas deben simular una falla de servicio y la restauración de la energía normal. El fallo de los componentes individuales se debe probar en sistemas redundantes diseñados para seguir funcionando durante la falla de un componente. Los sistemas deberán ser probados bajo carga con bancos de carga. Además, una vez que el centro de datos se encuentra en funcionamiento, los sistemas deben ser probados periódicamente para asegurarse de que van a seguir funcionando correctamente.

Del mismo modo, interruptores de transferencia automática con el aislamiento de derivación deben ser proporcionados a servir a los equipos del centro de datos. Interruptores de circuito de transferencia también se pueden usar para transferir cargas de utilidad al generador sin embargo, el aislamiento de derivación de interruptores de circuito debe ser añadido en caso de fallo del interruptor de circuito durante el funcionamiento.

- Sistema de alimentación ininterrumpida (UPS)

Los sistemas UPS pueden ser estáticos, rotativos o de tipo híbrido y pueden ser o bien en línea, fuera de línea o línea interactiva con suficiente tiempo de copia de seguridad para el sistema generador de reserva para venir en línea sin interrupción de la energía. Los sistemas UPS estáticos se han utilizado casi exclusivamente en los Estados Unidos durante los últimos años, y son los únicos sistemas que se describen en detalle en este documento; los conceptos de redundancia descritas son generalmente aplicables a sistemas rotativos o híbridos, así, sin embargo.

Los sistemas UPS pueden consistir en módulos UPS individuales o un grupo de varios módulos en paralelo.

Cada módulo debe estar provisto de un medio de aislamiento individual sin afectar a la integridad de la operación o la redundancia. El sistema debe ser capaz de bypass interno automático y manual y debe ser provista de medios externos para evitar el sistema y evitar la interrupción de la energía en caso de fallo del sistema o de mantenimiento.

Sistemas de baterías individuales se pueden proporcionar para cada módulo; múltiples cadenas de baterías pueden proporcionar para cada módulo para capacidad o redundancia adicional. También es posible para servir a varios módulos UPS desde un sistema de batería única, aunque esto normalmente no se recomienda debido a la fiabilidad muy baja esperada de un sistema de este tipo.

Cuando se instala un sistema de generador, la función principal del sistema UPS es proveer ridethrough durante un corte de energía hasta que los generadores de inicio y venir en línea o los rendimientos de servicios públicos. En teoría, esto implicaría una capacidad de batería requerida de unos pocos segundos. Sin embargo, en la práctica, las baterías deben ser especificadas para un mínimo de capacidad de 5 a 30 minutos con carga UPS nominal completa debido a la naturaleza impredecible de las curvas de salida de la batería y proporcionar cadenas de baterías redundantes o para permitir el cierre ordenado suficiente si el generador sistema falle. Si no se instala un generador, las baterías suficientes deben proporcionar, como mínimo, para que el tiempo requerido para un apagado ordenado del equipo de cómputo; que típicamente estará en el intervalo de 30 minutos a 8 horas. Mayores capacidades de batería a menudo se especifican para instalaciones específicas. Por ejemplo, las compañías telefónicas han ordenado tradicionalmente un tiempo de ejecución de 4 horas donde se proporciona copia de seguridad del generador, y 8 horas, donde se ha instalado ningún generador; empresas de telecomunicaciones y las instalaciones de colocación a menudo se adhieren a estos requerimientos de la compañía telefónica.

Ventilación, calefacción y aire acondicionado, monitoreo de hidrógeno, control de derrames, lavado de ojos y las duchas de seguridad deben ser considerados en una base de caso por caso. Hay dos tecnologías de baterías primarias que se pueden considerar: válvula regulada de plomo-ácido (VRLA), que también se conocen como células selladas o electrolito inmovilizado; y baterías de celdas húmedas. De plomo-ácido reguladas por válvula (VRLA baterías) tienen un tamaño más pequeño que las baterías de celdas húmedas, ya que pueden ser montados en armarios o bastidores, son virtualmente libre de mantenimiento, y por lo general requieren menos ventilación que las baterías de celdas húmedas, ya que tienden a producir menos hidrógeno.

Baterías de celdas húmedas suelen tener costes de ciclo de vida más bajos y una vida útil mucho más larga espera de la válvula regulada baterías (VRLA) de plomo-ácido, pero requieren de un mantenimiento periódico, ocupan más espacio en el suelo, ya que no se pueden montar en armarios, y suelen tener requisitos adicionales de ventilación.

Criterios de diseño típicos pueden especificar una densidad de potencia requerida de cualquier parte 0,38-2,7 kilovatios por metro cuadrado (35 a 250 vatios por pie cuadrado). La selección del sistema de UPS, por tanto, debe basarse en una calificación kW sistema de UPS que cumple los criterios de diseño, que normalmente se superaron antes de la capacidad en kVA sistema UPS. Esto se debe a las calificaciones relativamente bajas de factor de potencia de los módulos UPS en comparación con las necesidades de equipo informático: módulos UPS se clasifican normalmente en el 80% o 90%, o del factor de potencia unidad, frente a

un moderno equipamiento informático que tiene típicamente un factor de potencia de 98% o superior.

Además, un ingreso mínimo de 20% en la capacidad del UPS debe ser proporcionada por encima de ese requisito de densidad de potencia para el crecimiento futuro y para garantizar la potencia del UPS no se exceda durante los períodos de máxima demanda.

Precision Air Conditioning (PAC) unidades deben ser proporcionados por el UPS y salas de baterías. La esperanza de vida de la batería se ven gravemente afectadas por la temperatura; una desviación de la temperatura de cinco grados superior puede acortar la duración de la batería por un año o más. Una temperatura más baja puede hacer que las pilas proporcionan menos de su capacidad.

Los sistemas UPS redundantes pueden ser dispuestos en una configuración diferente. Las tres configuraciones principales están aislados redundante paralelo redundante y distribuyen aislado redundante. La fiabilidad de las configuraciones varía con aisladas redundante distribuido siendo el más confiable.

Los sistemas UPS Stand Alone no se deben utilizar en los circuitos ya soportados por un UPS centralizados, a menos que los sistemas UPS autónomos están vinculados al sistema UPS centralizada y configurados para trabajar en concierto con él. Párese sistemas UPS solamente en circuitos servidos por un sistema de UPS centralizado puede reducir en lugar de mejorar la disponibilidad si funcionan de forma totalmente independiente de las UPS centralizados.

Cualquier sistema UPS ubicadas en la sala de ordenadores debe estar vinculado a la sala de ordenadores del sistema EPO (Emergency Power Off) para que los sistemas de UPS no continúen para proporcionar energía si está activado el EPO.

Información adicional sobre el diseño del sistema UPS está disponible en el estándar IEEE 1100.

- Distribución de energía del ordenador

Unidades de Distribución de Energía (PDU) deben ser considerados para su distribución a los equipos electrónicos crítico en cualquier instalación de centro de datos, ya que combinan la funcionalidad de varios dispositivos en un solo recinto, que a menudo es más pequeño, y más eficaz que la instalación de varios tableros discretos y transformadores. Si el espacio de la sala de ordenadores se subdivide en diferentes salas o espacios de cada uno apoyado por su propio sistema (EPO) apagado de emergencia, a continuación, cada uno de estos espacios debe tener su propia área de distribución horizontal.

PDU deben proporcionar completa con un transformador de aislamiento, supresores de sobretensión transitoria (TVSS), los paneles de salida, y la supervisión de la alimentación. Estos paquetes ofrecen varias ventajas sobre las instalaciones de transformadores y paneles tradicionales.

Una PDU típico incluirá todo lo siguiente:

  - Desconexión del transformador. Disyuntores de entrada dual deben ser considerados para permitir la conexión de un alimentador

temporal para el mantenimiento o la fuente de la reubicación sin necesidad de apagar las cargas críticas;

- Transformador: Este debe estar ubicado lo más cerca posible de la carga para minimizar el ruido de modo común entre tierra y neutro y reducir al mínimo las diferencias entre la tierra de la fuente de voltaje y de señal. Se logra la ubicación más cercana posible cuando el transformador está situado dentro del recinto de la PDU. El transformador de aislamiento normalmente se configura como un transformador reductor 480:208 V/120 V para reducir el tamaño de alimentación del UPS a la PDU. Para soportar los efectos de calentamiento de las corrientes armónicas, se deben utilizar transformadores de-K. Para reducir las corrientes y tensiones armónicas, un transformador de cancelación de armónicos en zigzag o un transformador con un filtro de armónicos activo se puede utilizar. Reducción al mínimo de armónicos en el transformador de mejorar la eficiencia del transformador y reduce la carga de calor producida por el transformador;
- Supresión de tensión transitoria de picos (TVSS): Del mismo modo, la eficacia de supresión de sobretensión transitoria dispositivos (TVSS) se aumenta en gran medida cuando las longitudes de conductor se mantienen lo más corto posible, preferiblemente menos de 200 mm (8 pulgadas). Esto se facilita proporcionando a la supresión de sobretensión transitoria (TVSS), en el mismo recinto que los tableros de distribución;

- Tableros de distribución: Cuadros de mando se pueden montar en el mismo armario que el transformador o en los casos en que se necesitan más placas de panel, un panel de energía a distancia pueden ser utilizados;
- Medición, monitoreo, alarmas y las disposiciones para las comunicaciones remotas: tales características típicamente implica sustancialmente los requisitos de espacio cuando se le proporciona un sistema de placa de panel tradicional;
- (EPO) controles de apagado de emergencia;
- De un solo punto del bus de tierra;
- Conducto placa de aterrizaje: En la mayoría de los centros de datos, cada bastidor de equipo es alimentado a partir de al menos un circuito dedicado, y cada circuito está provisto de un, conducto dedicado separado. La mayoría de los cerramientos en paneles no tienen el espacio físico a la tierra hasta 42 conductos separados.

- Sistemas de puesta a tierra del edificio y de protección contra rayos

Un edificio de perímetro del bucle de tierra debe ser proporcionada, que consiste en el n º 4/0 AWG (mínimo) de alambre de cobre desnudo enterrado 1 m (3 pies) de profundidad y 1 m (3 pies) de la pared del edificio, con 3 mx 19 mm (10 pies x ¾ pulg) varillas de tierra de acero revestido de cobre espaciados cada 6 a 12 m (20 a 40 pies) a lo largo del bucle de tierra. Pozos de prueba deben ser proporcionados en las cuatro esquinas del bucle. Acero de construcción debe

estar unido al sistema en cualquier otra columna. Este sistema de construcción de tierra debe estar unido directamente a todos los principales equipos de distribución de energía, incluyendo todos los interruptores, generadores, sistemas de UPS, transformadores, etc., así como a los sistemas de telecomunicaciones y sistema de protección contra rayos. Se recomiendan los buses de tierra para facilitar la unión y la inspección visual.

Ninguna parte de los sistemas de puesta a tierra debe ser superior a 5 ohmios a tierra verdadera, medido por el método de cuatro puntos de caída de potencial.

- Tierra de la infraestructura del centro de datos.

Norma IEEE 1100 ofrece recomendaciones para el diseño eléctrico de la unión y conexión a tierra.

Debería considerarse la posibilidad de instalar una red de conexión común, como una estructura de referencia de la señal como se describe en el estándar IEEE 1100 para la unión de las telecomunicaciones y los equipos informáticos.

La infraestructura de conexión a tierra sala de informática crea una referencia de tierra equipotencial para la sala de ordenadores y reduce las señales de alta frecuencia perdidas. La infraestructura del centro de datos a tierra consiste en una cuadrícula de conductores de cobre de 0,6 a 3 m (2-10 pies) de centros que cubre todo el espacio de la sala de ordenadores. El conductor no debe ser menor que el # 6 AWG o equivalente. Tal rejilla puede utilizar conductores de cobre o bien desnudos o aislados. La solución preferida es el uso de cobre aislado, que se quitó cuando se deben hacer las conexiones. El aislamiento impide que los puntos

de contacto intermitente o no deseados. El color estándar de la industria del aislamiento es verde o marcados con un color verde característico que en ANSI-J-STD-607-A. Otras soluciones aceptables incluyen una rejilla prefabricada de tiras de cobre soldadas en un patrón de rejilla de 200 mm (8 pulgadas) centros que se rueda a la pista en secciones, o tela metálica, que se instala de manera similar, o un sistema de acceso a la planta eléctrica continua que ha sido diseñado para funcionar como una infraestructura de centro de datos de conexión a tierra y que está unido al sistema de edificio de puesta a tierra.

La infraestructura del centro de datos de conexión a tierra debe tener las siguientes conexiones:

- 1 AWG o mayor conductor de conexión a tierra de barras Telecomunicaciones (TGB) en la sala de ordenadores. Consulte ANSI/TIA/EIA-J-STD-607-A Edificios Comerciales Conexión a tierra y requisitos de fianza de Telecomunicaciones para el diseño de la puesta a tierra de Telecomunicaciones e Infraestructura Bonding;
- Un conductor de conexión al bus de tierra para cada PDU o la placa de panel al servicio de la habitación, tamaño de acuerdo a NEC 250.122 y según las recomendaciones de los fabricantes;
- 6 AWG o mayor conductor de conexión a equipos de climatización;
- 4 AWG o mayor conductor de conexión a cada columna en el aula de informática;
- 6 AWG o mayor conductor de conexión a cada escalera de cable, bandeja de cable, y el cable de canaleta sala de entrada;

- 6 AWG o mayor conductor de conexión a cada conducto, tubería de agua, y el conducto habitación que entra;
- 6 AWG o mayor conductor de conexión a cada pedestal para suelo sexto en cada dirección;
- 6 AWG o mayor conductor de conexión a cada ordenador o armario de telecomunicaciones, bastidor o marco. No unir bastidores, gabinetes y marcos de serie.

5.1.3.4 Aspectos Gestión y Administración de Datos

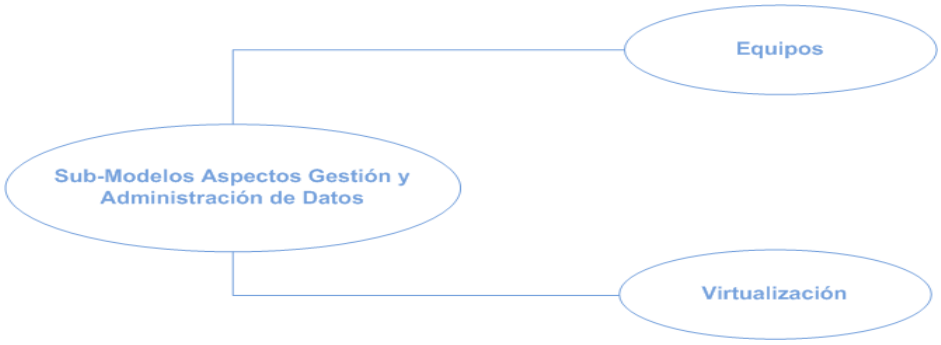


Figura 21. Aspectos Gestión y Administración de Datos.

Fuente: Propia.

En este aspecto se va especificar funcionalidades de los equipos y los aspectos a utilizar de la virtualización en la infraestructura de datos de la institución. Cabe destacar que el mismo abarca el entorno funcional de la organización basándose en su entorno laboral actual.

- **Redundancia del Hardware**

La disponibilidad y la integridad de los datos albergados en la institución deben contar con una redundancia del hardware para asegurar una continuidad del servicio aceptable en caso de siniestro:

- Cableado eléctrico y de red.
- Inversores / Planta
- Climatización
- Líneas de telecomunicaciones
- Servidores (Bahías de almacenamiento, switch, routers, etc.).
- Fuentes de alimentación
- Sensores ambientales
- Cámaras de vigilancia
- Controles de Acceso
- Dispositivos contra incendios.

Toda la infraestructura en general servidores, equipos de red y comunicaciones, deben poseer funciones o equipamiento redundantes, en los casos que sea posible:

- ✓ Tarjetas de Red
- ✓ Fibra
- ✓ Fuentes
- ✓ UPS
- ✓ Disco Duros
- ✓ Base de Datos
- ✓ Entre Otros

- Virtualización Corporativa

En la actualidad existen grandes fabricantes de esta tecnología, la misma han ayudado enormemente al entorno de la infraestructura aportando estabilidad y recuperación de recursos. La virtualización ayuda a consolidar los servidores, equipos, etc.

La virtualización aportara a la institución aportándole lo siguiente:

1. Seguridad: Cada equipo tiene privilegios diferentes, de administración, de tal manera que la institución será menos vulnerable ante cualquier ataque, ya que solo afectara ese equipo.
2. Protección y detección de problemas de hardware: Se podrá detectar cualquier problema que surja de en el equipo virtual.
3. Backup (Recuperación de desastres): La institución contara siempre con una buena productividad ya que gracias a esta herramienta podrá realizar una recuperación rápida casi automática en caso de desastres.
4. Portabilidad: Se podrá clonar o transportar los ficheros de los equipos virtuales.
5. Ahorro energético: Se consolidaran todos los servidores los cuales dejaran de realizar un consumo eléctrico.
6. Ahorro de espacio: La Institución podrá disponer de gran espacio ya que todo el entorno va a estar virtualizado.

Cabe destacar que en la actualidad 3 grandes empresas, entre ellas VMware que es líder indiscutible además de que tiene la mayor parte del mercado de sistema

de virtualizados en producción. La misma desde 1999 está desarrollando aplicaciones y tiene un gran portafolio de productos, contando así con funcionalidades con las cuales sus competencias no cuentan.

Por otra parte tenemos a Citrix la cual adquirió en el 2007 la empresa XenSource, que había recopilado el movimiento Open Source que empujaba la tecnología Xen como una alternativa válida y robusta frente al sistema propietario VMware.

Por último entra al mercado Microsoft la cual nos trae productos como Virtual PC y Virtual Server, quedando en una tercera posición pero con gran fuerza la misma se realza lanzando Hyper-v la cual da grandes esperanza a la empresa por su completa herramienta.

5.1.3.5 Aspectos de Telecomunicaciones

Figura 22. Aspectos Telecomunicaciones.

Fuente: Propia.

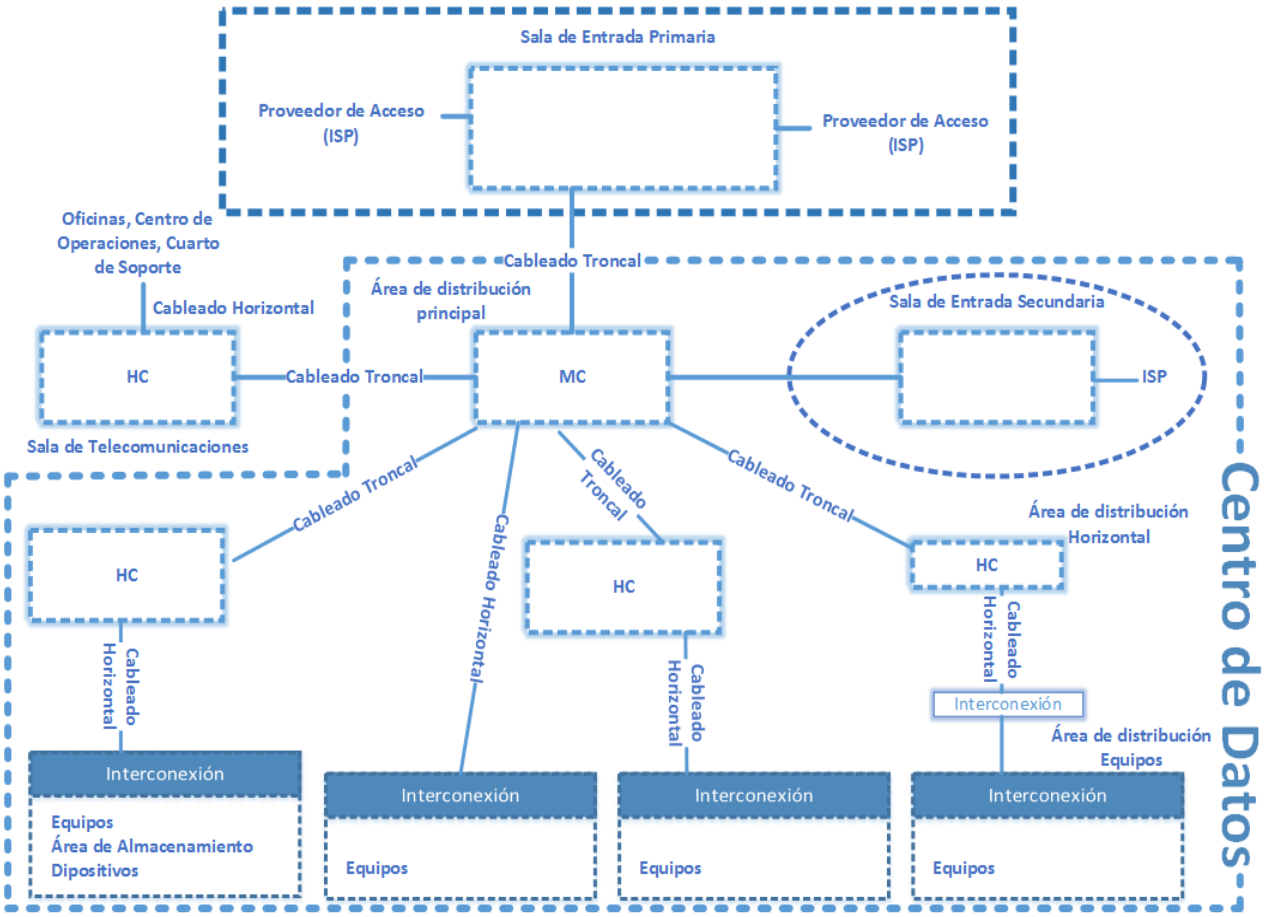


Figura 23. Topología Centro de Datos

Elaboración: Propia

Fuente: TIA-942

El centro de datos requiere de espacios dedicados a apoyar la infraestructura de telecomunicaciones. Estos ayudan al cableado y los equipos del mismo.

Espacios típicos que se encuentran en un centro de datos por lo general incluyen:

- La sala de entrada
- Área de distribución principal (MDA),
- El área de distribución horizontal (HDA),

- El área de distribución de la zona (ZDA)
- El área de distribución de equipos (EDA).

Dependiendo del tamaño del centro de datos, no todos estos espacios se pueden usar dentro de la estructura. Estos espacios deben ser planeados para proveer un crecimiento y la transición a las tecnologías en evolución. Estos espacios pueden o no pueden ser encerrados o mejor dicho separados de los otros espacios de la sala de ordenadores.

- Cableado Horizontal

El cableado Horizontal Ayuda a unir los equipos de una misma plantas, o diferentes ubicaciones con los enrutadores de planta. Desde la roseta de cada una de las áreas de trabajo se tiende un cable hasta un lugar común de centralización llamado panel de parcheo. Este último ayuda a centralizar todo el cableado de la plantas de un edificio y es donde llegan los cables procedentes de una de las dependencias donde se ha instalado un punto de red.

Cada roseta instalada en el edificio tienen en el otro extremo de su cable una conexión al panel de parcheo. De esta manera se le podrá dar o quitar servicio a una determinada dependencia simplemente con proporcionarle o no señal en este panel.

Todo el cableado Horizontal debe ser tendido por conducciones adecuadas. En la mayoría de los casos se elige para esta funcionas las llamadas canaletas, las cuales permiten de una forma flexible trazar recorridos desde el área de trabajo hasta el panel de parcheo. Es conveniente que el panel de parcheo, junto con los

dispositivos de interconexión centralizada (Enrutadores, latiguillos, fuentes de alimentación, etc.), estén encerrados en un armario de comunicaciones. De esta forma se aíslan del exterior y por tanto de su manipulación accidental por personal no cualificado. Además, facilita el mantenimiento, al tener todo en un mismo lugar.

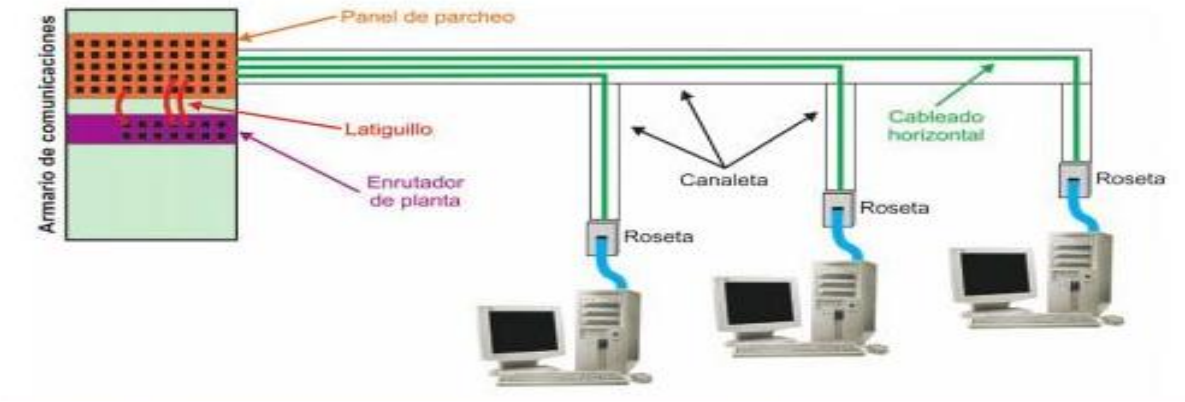


Figura 24. Cableado Horizontal

Fuente: Servicios En RED - Joaquín Andreu Gómez

La siguiente lista parcial de los servicios y sistemas comunes debe considerarse cuando el cableado horizontal está diseñado:

- Voz, módem y servicio de telecomunicaciones de fax;
- Instalaciones equipos de conmutación;
- Equipo y conexiones de administración de telecomunicaciones;
- Teclado / vídeo / ratón (KVM) conexiones;
- Las comunicaciones de datos;
- Redes de área amplia (WAN);
- Redes de área local (LAN);

- Redes de área de almacenamiento (SAN);
- Sistemas de señalización de otros materiales de construcción (sistemas de automatización de edificios, tales como incendios, seguridad, energía, sistemas de climatización, el EMS, etc.)

Además de satisfacer las necesidades actuales de telecomunicaciones, el cableado horizontal debe ser planificado para reducir el mantenimiento y la reubicación en curso. También se debe dar cabida a equipos y servicios en cambios futuros. Se debería considerar la posibilidad de acoger a una diversidad de aplicaciones del usuario con el fin de reducir o eliminar la probabilidad de requerir cambios en el cableado horizontal a medida que evolucionan las necesidades del equipo. El cableado horizontal se puede acceder para la reconfiguración bajo el piso de acceso o sobrecarga en sistemas de bandejas de cables. Sin embargo, en una instalación debidamente planificada, perturbación del cableado horizontal sólo debe ocurrir durante la adición de un nuevo cableado.

- Topología

El cableado horizontal debe ser instalado en una topología en estrella, como se muestra en la figura que está más abajo. Cada terminación mecánica en el área de distribución de equipo deberá estar conectada a una conexión cruzada horizontal en el área de distribución horizontal o conexión cruzada principal en el área de distribución principal a través de un cable horizontal.

El cableado horizontal deberá contener no más de un punto de consolidación en el área de distribución entre la zona de conexión cruzada horizontal en el área de

distribución horizontal y la terminación mecánica en el área de distribución de equipos.

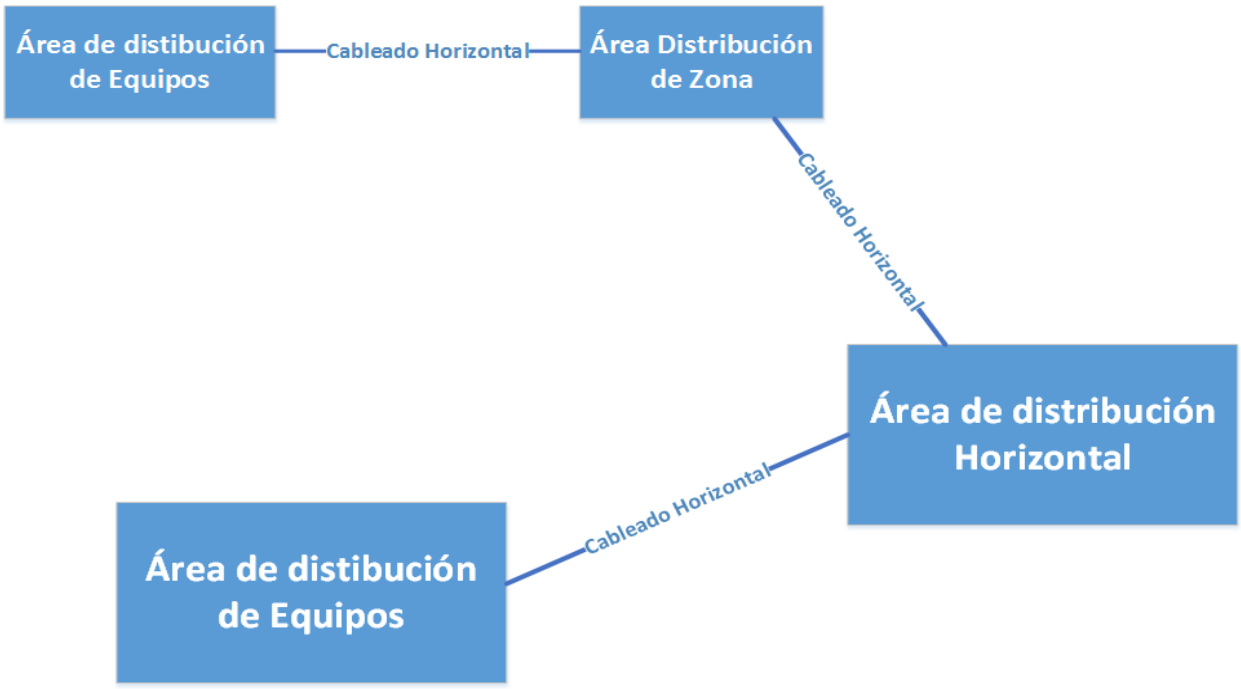


Figura 25. Típico Cableado Horizontal usando topología estrella.

Elaboración: Propia

Fuente: TIA-942

- Distancias de cableado horizontal

La distancia de cableado horizontal es la longitud del cable desde la terminación mecánica de los medios de comunicación en la conexión cruzada horizontal en el área de distribución horizontal o el área de distribución principal a la terminación mecánica de los medios de comunicación en el área de distribución de equipos.

La distancia horizontal máxima será de 90 m (295 pies), independientemente del tipo de soporte. La distancia máxima de canales incluyendo los cables del equipo

será de 100 m (328 pies). La distancia máxima de cableado en un centro de datos que no contiene un área de distribución horizontal será de 300 m (984 pies) para un canal de fibra óptica incluyendo cables del equipo, 90 m (294 pies) para el cableado de cobre con exclusión de los cables del equipo y los 100 m (328 pies) en los cables de cobre que incluye los cables del equipo.

Además, es posible que se reduzca a compensar más largos cables del equipo en las áreas de distribución de los centros de datos de distancias de cableado horizontal en una sala de ordenadores. Por lo tanto, se deben hacer consideraciones cuidadosas a la distancia del cable horizontal para garantizar las distancias de cableado y requisitos de transmisión que no se superan cuando se unen los cables del equipo.

- Las longitudes máximas de cableado de cobre

Equipo de cable de cobre utilizados en el contexto de los medios de la zona en el área de distribución de la zona, deberán cumplir los requisitos de ANSI/TIA/EIA-568-B.2. Con base en las consideraciones de la pérdida de inserción, la longitud máxima se determinará en función de:

- ✓ C = (102 - H) / (1 + D) (1)
- ✓ Z = C - T ≤ 22 m (72 pies) en el 24 AWG UTP / ScTP o ≤ 17 m (56 pies) de 26 AWG ScTP (2)

Dónde:

- ✓ C es la longitud combinada máxima (m) del cable de área de la zona, equipo de cable y cable de conexión.
- ✓ H es la longitud (m) del cable horizontal (100 m H + C ≤).
- ✓ D es un factor de reducción de potencia para el tipo de cable de conexión (0.2 para 24 AWG UTP/24 AWG ScTP y 0,5 para 26 AWG ScTP).
- ✓ Z es la longitud máxima (m) del cable de área de la zona.
- ✓ T es la longitud total de los cables de conexión y de equipos.

En la tabla que está más abajo se aplica la fórmula anterior suponiendo que hay un total de 5 m (16 pies) de 24 AWG UTP/24AWG ScTP o 4 m (13 pies) de 26 AWG ScTP cables de conexión y los cables de los equipos en el área de distribución principal, u horizontal área de distribución. La salida de la zona deberá estar marcada con la longitud máxima permitida del cable área de la zona. Un método de lograr esto es para evaluar marcas de longitud de cable.

	24 AWG UTP/24 AWG ScTP patch Cords		26 AWG ScTP patch Cords	
Longitud del Cableado Horizontal	Maxima Longitud zona de área cableada	Maxima Convinación de longitud, pacht cords, cableado de equipos	Maxima Longitud zona de área cableada	Maxima Convinación de longitud, pacht cords, cableado de equipos
H	Z	C	Z	C
m (ft)	m (ft)	m (ft)	m (ft)	m (ft)
90 (295)	5 (16)	10 (33)	4 (13)	8 (26)
85 (279)	9 (30)	14 (46)	7 (23)	11 (35)
80 (262)	13 (44)	18 (59)	11 (35)	15 (49)
75 (246)	17 (57)	22 (72)	14 (46)	18 (59)
70 (230)	22 (72)	27 (89)	17 (56)	21 (70)

Figura 26. Longitud máxima de cables de área horizontal y equipos.

Fuente: TIA-942

- Cableado Troncal

La función del cableado troncal es proporcionar conexiones entre el área de distribución principal, el área de distribución horizontal, y en las instalaciones de entrada en el sistema de cableado del centro de datos. El cableado troncal está formado por los cables principales, principales conexiones cruzadas, conexiones horizontales, terminaciones mecánicas, y cable de conexión o jumpers usados para la red troncal a troncal de conexión cruzada.

El cableado troncal permitirá la reconfiguración de la red y el crecimiento futuro sin perturbación del mismo. Debe apoyar diferentes necesidades de conectividad, incluyendo la red y la conectividad de la consola física, como redes de área local, redes de área amplia, redes de área de almacenamiento, canales informáticos, y las conexiones de la consola del equipo.

- Topología Estrella

El cableado troncal deberá utilizar la topología de estrella jerárquica como lo ilustra la figura más abajo, en la que cada conexión cruzada horizontal en el área de distribución horizontal está cableada directamente a una conexión cruzada principal en el área de distribución principal. No habrá más de un nivel jerárquico de conexión cruzada en el cableado troncal. A partir de la conexión cruzada horizontal, no más de una conexión cruzada se hace pasar a través para llegar a otra conexión cruzada horizontal.

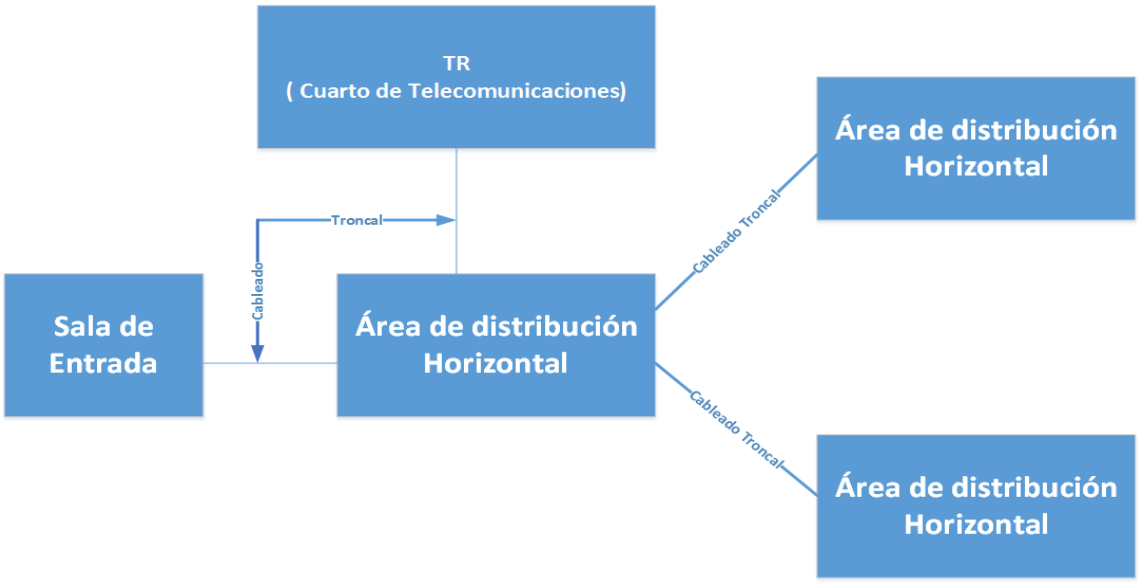


Figura 27. Típico cableado troncal utilizando una topología en estrella.

Fuente: Propia

La presencia de la conexión cruzada horizontal no es obligatoria. Cuando no se utilizan la misma, el cableado que se extiende desde la conexión cruzada principal para la terminación mecánica en el área de distribución de equipo se considera cableado horizontal. Si el cableado horizontal pasa a través de la HDA (área de distribución horizontal), dejando la suficiente longitud de cable debe existir en el área de distribución horizontal para permitir el movimiento de los cables cuando se migra a una conexión cruzada.

Cableado troncal conexiones cruzadas pueden estar ubicados en salas de telecomunicaciones, salas de equipos, principales áreas de distribución, áreas de distribución horizontal o en las salas de ingreso.

En el caso de múltiples salas de entrada, cableado troncal directo a la conexión cruzada horizontal se permitirá cuando se encuentran las limitaciones de distancia.

5.1.3.6 Aspectos de Mecánicos

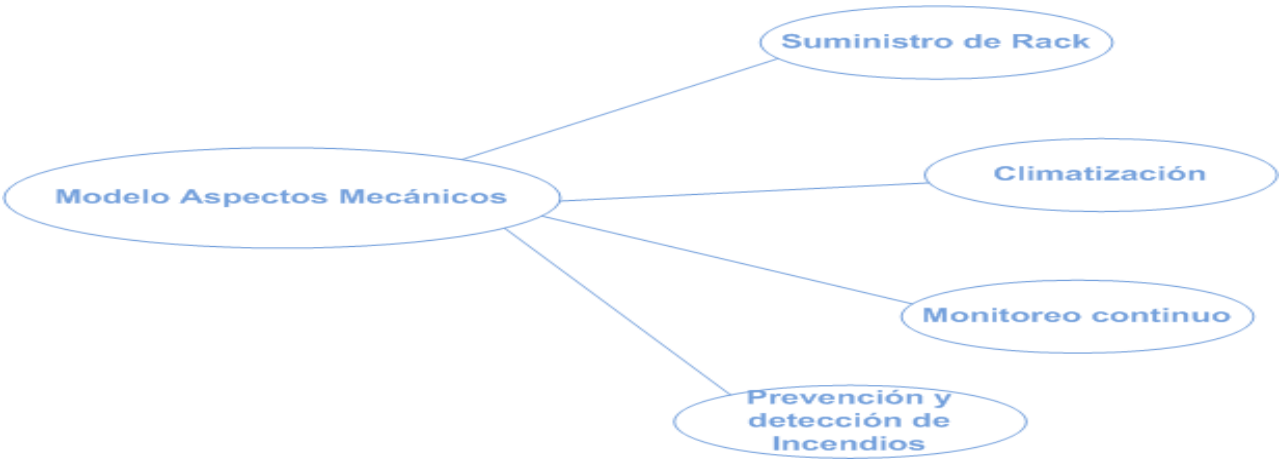


Figura 28. Aspectos Mecánicos

Fuente: Propia.

El sistema mecánico debe ser capaz de alcanzar los siguientes parámetros ambientales sala de ordenadores:

- ✓ Temperatura:
  - 20 ° C a 25 ° C (68 ° F a 77 ° F)
- ✓ Puntos de ajuste normales:
  - 22 ° C (72 ° F) Control de ± 1 ° C (2 ° F)
- ✓ Humedad relativa:
  - 40% a 55%
- ✓ Puntos de ajuste normales:
  - 45% de humedad relativa

- Control de ± 5%

Coordinar los planes de diseño de refrigeración del sistema y del piso equipos de manera que el flujo de aire de los equipos de refrigeración se desplaza en una dirección paralela a las filas de armarios / bastidores.

Salas de impresión deben ser aisladas habitaciones con sistema de aire acondicionado independiente para no introducir contaminantes, como el papel y el polvo de tóner en el resto del centro de datos.

- Ventilación del aire

La sala de ordenadores debe recibir ventilación exterior para los ocupantes. El aire de ventilación debe ser introducido en el nivel del techo, cerca de las unidades de habitación equipo de aire acondicionado cuando las unidades se encuentran en el interior de la sala de ordenadores.

La sala de ordenadores debe recibir aire de suministro para fines de presurización positiva ventilación y.

No se requiere de retorno y aire de escape de la sala de ordenadores.

- Aula de informática de aire acondicionado

El sistema de aire acondicionado debe ser diseñado para proporcionar las condiciones de temperatura y humedad de diseño recomendadas por los fabricantes de los servidores que se instalen dentro del centro de datos.

Sistemas de agua enfriada a menudo son más adecuados para los centros de datos más grandes. Unidades DX pueden ser más convenientes para los centros

de datos más pequeños y no requieren tuberías de agua que se instalará en las áreas de equipos informáticos y de telecomunicaciones.

Los equipos con altas cargas de calor pueden requerir conductos de aire o suelos técnicos para proporcionar una refrigeración adecuada.

- Detección de Fugas en el sistema

Un sistema de detección de fugas que consta de dos sensores de cable de tipo distribuido y sensores de punto se debe considerar siempre que existe la amenaza de agua. Sensores de cable ofrecen una mayor cobertura y aumentar las posibilidades de que una fuga se detectó con precisión. Sensores de punto son menos costosos, requieren un reemplazo menos frecuente, y son muy adecuadas cuando los puntos bajos en el suelo se pueden determinar. Un plan enmarcado indicando recorrido de los cables y de forma periódica que indica la longitud del cable calibrado para el sistema deberá haber junto al panel de alarma del sistema.

- Sistema de gestión del edificio

Un sistema de gestión de edificios (BMS) debe supervisar todos los equipos y sistemas de instalaciones mecánicas, eléctricas y otras. El sistema debe ser capaz de monitorizar y operación local y remota. Los sistemas individuales deberán permanecer en funcionamiento en caso de fallo del sistema central de gestión de edificios (BMS) o cabecera. Se debe considerar a los sistemas capaces de controlar (no sólo en el control) de sistemas de construcción, así como las tendencias históricas. 24 horas de vigilancia del sistema de gestión de edificios (BMS) debe ser proporcionada por el personal de las instalaciones, el personal de

seguridad, sistemas de localización, o una combinación de estos. Los planes de emergencia deben ser desarrollados para permitir una respuesta rápida a las condiciones de alarma.

- Los sistemas de cañerías

No hay agua o de drenaje de tuberías se enruta a través del centro de datos que no está asociado con el equipo del centro de datos. El agua o la tubería de drenaje que debe ser enviada dentro del centro de datos deben ser encerrados o bien cuentan con una chaqueta de protección contra fugas. Un sistema de detección de fugas debe ser proporcionada a notificar a los operadores del edificio en caso de una fuga de agua. Tier 3 y 4 centros de datos sólo deben tener agua o drenar la tubería que soporta equipos de centros de datos encaminada a través del espacio de la sala de ordenadores.

- Iluminarias de emergencia

Un ojo de lavado / ducha de emergencia debe estar ubicado en salas de baterías que tienen pilas húmedas.

- Climatización del rellenado de agua

Doméstica "frío" agua de reposición debe ser proporcionada para todos los equipos de aire acondicionado para salas de ordenadores que contienen un humidificador.

El material de conducción debe ser de cobre tipo "L" con uniones soldadas. Tubería de combustible no se debe utilizar.

- Drenaje de tubería

Proveer drenaje (s) planta dentro de la sala de ordenadores para recoger y drenar el agua de los rociadores de pre-acción después de una descarga. El drenaje (s) planta debe recibir el agua de drenaje de condensado y el humidificador de agua de lavado de las salas de ordenadores unidades de aire acondicionado.

El material de conducción debe ser de cobre tipo "L" con uniones soldadas. Tubería de combustible no se debe utilizar.

- Sistemas de protección contra incendios

Los factores de riesgo a tener en cuenta al seleccionar un esquema de protección para el centro de datos se pueden clasificar en cuatro áreas principales. La primera es la cuestión de la seguridad de personas o bienes afectados por la operación (por ejemplo, sistemas de soporte de vida, las telecomunicaciones, los controles del sistema de transporte, controles de proceso). La siguiente es la amenaza de fuego a los ocupantes en un lugar cerrado o la amenaza a la propiedad expuesta (por ejemplo, registros, almacenamiento en disco). La siguiente es la pérdida económica de la interrupción del negocio debido a la inactividad y, por último, es la pérdida del valor del equipo. Estas cuatro áreas se deben evaluar cuidadosamente para determinar el nivel adecuado de protección de la instalación en consideración.

A continuación se describen los diferentes niveles de protección que pueden ser proporcionados por el centro de datos. El nivel mínimo de protección que exige el código incluye un sistema de rociadores ordinaria junto con los extintores de

agente limpio apropiados. Esta norma específica que los sistemas de rociadores sean aspersores de acción previa.

Sistemas de detección y extinción de avanzada más allá de los requisitos mínimos del código incluyen sistemas de toma de muestras de aire de humo de detección, sistemas de riego de pre-acción y sistemas de supresión de agente limpio.

Detección y Alarma de Incendio, Muestreo de Aire de detección de humo, daños al equipo significativo puede ocurrir debido únicamente a humo u otros productos de la combustión que atacan a los equipos electrónicos. Por lo tanto, los sistemas de detección de alerta temprana son esenciales para evitar los daños y perjuicios que puedan producirse en las fases incipientes de un incendio. Un sistema de detección de humo ofrece otro nivel de protección para la sala de ordenadores e instalaciones asociadas de entrada, salas de máquinas y salas eléctricas. Este sistema se proporciona en lugar de los detectores de humo ordinarios, como su sensibilidad y capacidad de detección son mucho más allá de la de los detectores convencionales. El mecanismo de detección menos sensible utilizado por los detectores convencionales requiere una cantidad mucho más grande de humo antes de que incluso detectar un incendio. En un centro de datos, la diferencia y el tiempo de retardo es especialmente pronunciada debido al alto flujo de aire a través de la habitación, lo cual tiende a diluir el humo y detectores de retardo más comunes. Hay, sin embargo, algunos diversos sistemas de alerta temprana que los sistemas de detección de muestras de aire que utilizan la ionización convencional o detectores fotoeléctricos. También hay detectores de humo a base de láser que no utilizan el muestreo de aire y que no ofrecen un nivel equivalente

de detección de alerta temprana a los sistemas estándar de detección de muestras de aire. Lo mismo es cierto para los detectores de haz, así como la ionización convencional y detectores de humo fotoeléctricos. Estos sistemas de detección de humo alternativos pueden ser apropiados en los centros de datos, donde el potencial de pérdida y las consecuencias adversas de tiempo de inactividad del sistema no se consideran críticos. Si se opta por la detección de humos convencional, se debe utilizar una combinación de ionización y fotoeléctricos.

El sistema de detección de humo recomendado para centros de datos críticos donde la alta circulación de aire está presente es el que va a proporcionar una alerta temprana a través de muestreo de aire continuo y recuento de partículas y tiene un alcance de hasta a la de los detectores de humo convencionales. Estas características le permitirán funcionar también como el sistema de detección primaria y por lo tanto eliminar la necesidad de un sistema de detección convencional redundante para activar los sistemas de supresión.

El tipo de sistema de muestreo de aire más utilizado consiste en una red de tuberías en el techo y por debajo de la planta de acceso que atrae continuamente el aire de la habitación en un detector de láser basado. Cualquier liberación de humo u otras partículas (incluso de una pieza de equipo sobrecalentado) en el aire de la habitación se puede detectar en sus primeras etapas, debido a la alta sensibilidad del láser. La capacidad de respuesta temprana ofrece a los ocupantes la oportunidad de evaluar una situación y responder antes del evento cause daño o evacuación significativa. Además, el sistema tiene cuatro niveles de alarma que

van desde la detección de humo en el rango visible hasta que la detectada por los detectores convencionales. El sistema en su nivel más alto de alarma sería el medio para activar la válvula del sistema de pre-acción. Los diseños pueden requerir dos o más sistemas. Un sistema estaría en el nivel del techo de la sala de ordenadores, instalaciones de entrada, salas eléctricas y salas de máquinas, así como en la entrada a las unidades de tratamiento de aire para salas de ordenadores. Un segundo sistema cubriría el área debajo del piso de acceso en la sala de ordenadores, instalaciones de entrada, salas eléctricas y salas de máquinas. También se recomienda un tercer sistema para el centro de operaciones y sala de impresora para proporcionar un nivel consistente de detección para estas áreas. Los sistemas separados permiten umbrales separados y lecturas de referencia separados de la normalidad, para optimizar la detección temprana y reducir al mínimo las falsas alarmas. Estas unidades pueden, si se desea conectar a la red para el monitoreo remoto.

- Supresión de agua - la supresión de pre-acción

Un sistema de riego de pre-acción proporciona un nivel superior de protección para el centro de datos, ya que permite un mayor nivel de fiabilidad y mitigación de riesgos. El sistema de pre-acción es normalmente llenada de aire y sólo permitirá el agua en la tubería por encima del centro de datos cuando el sistema de detección de humo indica que hay un evento en curso. Una vez que el agua se libera en la tubería, que todavía requiere un aspersor para activar antes de que se libera el agua en la habitación. Este sistema responde a la preocupación común sobre las fugas de daños accidentales o mal funcionamiento. Aspersores Pre-

acción deben proteger el centro de operaciones, sala de impresora y salas eléctricas y salas de máquinas, ya que también se consideran esenciales para la continuidad de las operaciones. En situaciones de retro-ajuste, cualquier red de rociadores de tubería húmeda existentes y tuberías secundarias deberán ser reubicados fuera de los límites del centro de datos para eliminar toda el agua llena la tubería por encima del espacio.

Protección de riego debajo de los pisos de acceso es a veces un problema que se consulta en los centros de datos. Sin embargo, en general, esa protección debe evitarse siempre que sea posible, ya que su eficacia se limita a ciertas aplicaciones donde el suelo es más de 410 mm (16 pulgadas) de altura y la carga de combustible bajo el suelo es significativa. Esta protección general puede omitirse cuando las siguientes condiciones favorables están presentes.

El espacio de cable se utiliza como una cámara de aire, los cables son el grupo de FM 2 o 3, los cables de señal superan en número a los cables de alimentación por 10 a 1, el cable no ha sido sujeto a un deterioro significativo debido a la degradación térmica o daño mecánico, el acceso piso no es combustible, el espacio del subsuelo es accesible, y no hay cables eléctricos no estén relacionados con las líneas de centro de datos o de vapor o cualquier otras fuentes importantes de calor en el espacio del subsuelo. Cuando se considere apropiada una necesidad de un sistema de extinción en un espacio del subsuelo, que también se tengan en cuenta limpiar los sistemas de agentes como un medio alternativo para lograr esta protección.

- Supresión Gaseoso - supresión de incendios de agente limpio

Un sistema de supresión de incendios de agente limpio proporciona el más alto nivel de protección para la sala de computación y las salas eléctricas y mecánicas asociadas. Este sistema sería instalado además de la supresión de pre-acción y sistemas de detección de humo. El sistema de supresión de incendios está diseñado, al ser activado, para que el gas de agente limpio inundar completamente la habitación y el área del piso bajo. Este sistema consiste en un gas no tóxico que es superior a los rociadores de protección de varias maneras. En primer lugar, el agente puede penetrar en los equipos informáticos para extinguir fuegos profundamente arraigados en equipos electrónicos y otros relacionados. En segundo lugar, a diferencia de los rociadores no hay residual del gas a ser eliminado después de que se activa el sistema. Por último, este agente permite que el fuego se extinga sin atentar contra los otros equipos que no participan en el fuego. Por lo tanto, mediante el uso de la supresión gaseosa del centro de datos fácilmente podría volver a la operación después de un evento con un mínimo de retraso y la pérdida se limita sólo a los elementos afectados.

Se requiere sellado habitación efectiva para contener el agente limpio, de modo que las concentraciones efectivas se logran y mantienen el tiempo suficiente para extinguir el fuego.

NFPA recomienda que el equipo electrónico y de climatización se apaga automáticamente en caso de cualquier descarga sistema de extinción, aunque el razonamiento detrás de esto es diferente para los sistemas de agentes de limpieza a base de agua y. Los equipos electrónicos a menudo se pueden salvar después

del contacto con el agua, siempre y cuando se haya desactivado antes del contacto, la parada automática se recomienda principalmente para guardar el equipo. Con los sistemas de agente limpio, la preocupación es que una falla de arco podría volver a encender un fuego después de que el agente de limpieza se ha disipado. En cualquiera de los casos, sin embargo, la decisión de establecer el apagado automático es en última instancia el dueño de, que pueden determinar que la continuidad de las operaciones supera cualquiera de estas preocupaciones.

Los propietarios deben evaluar cuidadosamente sus riesgos, para determinar si el centro de datos debe incluir un sistema de extinción de gas de agente limpio.

Los códigos locales pueden dictar el tipo de sistema de supresión de agente limpio que puede ser utilizado. Información adicional sobre los sistemas de extinción de incendios mediante agentes limpios está disponible en NFPA 2001.

- Extintores de mano

Se recomienda utilizar un extintor de incendios de agente limpio para la sala de ordenadores, ya que evita que el polvo químico seco de los extintores de incendios ordinarios ABC, que puede afectar el equipo asociado. Este impacto va más allá de la del fuego y por lo general requiere un importante esfuerzo de limpieza. Consulte la norma NFPA 75 para orientación con respecto a los extintores de mano.

Figura 29. Prevención de Incendio

Fuente: Externa

Las diferentes fases aquí contempladas, se demostraron que la infraestructura tecnológica de la institución, contiene grandes deficiencias en cuanto a la disponibilidad y producción, de tal manera que se ve afectada la continuidad del negocio. Mediante observaciones en la fase de diagnóstico, se establece que lo fundamental para el diseño del centro de datos, es la nueva construcción o adecuación del espacio especificado para tales fines. Este sitio funcionara como espacio neurálgico de la gestión y administración de los datos de la institución.

Esta nueva infraestructura tendrá que seguir las recomendaciones aportadas aquí en el diseño para de esta manera alcanzar una alta disponibilidad y continuidad del negocio.

5.2. Diseño Infraestructura Completo

Figura 30. Grafico Diseño Infraestructura

Fuente: Anixter.com

Se tomó esta imagen como referencia ya que se adapta al diseño y a la infraestructura de la empresa SOTO DOMINICANA. Esta conglomera todo lo especificado en este capítulo en torno al proyecto.

La misma refleja varios puntos que se definen a continuación:

Puntos 1: Indican componentes del cableado, bandejas, tuberías, gabinetes, etc.

Puntos 2: Indican las conexiones eléctricas, PDUs, UPS, Etc.

Puntos 3: Indican la seguridad física del centro de datos sistema de vigilancia, controles de acceso, detecciones del perímetro, etc.

Puntos 4: indican la conexión a tierra siguiendo el estándar TIA-942.

CAPÍTULO 6

Una de las parte clave de un centro de datos y una plataforma de educación a distancia es la seguridad, en este capítulo explicaremos los diferentes tipos de seguridad que requiera esta tecnología y así mismo que tipo de seguridad esta emplea.

En esta parte vamos a profundizar sobre la seguridad, la misma puede ser tanto física como lógica y aportara a la institución protección contra ataques informáticos, uso inadecuado de los recursos por personal no cualificado, virus, acceso a información sin autorización, etc.

Pero antes debemos conocer que es la seguridad informática, para poder tener una clara percepción de la misma, Según ACISSI la seguridad en los sistemas de información, representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y recursos (Físicos, Lógicos y Humanos) que permiten almacenar y que circule la información que contiene.

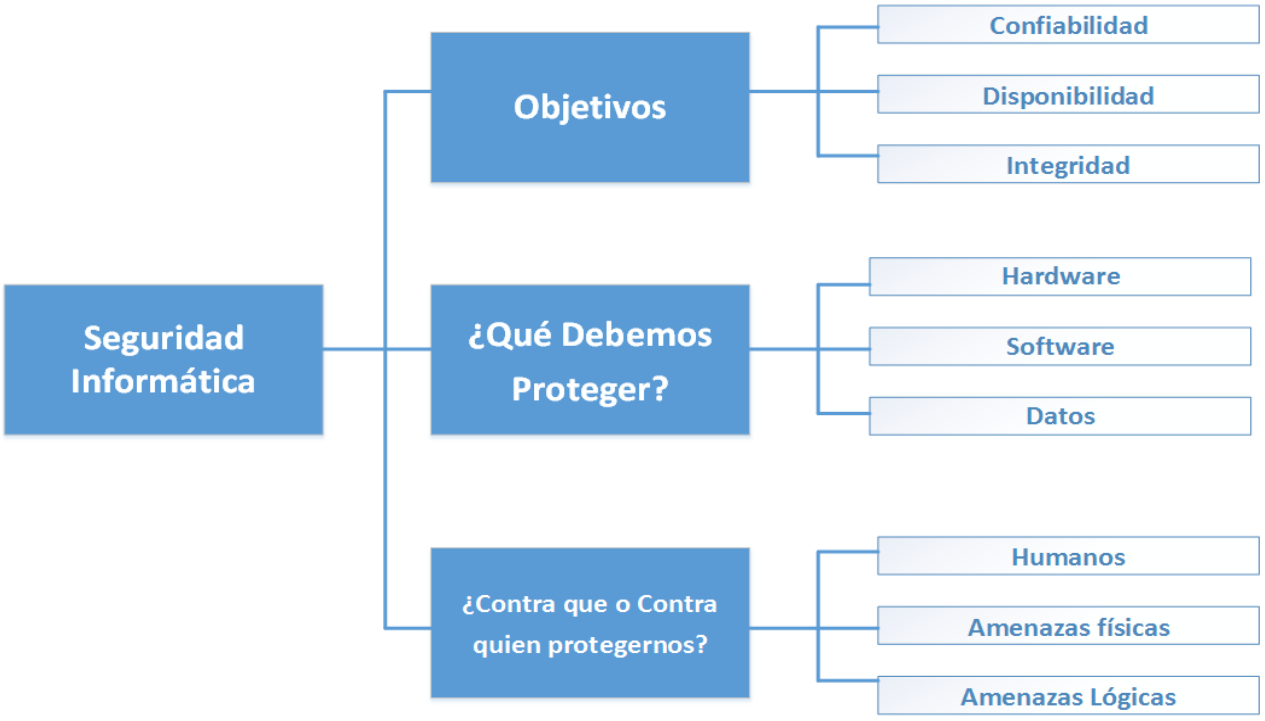


Figura 31. Seguridad Informática.

Figura: Propia

6.1 Importancia de la Seguridad

No importa el nivel, empresarial, multinacional, país o de un usuario común privado, la seguridad de un sistema de información adquiere una importancia proporcional al valor de los datos que contiene. En el despliegue de una red, no solo hay que enfrentarse con el problema del aumento de la cantidad, sino también, y sobre todo, con la importancia de los datos que la recorren.

La seguridad informática toma importancia y medidas completamente distintas según el contexto en que se aplique la misma.

El usuario particular debe, siempre en lo posible, preservar las informaciones o datos que se consideren de carácter confidencial, privado o personal. Ya sea cuando intercambie información con familiares o amigos, cuando acceda a sus datos bancarios en línea o cuando realice sus compras por internet.

A diario vemos como usuarios son víctimas con problemas de seguridad y eso que solo podemos ver públicamente las vulneraciones que al parecer son menos graves. Con el crecimiento de las redes sociales, juegos, etc., herramientas que se utilizan a diario son las mejores fuentes de información (Facebook, Google, etc.) Son lugares que recogen toda la información que se les proporcione, y tardan mucho tiempo en eliminarlas.

6.1.1 Entorno empresarial y centro académicos

Para una institución, los sistemas de información representan gran valor, de tal manera que es lo esencial que debe proteger. Comprometer este sistema seria comprometer la empresa. Por consiguiente, es conveniente asegurar la seguridad del sistema, en tal sentido, garantizar que los recursos sean utilizados únicamente en el marco previsto, por

las personas acreditadas y, sobre todo, que no se utilicen la misma en cualquier otra circunstancia.

La implementación de un sistema de seguridad implica generalmente el despliegue de medidas técnicas, pero, por encima de todo, de soluciones de prevención que deben contar con la información y la sensibilización de los actores del sistema.

La institución deberá crear normas y manuales indicando las buenas prácticas para evitar las formación de brecha humana, un fallo demasiado a menudo ignorado y conocido por los atacantes.

Los vínculos entre la empresa, sus socios, sus proveedores y los empleados forman un conjunto que hay que conocer muy bien para asegurarlo. Los recursos que circulan tienen que estar absolutamente protegidos, y para ello es imprescindible el dominio del sistema de información. Cada actor del sistema toma un papel que hay que respetar y que tiene que estar escrupulosamente definido.

6.2 Tipos de seguridad a implementar en el instituto

Cabe destacar que la empresa SOTO DOMINICANA en la actualidad no cuenta con buen un sistema informático de seguridad, ni físico ni lógico, de tal manera que plasmaremos aquí las recomendaciones y procedimientos a realizar en el centro de datos a implementar.

6.2.1 Tunel VPN

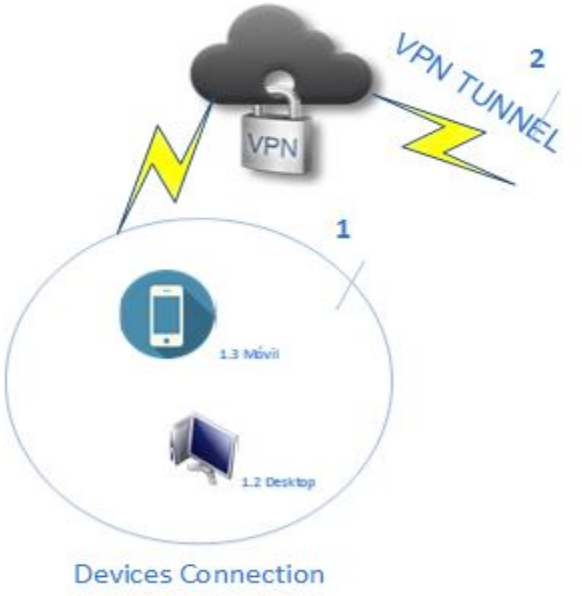


Figura 32. Grafico Anteproyecto – Tunel VPN

Fuente: Propia.

Como vemos esta figura anterior la tecnología VPN permitirá la conexión a una red desde una localización remota, a través de otro tipo de red, como por ejemplo desde el internet.

Como sabemos la empresa va a tener acceso desde internet de la gran mayorías de sus alumnos, para impartir sus cursos en línea, de tal manera que para que esto suceda se necesitara crear una conexión mediante VPN, la cual ayudara a registrar los mismo como perteneciente a la red local y le otorgara dicho acceso.

Según Aguilera López en su libro sobre seguridad informática indica que para que todo el tráfico VPN pueda considerarse seguro, es necesario que se garanticen cuatro principios básicos:

1. **Autentificación y autorización.** Debe conocerse en todo momento que persona realizara las operaciones, para que tenga las mismas garantías que si las realizara personalmente en la empresa.
2. **No rechazo.** Debe poder garantizar que las tareas que se efectúen han sido realizaras, efectivamente, por la persona que se ha autenticado para que, de esa manera, no exista posibilidad de rechazo.
3. **Integridad.** Los datos enviados y recibidos no pueden ser modificados durante el trayecto, ya sea por terceras personas o por fallos en la red.
4. **Confidencialidad.** Los datos enviados y recibidos deben ser encriptados para que en su trayecto a través de internet no sean interceptados, y en caso de serlo, no resulten entendibles.

6.2.1 Formas de conexión de en una red VPN

Gracias a las conexiones VPN se pueden realizar tres formas de conexión distintas:

1. **Tunneling (Tuneles).** Se intenta transmitir el concepto de un túnel a través de internet. Si se piensa en Internet como un medio inseguro por definición, y carecemos de sistema de encripten la comunicación, podemos crear a través de internet un paso seguro o túnel por lo cual enviamos información insegura. La información, en caso de ser interceptada, podría ser interpretada, por esto no es posible ya que para la transferencia se usa protocolo seguro, como por ejemplo conexión SSH.
2. **VPN de acceso remoto.** Se trata de acceder a los recursos disponibles desde ubicaciones remotas, utilizando internet como plataforma de acceso. Realizad la conexión y autenticado el usuario, puede acceder a los mismos recursos que si tuviera presente en la red local de los sistemas a los que accede.

3. **VPN punto a punto.** Similar al funcionamiento del tunneling (túneles), se trata de crear un túnel sobre Internet para la transmisión de datos, pero en lugar de aceptar la conexión de un equipo, el servidor VPN conectado permanentemente a internet acepta la conexión de diversos servidores y sitios, estableciendo el túnel.

6.2.2 Firewall o Cortafuegos

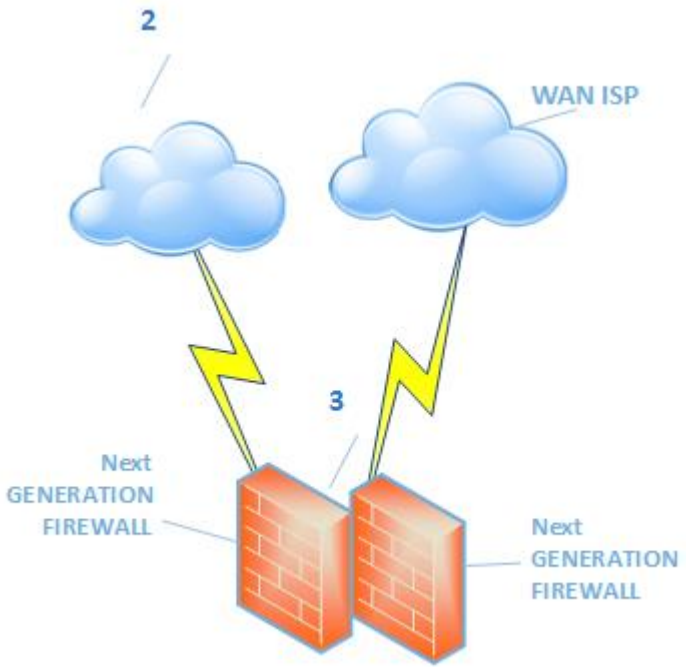


Figura 33. Grafico Anteproyecto – Firewall

Fuente: Propia.

Un firewall / Cortafuegos es un dispositivo, o conjunto de ellos, que están configurado para impedir el acceso no autorizado a una determinada zona de red o dispositivo, pero que al mismo tiempo permite el paso a aquellas comunicaciones autorizadas.

En la empresa SOTO DOMINICANA se implementara esta tecnología para controlar el acceso a los recursos de la misma. Dicha implementación será realizada tanto en software como en hardware de ellas aplicaremos sus políticas:

- Política Restrictiva. A través de la misma impediremos el tráfico salvo autorización expresamente en la configuración.
- Política Permisiva. Ayudará a permitir el paso a toda la comunidad salvo la expresamente prohibida.

6.2.2.1 Implementación Firewall por Software

Esta configuración dependerá del software que se vaya utilizar o con del que disponga la empresa, en el caso de la misma se realizara políticas de sistema operativo las cuales van a permitir configurar un amplio conjunto de reglas a modo de cortafuegos, tanto de entrada como de salida, además de otras importantes funciones y filtros de seguridad.

Cabe destacar que aun el funcionamiento cambien, en todos los firewall existen elementes comunes, como las reglas de entrada y reglas de salida, donde se configura si el mismo debe o no permitir el tráfico de ciertas aplicaciones.

6.2.2.2 Implementación Firewall por Hardware

La instalación y configuración de un firewall hardware es algo más compleja que por software, aunque afortunadamente la mayoría de los routers actuales incluyen esta tecnología que cumple perfectamente las funciones deseadas.

La empresa SOTO DOMINICANA implementara dispositivos que realizaran la gestión de cortafuegos, la cual ayudara en la seguridad de acceso a internet. Se dedicara grandes recursos a la protección de la misma ya que los ataques pueden

ser dirigidos desde cualquier parte del mundo y por muchos atacantes distintos, coordinamos o no.

Se crearan políticas en el firewall para darle valor a las buenas prácticas seguras, como la navegación por páginas que cuentan con certificados de seguridad, y en el caso de no contar con el mismo no introducir ningún dato que sea susceptible de ser robado. Se utilizaran navegadores actuales en la red y se mantendrán siempre actualizados de esta manera nos protegemos de vulnerabilidades que se hayan detectado.

Pero sobre todo se utilizara esta herramienta, para el bloquear el acceso a páginas con contenido peligroso así como la ejecución de Java Scripts que pudieran realizar tareas sin nuestra aprobación.

6.3 Servidor Proxy

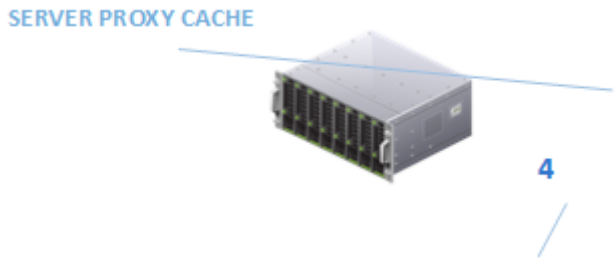


Figura 34.Grafico Anteproyecto – Proxy

Fuente: Propia.

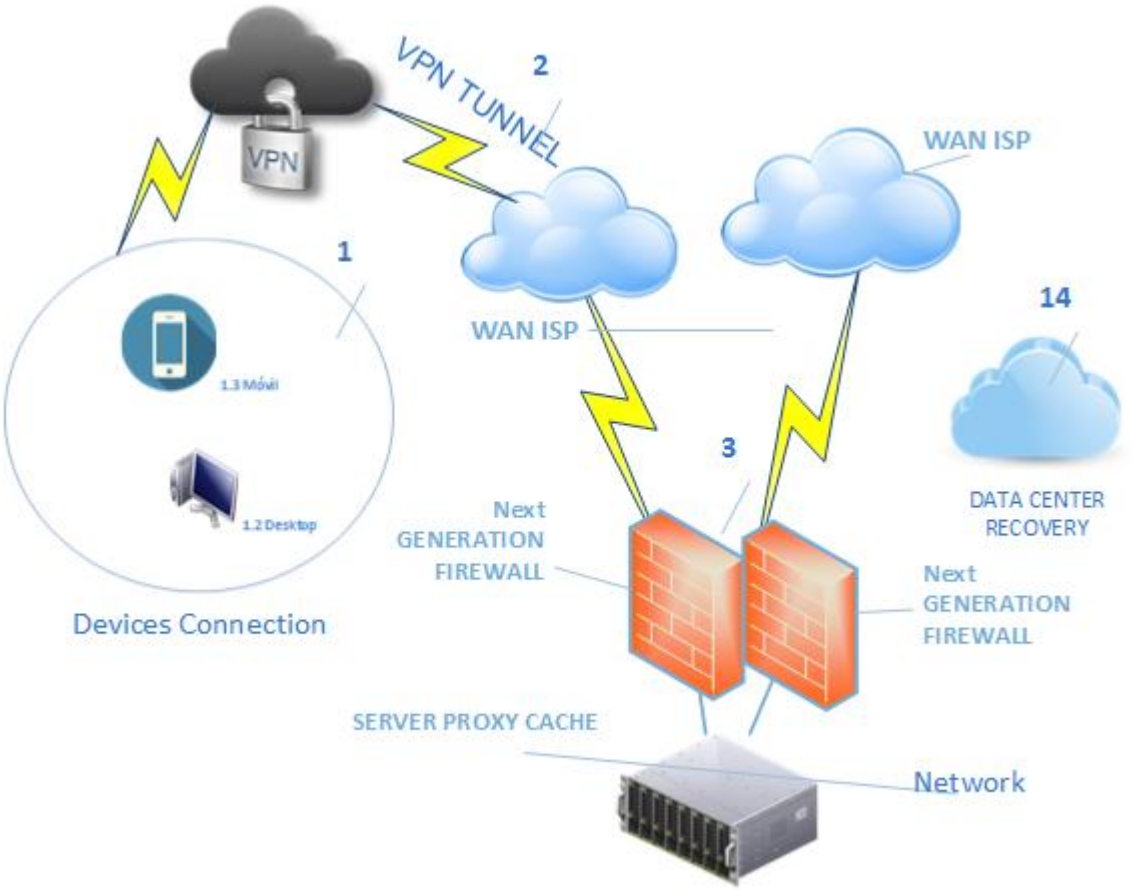
La empresa SOTO DOMINICANA busca perfeccionar su entorno de seguridad y para ello implementara un servidor proxy el cual además de estar de intermediario con la red externa, centralizara las conexiones de toda la misma.

Se implementara esta tecnología ya que:

- En la actualidad solo existen un único equipo o router con conexión a Internet;
- Ayudará a forzar a que todos los equipos pasen por un servidor seguro (Con SSL, Antivirus, cortafuegos, registros o log de sucesos y toda la medida de seguridad necesaria);
- Ayudará a aprovechar una conexión proxy cache y así hacer más eficaz el uso de ancho de banda de varios equipos;
- Pasen todo por un único puerto abierto, evitar conexiones a determinadas DNS, IP, Páginas Web, etc. O cualquier filtrado de paquetes.

La seguridad informática aportara grandes beneficios a la empresa SOTO DOMINICADA, la cual hoy en día no cuenta con ninguna de las tecnologías aquí citadas, en el levantamiento realizado a dicha institución se pudo observar las vulnerabilidades de la misma y lo mucho que afecta a la productividad esta problemática. De tal manera que si se siguen estas instrucciones se podrá sacar mayor provecho a la red y los recursos de la misma serán mejor distribuidos en el entorno.

6.4 Seguridad Implementación SOTO DOMINICANA



Fuente: Elaboración propia

Figura 35: Grafico Proyecto – Seguridad

SOTO DOMINICANA podrá disponer de una infraestructura segura y que cumple con los estándares y requerimientos internacionales entorno a la seguridad.

Como vemos parte del grafico nos indica los niveles de seguridad que se implementaran en la organización. En la misma desde un móvil o equipo (PC, laptop, etc.) tendrá que identificarse o disponer de un agente o cliente para tener acceso a la interacción a través de una conexión segura llamada VPN.

Además dispondrá de dos empresas de ISP (Internet Service Protocol) que aportaran redundancia ante cualquier inconveniente en la misma con el servicio. Toda estas conexiones tendrá que pasar por un Firewall el cual en coordinación con un proxy aportara más seguridad a la institución, de esta forma aportamos una mayor disponibilidad de negocios.

CAPÍTULO 7

Se realizará un estudio sobre los resultados y beneficios económicos de esta implementación.

7.1 Estudio de la factibilidad técnica, operativa, y económica

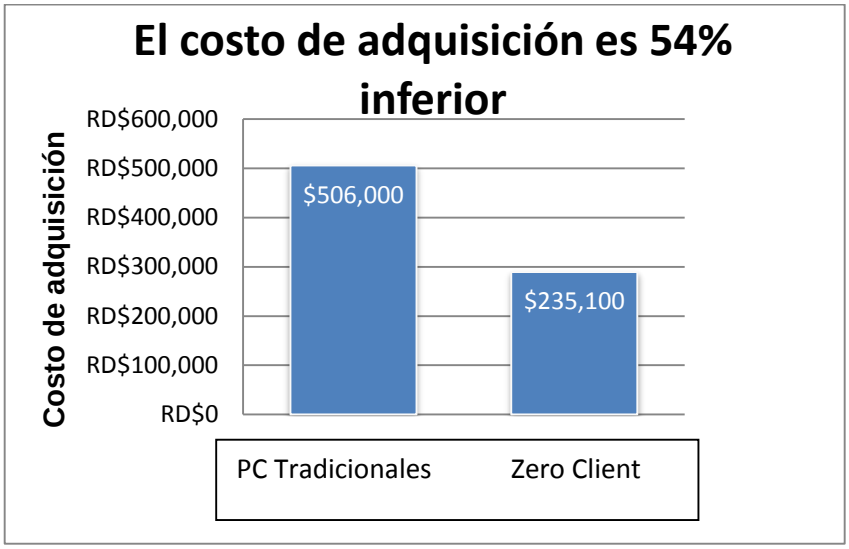
Las siguientes gráficas, cálculos y textos muestran la factibilidad de implementar el sistema multilenguaje en línea, con este sistema se logra un incremento en la venta de cursos en línea de hasta un 60%. En el aspecto económico es una inversión tan considerable que el simple ahorro en la factura de la energía eléctrica por el uso de zero client en los laboratorios y el aumento en la demanda de capacitaciones puede pagar el proyecto de implementación en pocos años.

7.2 Retorno de la inversión (ROI)

Realizar la inversión en mejorar la infraestructura de la tecnológica del data center y sus laboratorios e implementar un sistema traducción en tiempo real para las capacitaciones a distancia es una inversión de plazos de cinco a seis años. Adicional mostramos tablas que contemplan comparaciones del uso de energía eléctrica, los costos de mantenimiento y de actualizaciones de los equipos.

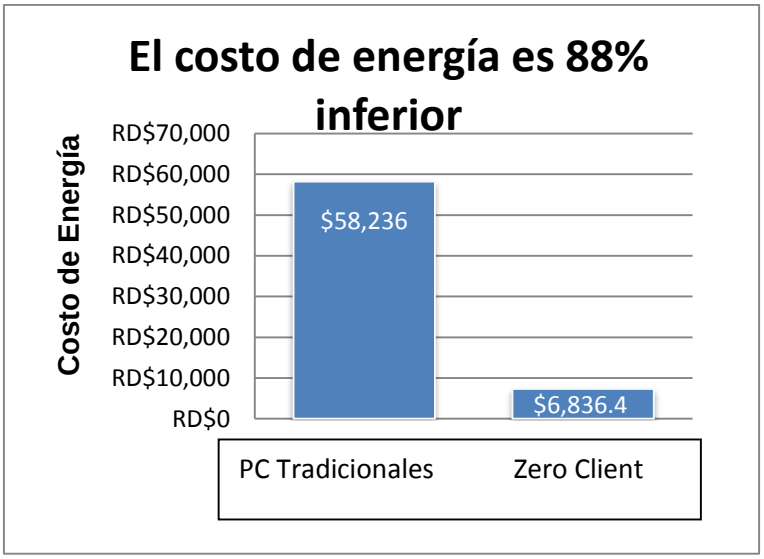
Las siguientes tablas equivalen al análisis:

Gráfica No. 1



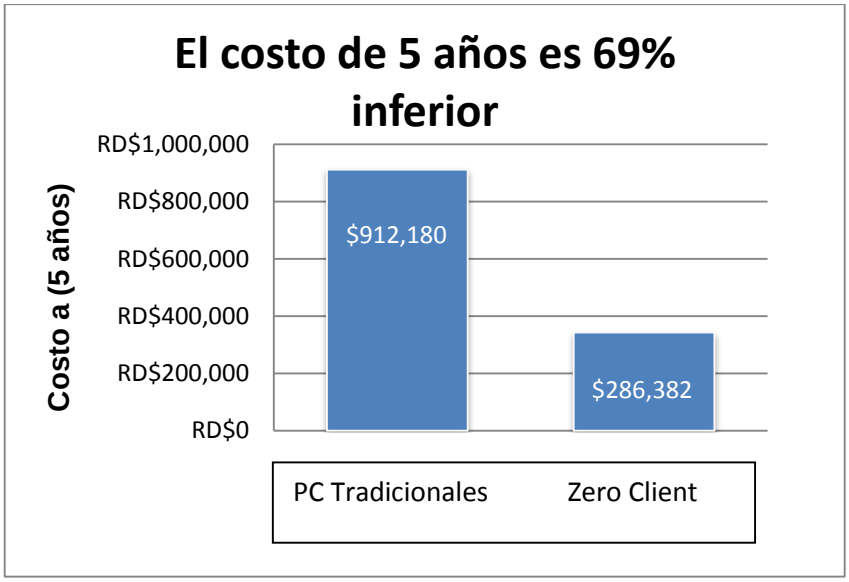
Adquirir las ciento treintas consolas ligeras + dos servidores es 54% inferior que adquirir ciento treintas computadoras de escritorio.

Gráfica No. 2



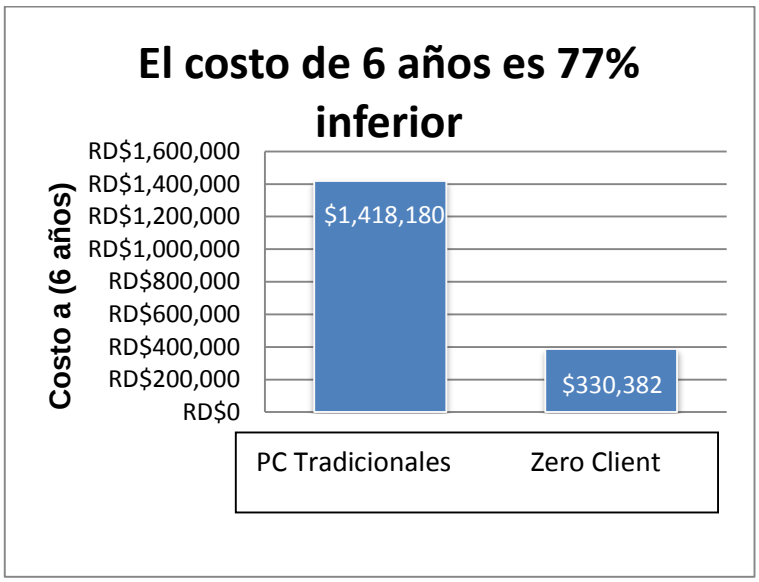
Las consolas ligeras consumirán 88% menos energía que las computadoras normales.

Gráfica No. 3



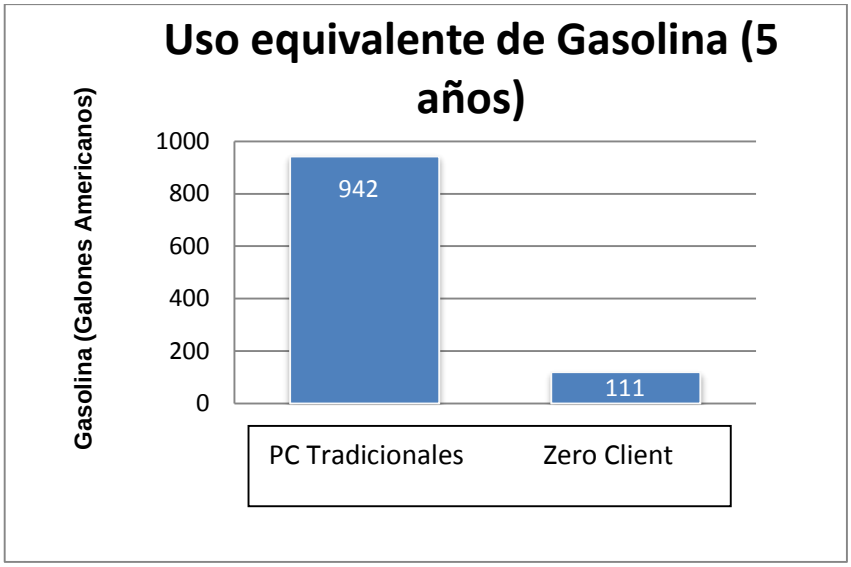
Al cabo de 5 años, el costo de poseer las consolas ligeras y darles mantenimiento es 69% inferior al costo de mantener productivas las computadoras por 5 años.

Gráfica No. 4



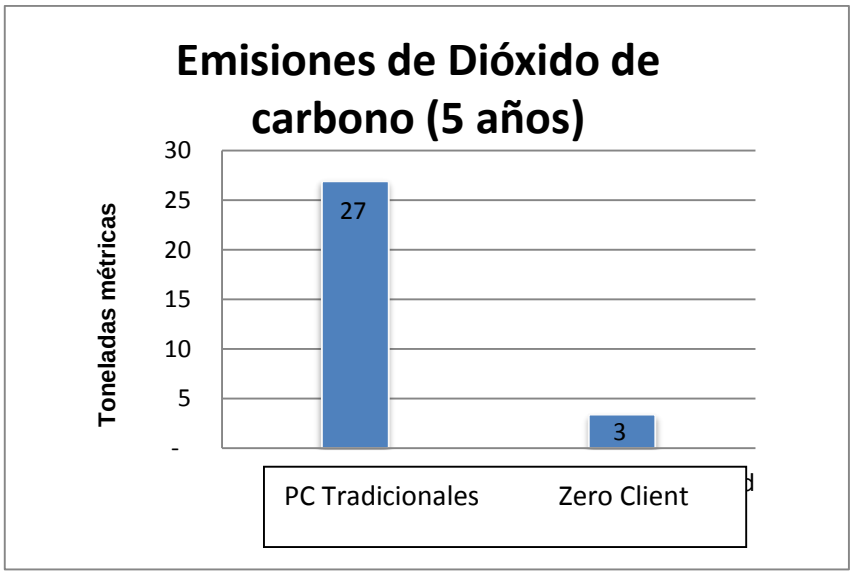
Al cabo de 6 años, el costo de poseer las consolas ligeras y darles mantenimiento es 77% inferior al costo de mantener productivas las computadoras por 6 años.

Gráfica No. 5

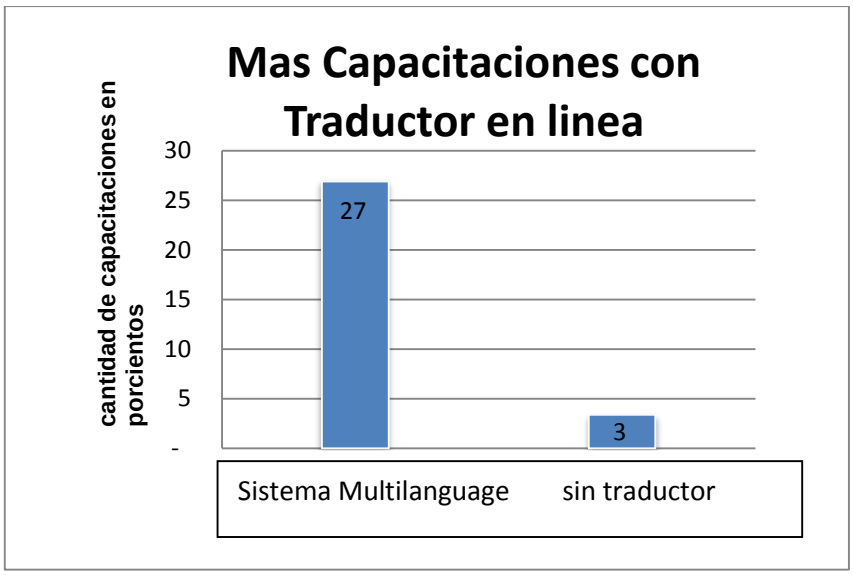


El tener estas computadoras trabajando por 5 años, equivale a 942 galones de gasolina contra 111 galones de gasolina de tenerse consolas ligeras.

Gráfica No. 6



Durante un periodo de 5 años las computadoras habrán emitido 27 toneladas métricas y las consolas ligeras a penas 3 toneladas métricas.



Durante un periodo de 1 año las capacitaciones tendrán una demanda de un 27 por ciento de aumento y las capacitaciones tradicionales sin traductor en línea a penas 3 por ciento.

7.3 Recomendaciones para la implementación

La implementación de los Virtual Desktop tendrá un periodo de 1-2 meses y se realiza acorde con las normativas y directrices establecidas por esta institución que realice el proyecto también se entrega documentos llamados “Best Practices”, dentro de las recomendaciones se destacan las siguientes:

- Definir correctamente los recursos de la implementación.
- Delimitar en tiempo y espacio el alcance de la implementación.
- Asegurar un calendario de actividades.
- Reemplazar paulatinamente las computadoras tradicionales por consolas ligeras y evaluar el desempeño de estas.
- La empresa que desea implementar debe definir el personal asociado al proyecto y únicamente debe de velar por esta asignación.

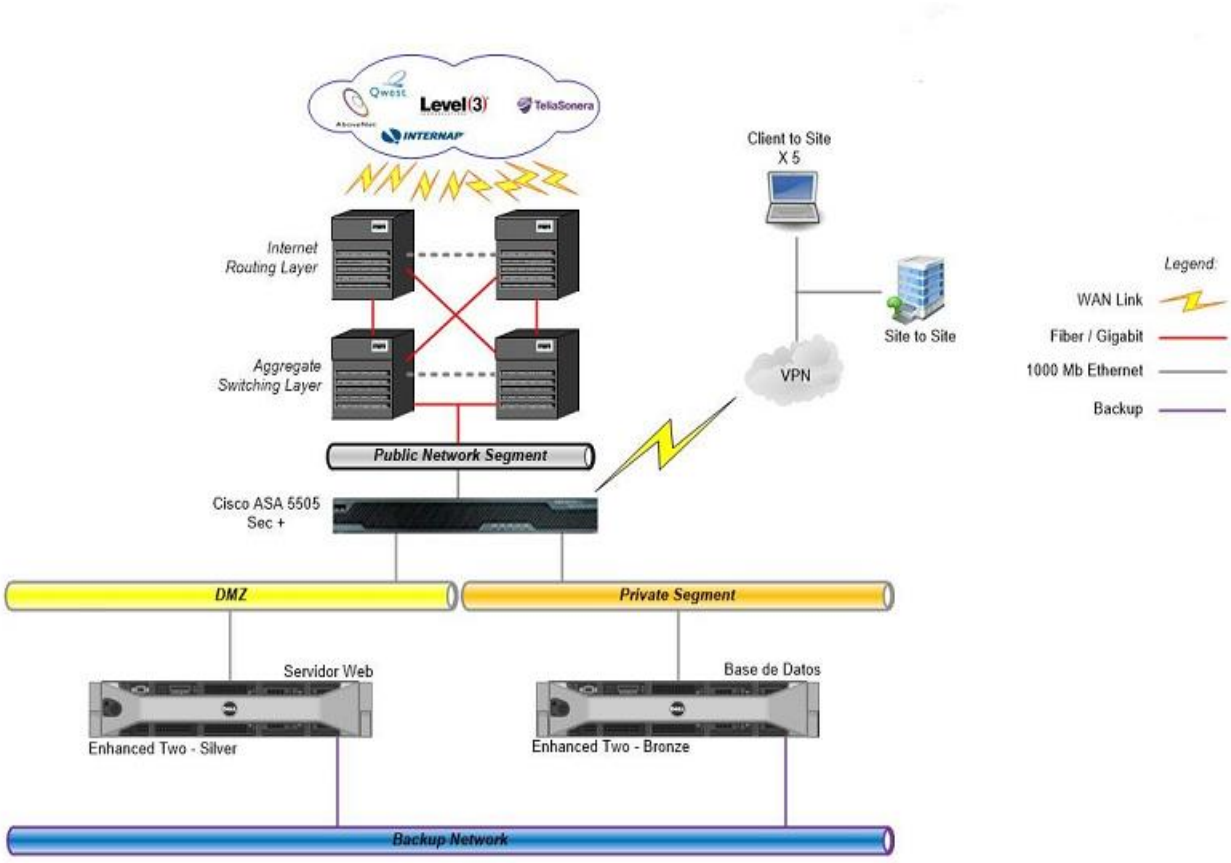
- La compenetración de los empleados de TI de la empresa que adquiera las consolas y los empleados de la compañía que realiza la implementación debe de ser óptima para asegurar una calidad en el proyecto.
- Durante el periodo de implementación se deben de realizar pequeñas entrevistas a las personas que ya han empezado a utilizar las consolas ligeras para tomar un pulso de la implementación y corregir fallas tempranas de tener que hacerlo.

Es importante seguir ciertas directrices para una correcta implementación, que cada cual vele por realizar correctamente su parte y un supervisor certifique estas actividades son algunos pasos extras que llevaran el proyecto a un final exitoso.

7.4 Presupuesto para la implementación Mejoras de la infraestructura tecnológica

Capacitación e-Learning

En este diagrama se presenta un modelo de infraestructura de alta disponibilidad de los servidores de la plataforma virtual



Fuente:(Soto 2014)

Figura 33: Diagrama de la Arquitectura que proponemos

Presupuesto de servidores Dedicados en un Data Center Fuera del País Por la Empresa RackSpace

Data Center:

Managed Linux Support Segment

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	Included	Included

- 24x7x365 Fanatical Support™
- 1 Hour Hardware Replacement Guarantee
- The Rackspace Zero-Downtime Network™
- Dedicated Account Management and Business Development Team
- Rackwatch Port Monitoring Service
- Included Access to My.Rackspace Portal (Ticket Manager, DNS Manager, Bandwidth and Backup Reports, Doc Center, Knowledgebase, Billing Options)
- Automated Server Patching via Distributed Red Hat Satellite Server

Rackwatch Platinum Port Monitoring

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	$0.00 USD	$0.00 USD

- Automated Ticket Creation and Response in Accordance with Support Policy
- 5 Minute Polling
- Choice of 6 Additional Ports to be Monitored (eg. FTP, SSH, DNS, POP3, MS SQL)
- Ping and TCP Port 80

Advanced Availability Monitoring

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	$0.00 USD	$0.00 USD

- Automatic Alert Escalation
- 10 Minute Polling
- Choice of URL, FTP or Mail Service Monitoring
- 1 Monitor

Additional Segment(s) / DMZ

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	$0.00 USD	$0.00 USD

- Please see included network diagram for details

Cisco VPN Access - Site to Site

Quantity	Setup Per Unit	Total Setup	One Time Per Unit	Total One Time
1	$0.00 USD	$0.00 USD	$65.00 USD	$65.00 USD

- Fully Managed, Software Updates and Management Included
- 3DES Encryption
- 1 Per Site

Cisco ASA 5505 Firewall Sec+

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	$200.00 USD	$200.00 USD

- Fully Managed Device, includes 24x7 Monitoring, Rule Changes and 1 Hour Replacement Guarantee
- Stateful packet inspection
- 150 Mbps Aggregate and 25,000 Concurrent Connections
- 100 Mbps Connectivity
- 3 DES
- Cisco VPN Access - Client to Site: Five (5) included [SKU: 106239]

Servidor Web
Enhanced Two - Silver

Quantity	Setup Per Unit	Total Setup	Monthly Per Unit	Total Monthly
1	$0.00 USD	$0.00 USD	$708.46 USD	$708.46 USD

- **Promotion Details:**Special pricing is subject to inventory availability. Please contact your sales representative for details on the date of acceptance to confirm pricing.
- **Operating System:**Red Hat Enterprise Linux 6 (licensed for 2 processors) [SKU: 106274]
- **Processor:**Dual Processor, Quad Core Intel 2.26GHz (Std.)
- **Memory:**24 GB (Std.)
- **Drive and RAID Configuration:**
  - RAID 1 [SKU: 102000]
  - 146 GB Std. (15K SAS 3.5") - Qty: 2
- **Drive Partitioning:**Rackspace Suggested Partitioning
- **Network:**1000 Mbps
- **Backup Agent:**Base Backup Agent [SKU: 103485]
- **Managed Backup:**
  - Unmetered Managed Backup (Requires Unmetered MBU Terms) [SKU: 105753]
  - Weekly Full, Daily Incremental
  - 2 Week On-site Retention (Per GB) [SKU: 105496]
- **Bandwidth:**2000 GB - Excluding SYD2 Datacenter - For Hosted Services in SYD2, please refer to pricing found at http://www.rackspace.com/information/legal/bandwidthpricing [SKU: 105549]
- **Operating System Options:**Standard File System
- **Operating System Add Ons:**No OS Add-Ons

Servidor de Base de Datos Enhanced Two - Bronze				
Quantity	**Setup Per Unit**	**Total Setup**	**Monthly Per Unit**	**Total Monthly**
1	**$0.00 USD**	**$0.00 USD**	**$708.74 USD**	**$708.74 USD**

- **Promotion Details:**Special pricing is subject to inventory availability. Please contact your sales representative for details on the date of acceptance to confirm pricing.
- **Operating System:**Red Hat Enterprise Linux 6 (licensed for 1 processor) [SKU: 106274]
- **Processor:**Single Processor, Quad Core Intel 2.26GHz (Std.)
- **Memory:**12 GB (Std.)
- **Drive and RAID Configuration:**
  - RAID 1 [SKU: 102000]
  - 146 GB Std. (15K SAS 3.5") - Qty: 2
  - RAID 10 [SKU: 102694]
  - 146 GB (15K SAS 3.5") - Qty: 4 [SKU: 103668]
- **Drive Partitioning:**Rackspace Suggested Partitioning
- **Network:**1000 Mbps
- **Backup Agent:**Base + MySQL Backup Agent (Red Hat Linux / CentOS Only) [SKU: 105087]
- **Managed Backup:**
  - Unmetered Managed Backup (Requires Unmetered MBU Terms) [SKU: 105753]
  - Weekly Full, Daily Incremental
  - 2 Week On-site Retention (Per GB) [SKU: 105496]
- **Bandwidth:**2000 GB - Excluding SYD2 Datacenter - For Hosted Services in SYD2, please refer to pricing found at http://www.rackspace.com/information/legal/bandwidthpricing [SKU: 105549]
- **Operating System Options:**Standard File System
- **Operating System Add Ons:**No OS Add-Ons

Monthly Recurring (1)	$1,617.20 USD
Total Monthly Invoice (2)	**$1,617.20 USD**
Setup Fee	$0.00 USD
One Time Fee	$65.00 USD
Total One Time/Setup Fee	**$65.00 USD**

7.5 Beneficios de esta implementación

Estará en un site alterno fuera del data center local para tener tolerancia a fallos y alta disponibilidad ya que se estará replicando los servicios y haciendo balanceo de carga entre las peticiones de los usuarios en los dos data center.

Propuesta de actualización del sistema de Gestión de Capacitación Fase (III)

A nivel tecnológico incluiría:

Sistema Multilenguaje en línea

Objetivos:

Desarrollo del Sistema multilenguaje en línea, el mismo estará implementado en un diseño web responsivo, con un alto nivel de seguridad, integración nativa con el sistema de evaluación virtual y capacidades de acceso remoto entre otras. Creación del portal institucional y la nueva cara gráfica para los demás componentes web (inclusión en el rediseño de las áreas de SOTO DOMINICANA virtual).

Sistema Multilenguaje en línea

Estará basada en las tecnologías más modernas con capacidades de acceso remoto, un amplio alcance tanto en vida útil como en su ejecución en una plataforma móvil. Se implementarán los Módulo que componen al sistema actual como son: Módulo de Registro, Módulo de administración, Módulo de diagnósticos, Módulo de caja y agregando nuevas capacidades como el módulo de integración entre otros.

Será una Sistemas móvil el cual podrá ser accesado desde una Tableta o cualquier navegador como: Google Chrome, Mozilla Firefox, Apple safari y Microsoft internet Explorer. La nueva tecnología que utilizaremos permite que el sistema opere en un alto nivel de eficiencia, brindando al mismo tiempo una aplicación estable y robusta.

A un alto nivel, el Sistema deberá proveer las siguientes funciones:

- Acceso en línea o Acceso remoto.
- Diseño Web Responsivo.

- Un alto nivel de seguridad.
- Integración nativa con el Sistema de Evaluación Virtual.
- Integración nativa portal Institucional.

Acceso remoto

Esta nueva capacidad permitirá el acceso remoto al sistema desde cualquier ordenador o tableta con acceso a internet desde cualquier parte del mundo.

Diseño web Responsivo adaptable

El Diseño web responsivo o adaptable permitirá que el sistema se adapte al entorno de usuario.

Integración nativa con el Sistema de Evaluación Virtual

La integración del sistema de evaluaciones virtual o Moodle será natural y sin esfuerzos. Desde el sistema se podrán accesar a las calificaciones, asistencias, notas, etc. de forma simple y fluida.

Vida útil

Este nuevo Sistema tendrá un alcance estimado de 9 años de vida útil, puesto que el mismo estará basado en nuevas tecnologías como son: .net mvc 2012, en c#, Sql Server. Esto nos permitirá crear un sistema pensado en satisfacer las necesidades actuales y futuras de los usuarios.

Creación PORTAL 2.0

Dentro de la propuesta está contemplada la creación de una nueva página web para la institución la cual se realizará en diseño plano o minimalista y Diseño Web Responsivo, esto permitirá un acceso rápido desde cualquier equipo como son: móviles, tabletas y ordenadores manteniendo una única dirección web; El nuevo PORTAL tendrá una Integración nativa con el Sistema de Evaluación Virtual.

Metodología

Para lograr los resultados antes descritos, proponemos un plan dividido en 5 fases:

- **Análisis de requisitos (y planificación)**
- **Diseño**
- **Implementación o desarrollo**
- **Lanzamiento**
- **Evaluación y Soporte**

Se planteó realizar este trabaja bajo fase, para lograr una metodología de trabajo que permita la realización de tareas puntuales. Se realizarán entregas previamente acordadas o marcadas como hitos dentro del plan detallado y se mantendrán reuniones de seguimiento de al menos 15 minutos y una reunión semanal con el cliente.

ESTIMACIÓN DE RECURSOS

- **Tiempo: Estimación de 12 meses para completar el sistema**
- **Costo: El proyecto tiene un costo de US$ 70,000.**

Presupuesto Equipos Informáticos

El proyecto tiene un costo global de **RD$13, 103,373.94** distribuidos de la siguiente forma:

DESCRIPCIÓN	Cantidad	PRECIO sin +ITBS	TOTAL + ITBIS
Cableado estructurado y electricidad de 2 laboratorios Nuevos	2	1,026.193.00	1,210.907.74
Línea de internet 100MB/3MB de velocidad	1	50,000.00	65,000.00
Servidores para Virtualizar	4	1,269.360.00	1,548.000.00
MOUSE KLIPX Optical KMO-104 USB	135	37,665.00	44,444.7
TECLADO KLIPX Multimedia KKM-101 USB	135	48,870.00	57,666.6
Laptop	25	26,506.5	RD$808,125.00
Thinclient	130	17,200.00	2,638.480.00
Equipos Wifi	4	85,140.00	100,465.2
Academic VMware Horizon View 5 Bundle:100 Pack	1	645,000.00	761,100.00
Academic Basic		135,450.00	159,831.00

Support/Subscription for VMware Horizon View 5 Bundle: 100 Pack for 1 year	1		
Academic VMware Horizon View 5 Bundle: 10 Pack	3	193,500.00	228,330.00
Academic Basic Support/Subscription for VMware Horizon View 5 Bundle for 1 year	3	40,635.00	47,949.30
Microsoft Windows Virtual Desktop Access - Subscription license (1 month) - 1 device - EDU, additional product - MOLP: Open Value Subscription	1	1,293.87	1,526.76
Win SvrStd 2012R2 OLP NL Gov 2Proc	6	161,464.14	190,527.68
WinRmtDsktpSrvcs CAL 2012 OLP NL GovDvcCAL	20	1,436.00	1,694.48
Kasperskyfor Virtualización	130	451.5	532.77
SQL Server Std 2012 OLP NL Gov	2	54,726.96	64,577.81
SQLCAL 2012 OLP NL GovUsrCAL	40	5,923.6	6,989.84
Office Std 2013 OLP NL Gov	130	34,307	40,482.26
Equipos de seguridad	2	318,405.97	375,719.04
Proyectores	5	25,830.00	157,500.00
Pantallas Para proyectores	5	14,750.00	17,405.00
CABLE NETSYS HDMI M/M 50FT	5	10,675.00	12,596.5
Total			**RD$9,571,850.74**

Presupuesto para mobiliario de laboratorios

DESCRIPCIÓN	Cantidad	PRECIO sin +ITBS	TOTAL + ITBIS
Mobiliarios de laboratorios (Sillas Y mesas)	190	441,740.00	521,253.20

Presupuesto del sistema Gestión de Capacitación

DESCRIPCIÓN	Cantidad	PRECIO sin +ITBS	TOTAL + ITBIS
Sistemas de Gestión de Capacitación	1	2,468.200.00	3,010.000.00

PRESUPUESTO TOTAL

DESCRIPCIÓN	Cantidad	PRECIO sin +ITBS	TOTAL + ITBIS
Sistemas de Gestión de Capacitación	1	2,468.200.00	3,010.000.00
Mobiliarios de laboratorios (Sillas Y mesas)	190	441,740.00	521,253.20
Cableado estructurado y electricidad de 2 laboratorios Nuevos	2	1,026.193.00	1,210.907.74
MOUSE KLIPX Optical KMO-104 USB	135	37,665.00	44,444.7
TECLADO KLIPX Multimedia KKM-101 USB	135	48,870.00	57,666.6
Línea de internet 100MB/3MB de velocidad	1	50,000.00	65,000.00
Servidores para Virtualizar	4	1,269.360.00	1,548.000.00
Storage Network VNX5100	1	1,559,671.49	1,840,412.35
Laptop	25	26,506.5	RD$808,125.00
Thinclient	130	17,200.00	2,638.480.00
Equipos Wifi	4	85,140.00	100,465.2
Academic VMware Horizon View 5 Bundle:100 Pack	1	645,000.00	761,100.00
Academic Basic Support/Subscription for VMware Horizon View 5 Bundle: 100 Pack for 1 year	1	135,450.00	159,831.00
Academic VMware Horizon View 5 Bundle: 10 Pack	3	193,500.00	228,330.00
Academic Basic Support/Subscription for VMware Horizon View 5 Bundle	3	40,635.00	47,949.30

for 1 year			
Microsoft Windows Virtual Desktop Access - Subscription license (1 month) - 1 device - EDU, additional product - MOLP: Open Value Subscription	1	1,293.87	1,526.76
Win SvrStd 2012R2 OLP NL Gov 2Proc	6	161,464.14	190,527.68
WinRmtDsktpSrvcs CAL 2012 OLP NL GovDvcCAL	20	1,436.00	1,694.48
Kasperskyfor Virtualización	130	451.5	532.77
SQL Server Std 2012 OLP NL Gov	2	54,726.96	64,577.81
SQLCAL 2012 OLP NL GovUsrCAL	40	5,923.6	6,989.84
Office Std 2013 OLP NL Gov	130	34,307	40,482.26
Equipos de seguridad	2	318,405.97	375,719.04
Proyectores	5	25,830.00	157,500.00
Pantallas Para proyectores	5	14,750.00	17,405.00
CABLE NETSYS HDMI M/M 50FT	5	10,675.00	12,596.5
Total			**RD$13,103,373.94**

Resultado esperado

Mejoramiento de la infraestructura tecnológica para poder brindar servicios de capacitación de calidad a la ciudadanía.

Beneficios:

- Un extendido período de obsolescencia en los equipos. Superior a 10 años
- Baja o mediana inversión inicial y reducción de costos. Mejora el TCO
- No requiere una renovación frecuente de equipos. Ahorro económico a mediano y largo plazo.

- Simplificados procedimientos de instalación y configuración. Rápido despliegue de equipos instalados y configurados.
- No se requiere de mantenimiento. Ahorro de recursos humanos y recursos operativos.
- Ahorro económico significativo mientras mayor es el número de equipos adquiridos.
- Ahorro de un 70 % de energía eléctrica comparados con equipos tradicionales. Ya que estos equipos consumen unos 13 Watts de electricidad.
- Mayor demanda de capacitaciones online

Capítulo 8

Se inicia con la historia de educación en línea, cuales son los desafíos y fronteras también sus características ventajas y desventajas.

8.1 ¿Cómo empieza la Educación a distancia?

La Educación a Distancia organizada puede remontarse al siglo XVIII, con un anuncio publicado en 1728 por la Gaceta de Boston, en donde se refería a un material auto-instructivo para ser enviado a los estudiantes con posibilidad de tutorías por correspondencia. Sin embargo, hay quienes arguyen que tal modalidad puede remontarse al texto bíblico, mencionándose las epístolas de los apóstoles.

En la Europa Occidental y América del Norte, la Educación a Distancia empezó en las urbes industriales del Siglo XIX, con el fin de atender a las minorías, que por diferentes motivos, no asistieron a escuelas ordinarias.

En 1922 el Pennsylvania StateCollege comienza con sus cursos por radio al igual que Columbia University mientras que en 1925 hace lo propio la State University of Iowa. El National Home Study Council se fundó en 1926 y en 1934 los cursos filmados comienzan con The State University of Iowa.

Al finalizar la Segunda Guerra Mundial, se produjo una expansión de esta modalidad para facilitar el acceso a los centros educativos en todos los niveles, especialmente en los países industrializados occidentales, en los centroeuropeos y en las naciones en desarrollo "tercermundistas". Esto obedeció al incremento de la demanda de mano de obra calificada registrada.

La educación por correo o correspondencia, también fue usada por las instituciones para ganar acceso a programas especializados o maestros que no estaban disponibles en el recinto.

El sistema de educación por correspondencia fue siendo reemplazado por el tipo de sistema de Educación de una dirección, lo cual se concreta para los años 1970 con el uso de medios electrónicos tales audios cintas, videocintas, radio, televisión y las computadoras. Tenemos así que en 1950 la Ford Foundation comienza con programas educativos por televisión, en 1965 la University of Wisconsin da cursos basados en comunicación telefónica y en 1968 la Stanford University crea una red por televisión. En 1969 comienza Open University de Londres.

En años recientes han tenido gran desarrollo las redes de computadoras de sistemas abiertos. En la actualidad, casi cualquier computadora se puede conectar a una red. Las redes como un medio para compartir recursos, de forma tal que una computadora personal puede utilizar el poder de procesamiento de una supercomputadora conectada a la misma red. Estas redes también resultan eficaces para apoyar el trabajo en grupo.

El correo electrónico, y el acceso a fuentes comunes de información, distribuidas en los dispositivos de almacenamiento de las computadoras son parte de los servicios típicos que ofrecen las redes de computadoras, es el medio organizacional para apoyar la organización de actividades cooperativas, a través del intercambio de mensajes entre los usuarios de la red.

A fines de la década de los ’90 e inicios del siglo XXI nos encontramos con un gran despliegue de las ofertas a distancia en diversos ámbitos y para todos los gustos: desde una carrera universitaria o de postgrado, hasta cursos para la satisfacción de un interés personal o el uso del tiempo libre.[9]

Figura 34: Educación Tradicional Vs Educación a Distancia

Imagen extraída de: http://1.bp.blogspot.com/-jNJS8V8zgN0/T10NZivHPeI/AAAAAAAAACs/LNRyAdJa4Dg/s1600/tradicional_vs_distancia.png

8.2 Características de la formación a distancia

A) Carácter interactivo. Al permitir que el alumno se comunique por medio de internet con su profesor tutor y con sus compañeros de clase, el carácter interactivo hace la gran diferencia de la web-basededucation en relación con otras

[9] Profesor loayza, http://www.galeon.com/histedudistan/

modalidades de educación a distancia. Una buena manera de conseguir un grado más elevado de interacción es por medio de programas basados en la lectura común de un texto. Estos programas permiten mayor interacción sincrónica entre personas conectadas simultáneamente al servidor.

B) Comunicación no sincrónica. El alumno se puede formar donde quiera, cuando lo quiera y durante el periodo que desee, promoviendo una libertad de acción que solo un curso por medio de la red puede ofrecerle.

C) Mediación personalizadas. Para cada grupo de alumnos debe haber un tutor disponible, es decir, un profesor orientador que podrá aclarar cualquier duda mediante el correo electrónico, conferencia en líneas y chats. Estas herramientas permitirán que cada alumno disponga de un trato personalizado, eliminando los problemas de introversión, creando una nueva interfaz con su profesor.

D) Aprendizaje significativo. Una serie de experiencias ya realizadas en diversas partes del mundo han evidenciado que los cursos basados en internet presentan un índice de efectividad mucho mayor que los convencionales. Si se les compara con los talleres y seminarios, los cursos que utilizan plataforma tecnológica presentan una tasa de retención 42% mayor. Al ser comparados con manuales impresos, presentan un resultado 61% mayor.

E) Seguimiento estadístico del desempeño del aprendiz. La plataforma de formación e entrenamiento de internet permite el seguimiento integral del alumno, validando su identidad por medio de mecanismo de seguridad y seguimiento y evaluando su desempeño y frecuencia. Este seguimiento también podrá ser hecho por el propio alumno.

8.3 Desafíos De la Educación a Distancia con base en internet

La mayoría de los cursos actualmente ofrecidos por medio de internet son de corta duración: de dos a seis horas, sin tutoría, en atención al concepto de justenough, just in time. Los estadunidenses hablan de distancelearning (aprendizaje a distancia) y no de education. Educación es más que aprendizaje: implica un proceso de interacción, comunicación y cultura.

Que puede ser educación a distancia con base en internet? La educación a distancia con base en internet, como el nombre lo dice web-basededucation, es aquella que utiliza como vehículo internet, o mejor que usa tecnologías de internet. La tecnología utilizada y la concepción de educación a distancia de la web son completamente diferentes de la computer-based training.

Unos de los mayores desafíos de la educación a distancia con base en internet están en el desarrollo de un lenguaje propio. La mayoría de los cursos ofrecidos vía internet reproduce la web la estructura presencial del salón de clase.[10]

8.4 Educación en línea

Se entiende por educación en línea (estudios en línea, formación virtual) aquellos especialistas, docentes y estudiantes que participan remotamente, a través de las redes de computadoras, haciendo uso intensivo de las facilidades que proporciona el internet y la tecnología, es una modalidad de educación a distancia que habilita un entorno de comunicación para los procesos de enseñanza y aprendizaje a

[10] (Moacir Gadotti, Siglo XXI 2003, Perspectivas actuales de la educación)

través de las tecnologías de la información y la comunicación(TIC). Esta, además, puede servir de complemento a la educación presencial o semipresencial, siempre que el proceso de enseñanza y aprendizaje entre los docentes y el estudiante se realice a través de las TIC.

Cada vez más, la educación en línea está convirtiéndose en una opción factible de continuar con los estudios de bachillerato, universitarios y de especialización o posgrado para aquellas personas que por su ubicación geográfica o por cuestiones laborales les resulta muy difícil acudir a una institución presencial, además de ser una estrategia educativa basada en la aplicación de tecnología al aprendizaje sin limitación del lugar, tiempo, ocupación o edad de los estudiantes. Con el tiempo el campo de la educación online se ha profesionalizado cada vez más hasta abarcar no solo estudios formales, sino también cursos de actualización y capacitación laboral en múltiples profesiones y oficios.

Se dice que es a distancia porque el estudiante no se encuentra en ningún centro educativo, sino que puede aprender desde su casa u oficina. Así, el estudiante no cuenta con un maestro en forma presencial y en ese mismo instante. A su vez la educación semipresencial combina clases presenciales y virtuales, así también los estudiantes puedan participar en tareas o actividades en el mismo momento, tiempo real (sincrónico) o en el tiempo particular (asincrónico).[11]

La educación en línea o el e-learning es la nueva modalidad de implementar o impartir clases de manera virtual mediante equipos o recursos tecnológicos. Estas clases son a distancia ya que el estudiante no se muestra de manera presencial

[11] Recuperado: revisado el 27 may 2014, http://es.wikipedia.org/wiki/Educaci%C3%B3n_en_l%C3%ADnea

en ningún centro educativo, si no que este puede tomar sus clases en cualquier lugar siempre y cuando tenga una computadora con acceso a internet. El estudiante no cuenta con un maestro presencial si no de manera virtual, muchas veces estas clases son pregrabadas, esta manera de implementar la educación es una manera factible ya que las mayorías de las personas hoy en día no poseen tiempo para desplazarse a un centro educativo y estas prefieren tomar sus clases de manera en línea. (Serrata, 2014)

8.5 Diferencias Entre Educación a Distancia e E-Learning

La educación a distancia no es más que la educación formal, basada en una institución en la que el grupo de aprendizaje se separa y en la que se utilizan sistemas de telecomunicaciones interactivos para conectar a los estudiantes, los recursos y los instructores, mientras que el E-learning usa nuevas tecnologías multimedia y de internet para mejorar la calidad del aprendizaje mediante el acceso a recursos y servicios o colaboraciones e intercambios a larga distancia.

Estas poseen similitudes, pueden ser sincrónica o asincrónica, ambas tienen conexión entre estudiantes y recursos con la mediación del instructor. Las diferencias que poseen estas se encuentran:

Educación a distancia:

-multitud de recursos para conectar al alumnado y/o profesorado: internet, correo postal, radio y televisión, etc.

-separación entre docente y estudiante (temporal e intelectual)

-telecomunicación interactiva, deseable pero no imprescindible.

-la información no siempre llega rápidamente no es posible actualizarla de manera inmediata.

E-Learning

-los recursos provienen casi exclusivamente de las nuevas tecnologías.

-la separación entre el docente y estudiante no siempre es temporal.

- la interactividad es mucho más probable entre estudiantes y entre estos con el profesorado por la propia naturaleza de los recursos tecnológicos utilizados.

-tanta la información como la actualización de dicha información pueden ser inmediatas. (Herrera, 2008)

La educación a distancia no es más que la educación que se recibe bajo el reglamento de una institución pero con el grupo de alumnados separados, esta evalúa cada persona de manera singular ya que todo se basa en correos, cartas u otros medios de comunicación, mientras que el E- learning es el nuevo método de implementación de una educación a distancia pero más personalizada ya que los medios de comunicarse el alumnado y el profesor se hace de una manera virtual u videos chats que permiten al alumno interactuar de manera más eficaz con el profesor, este método mejora la calidad del aprendizaje.**(Serrata, 2014)**

8.6 ELEARNING

UNESCO (1998) define elearning como: entornos de aprendizajes que constituyen una forma totalmente nueva, en relación con la tecnología educativa. Un programa informático- interactivo de carácter pedagógico que posee una capacidad de comunicación integrada. Son una innovación relativamente reciente y fruto de la convergencia de las tecnología informáticas y de telecomunicaciones que se ha intensificado durante los últimos diez años.

Haciendo una revisión bibliográfica se encentran innumerables definiciones de elearning, pero sintetizado, podemos considerar elearning como una nueva forma de educación caracterizada por el uso de las TIC, particularmente tecnologías internet, que aprovecha la facilidad de distribución de materiales formativos y herramientas de comunicación para crear un entorno de aprendizaje. Mediante esta tecnología, el estudiante tiene acceso a cursos interactivos bien sea en multimedia o en formato web, apoyados con sistemas que permiten la colaboración y discursos online.

Fuente: Elaboración Propia

Figura 35:

8.6.1 Ventajas de E-learning

El entorno elearning ha suscitado muchas discusiones, al igual que se dio en los comienzos de la educación a distancias. No se trata de que el sistema de educación tradicional sea revaluado, se trata de que estemos ante un sistema que ofrece ventajas respecto a dificultades presentadas por los estudiantes. La educación virtual no reemplaza los sistemas tradicionales, solo ofrece a la población diferentes alternativas y potencialidades. Las ventajas de la educación utilizando e learning se puede sintetizar en:

1. Costo-efectividad: particularmente en el caso del mercado corporativo, la información distribuida a través internet, sin duda tiene una relación costo-eficiencia en gran medida, ya que quieres participan, ven disminuido sus costo respecto de si tuvieran un instructor presencial. Esto deriva de menos gastos en viajes e instalaciones pues el docente puede estar en su casa.
2. Tiempo: a diferencia de la educación tradicional, quienes se forman a distancia, se ven liberados del condicionamiento tiempo y es así que el participante distribuye su esfuerzo en consonancia con su forma de vida y su contexto, pudiendo acceder a la información en el momento que lo considere oportuno.
3. Aprendizaje auto gestionado: esto surge de los sistemas a distancia como aquellos que favorecen el aprendizaje independiente.
4. Flexibilización del proceso didáctico: aprendizaje en los tiempos personales.

5. Interactividad: un medio es interactivo cuando tiene la capacidad de implicar a quien aprende activamente en la actividad que viene implícita en el diseño. Si bien, el computador tiene un alto grado de interactividad funcional, puede no favorecer la interacción cognitiva si el programa no se diseña con esa intencion.uni
6. Aprendizaje en el lugar conveniente: con ello se consigue disminución de costo de traslado y permanencia.
7. Accesibilidad: sin duda el acceso se amplía con la distribución a domicilio, con este tipo de aprendizaje on-line el mercado se segmenta y se puede acceder a distintos grupos tales como los que estudian a domicilio o los que se capacitan en su trabajo.
8. Uniformidad de contenido: todos los participantes reciben igual material didáctico.
9. Actualización rápida: frente a una sociedad tan dinámica, es importante el cambio y la revisión rápida de los contenidos y es precisamente una de las fortalezas de internet, sus capacidades para acceder a la información más reciente. (Edgar Javier Carmona Suarez, Elizabeth Rodríguez Salinas, ELIZCOM S.A.S, Tecnologías de la Información y la Comunicación Ambientes Web para la calidad educativa)

8.6.2 Recomendaciones:

- Mayor trabajo de planificación y desarrollo del curso.

- Necesidad de un equipo técnico de producción y de gestión.
- Producción de materiales educativos de calidad.
- Depende de la conexión a internet y de la existencia de un ordenador, lo que conlleva que, si es un equipo personal, debe hacer frente a los costes de acceso a internet.

Obstáculos en la implantación de e-learning

De acuerdo a la opinión mostrada por los profesionales encuestados, una crítica importante lo constituye que el e-learning al estar basado en tecnologías de red sea considerado como un sistema de formación frio, motivado por la falta de interacción, de intercambio espontaneo entre las partes, faltando una presencia para los usuarios en la que exista acción reciproca, alguien más que participa también en el acto formativo. Además en ocasiones se le tilda de un sistema distante y distanciador. Sin embargo, los potenciales usuarios que se refieren al sistema como frio y poco conectado tienen una imagen ambigua del sistema, carecen de referentes claros y únicos sobre lo que conlleva. Los aspectos comportamentales y relaciones que se valoran como tan importantes en la formación no se desarrollarían en este tipo de formación, e-learning se posiciona como método auxiliar, no suplementario de la formación presencial. (Manzanedo, 2003)

8.6.3 Reseña

El mayor obstáculo que presenta el e-learning es que no todas las personas tienen acceso a internet, ya que existen países que el margen de pobreza es extrema y esto sería un gran obstáculo ya que no todas las personas tienen un acceso a una computadora o acceso a la internet. Otro obstáculo es la energía eléctrica ya que sin esta no se podría hacer nada, el e-learning es una excelente manera de impartir clases a distancias pero se debe ver todas las caras para saber cuáles seria sus obstáculos, aparte de que no todas las personas saben manejar una computadora, este sería una gran problemática. (Serrata, 2014)

Ulearning

El aprendizaje ubicuo o u-learning es una metodología de formación que se caracteriza por englobar actividades formativas apoyadas en las nuevas tecnologías.

Bajo este término se agrupa la presencia las TIC en todos los momentos y situaciones en los que la persona aprende. El termino ingles ubitoquious que se traduce al español ubicuo hace referencia a formación disponible en distintos canales y soportes en cualquier momento. Sin ánimo de establecer una norma, proponemos que al hablar de u learning lo asociemos a aprendizaje universal ya que nos parece una forma interesante para recordar la idea global.

El objetivo del u-learning es brindar la posibilidad de aprender una persona cuando trabaja con su ordenador, cuando tiene a mano un dispositivo móvil más o menos

sofisticado, cuando se sienta frente al televisor o cuando esta compartiendo la web participativa cuando está viviendo su vida virtual. (U-learning Lorena Goetschel, 17 Feb 2011.)

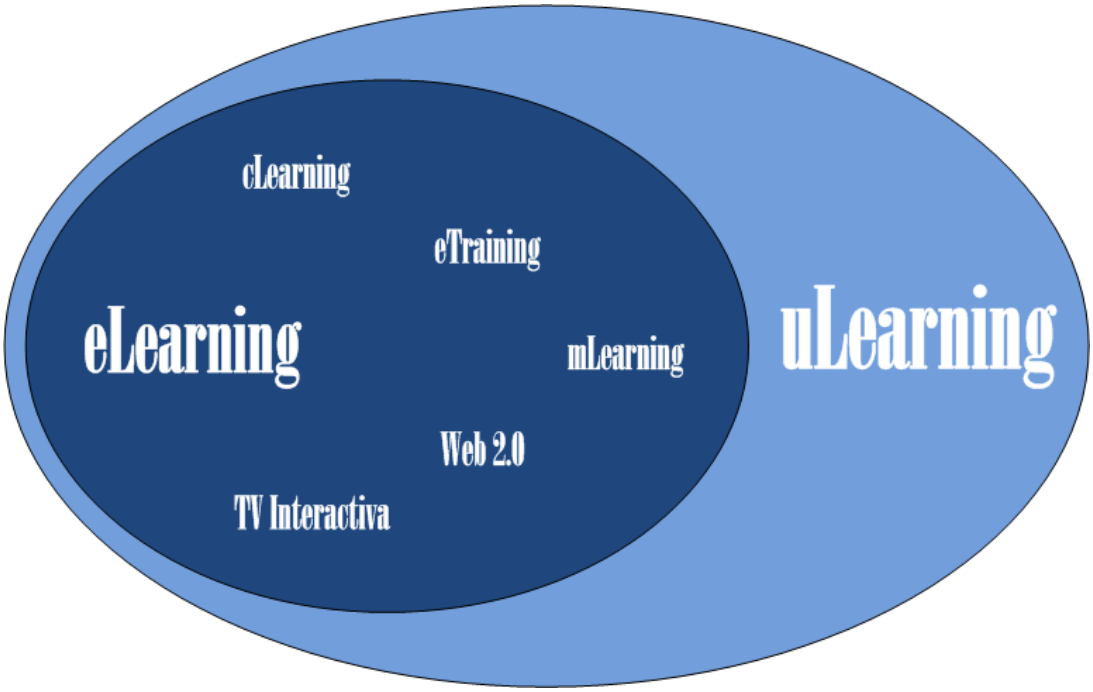


Imagen extraída de: Elaboración Propia

Figura 36:

Ventajas:

- Eliminar barreras de tiempo, distancia, económicas y sociales, los individuos pueden tomar las propias riendas de su vida educativa.
- Sesiones de aprendizaje más cortas, de mayor frecuencia y compaginadas con las actividades cotidianas de las personas.
- Aprendizaje en entornos virtuales atractitvos y sofisticados.

- Se promueve el aprendizaje autónomo y colaborativo
- Desarrollo de habilidades y competencias tecnológicas para el trabajo y para la vida.

Recomendaciones

- Se pueden elevar el número de deserciones por no saber usar las herramientas tecnológicas
- No todas las personas tienen acceso a estas herramientas, sobre todo las personas que viven en pobreza
- Aun no existe una cultura sobre el uso de estas herramientas tecnológicas que garantice el adecuado uso de la información.[12]

8.7 M-Learning

Es un tipo de aprendizaje móvil que es facilitado vía PDA, teléfono móvil o una laptop de manera inalámbrica. El m-learning o aprendizaje móvil constituye una nueva forma de aprendizaje personal que nunca termina, permitiendo que más y más personas se den cuenta de que nuestras vidas en este planeta puedan convertirse en múltiples y verdaderas aventuras de aprendizaje personal.

Los partidarios del aprendizaje de por vida han estado promoviendo este cambio de como concebimos, diseñamos y compartimos información. Los individuos están aprendiendo de forma constante, buscando, cuestionando y reconociendo nueva

[12] http://yessedik.blogspot.com/2012/07/u-learning-ventajas-y-desventajas.html

información del entorno en el cual operan, sin importar cuáles son sus intereses o especializaciones. **(Enrique Ruiz Velasco Sánchez, Ediciones Díaz De Santos, 22-4-2013, Cibertronica).**

El aprendizaje móvil ha sido una nueva forma de aprovechar las tecnologías de información y comunicación (TIC) para acceder al conocimiento, mediante dispositivos como el celular o los asistentes personales(PDA), relacionado las aplicaciones y los servicios que ofrecen, posibilitando adecuarlos a actividades educativas que pueden soportar estas herramientas. Algunas aplicaciones son videos, audios, juegos y servicios como el correo electrónico, entre otros. Existen varios requisitos a considerar para la selección de las aplicaciones**. (María Soledad Ramírez Montoya, lulu.com, Recursos educativos abiertos y móviles para la formación de investigadores: Investigaciones y experiencias prácticas.)**

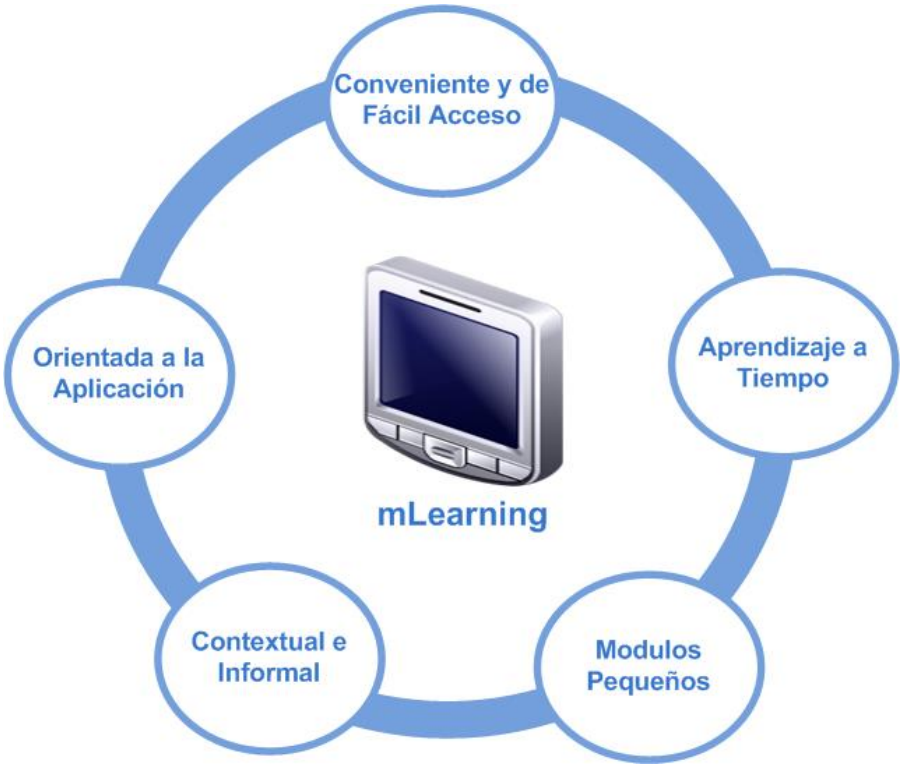


Imagen extraída de: Elaboración propia

Figura 37:

Ventajas:

- Permite el aprendizaje en cualquier momento y lugar.
- Puede mejorar la interacción didáctica de forma sincrónica y asincrónica
- Potencia el aprendizaje centrado en el alumnado
- Permite la personalización del aprendizaje
- Favorece el aprendizaje colaborativo
- Evaluación inmediata de contenidos educativos
- Creación de comunidades de educandos
- Mejora de la formación continua
  (Luz, 2014)

Recomendaciones:

- Usabilidad: la tarea de escribir en las pequeñas pantallas, con sus teclados peliculiares se puede complicarse hasta extremos.
- Existen pocas aplicaciones educativas
- Dificultades o imposibilidad de instalar y usar determinado software.[13]

El m- learning es la educación implementanda mediantes PDA´s o tablets, esta se ejecuta de manera inalámbrica, ya que las mayorías de los teléfonos tienen acceso a internet. Este tipo de manera de implementación es factible en el ámbito de que no necesitas un lugar especifico siempre tendrás acceso a esta mediante tu equipo móvil o tu tablets. Uno de las desventajas que posee estas es el tamaño de la pantalla o las pocas aplicaciones que están disponibles para implementar el m-learning. (Serrata, 2014)

8.8 Traducción en línea

La **traducción automática o en línea** es un área de la lingüística computacional que investiga el uso de software para traducir texto o habla de un lenguaje natural a otro. En un nivel básico, la traducción por computadora realiza una substitución simple de las palabras atómicas de un lenguaje natural por las de otro. Por medio del uso de cuerpos lingüísticos se pueden intentar traducciones más complejas, lo que permite un

[13] http://mlearning2012.blogspot.com/p/ventajas-y-desventajas.html

manejo más apropiado de las diferencias en la tipología lingüística, el reconocimiento de frases, la traducción de expresiones idiomáticas y el aislamiento de anomalías.

Normalmente, los sistemas de traducción automática actuales permiten establecer parámetros (por ejemplo, limitando el rango de sustituciones permitidas) de acuerdo con el dominio o la profesión en la que se hace la traducción, lo que efectivamente mejora el resultado. Esta técnica es particularmente útil en campos donde se emplea un lenguaje formal o basado en formularios, como los reportes del tiempo y los documentos legales o administrativos, pero su uso no es viable en la traducción de conversaciones u otros textos menos estandarizados.

En las últimas décadas ha habido un fuerte impulso en el uso de técnicas estadísticas para el desarrollo de sistemas de traducción automática. Para la aplicación de estas técnicas a un par de lenguas dado, se requiere la disponibilidad de un corpus paralelo para dicho par. Mediante este corpus se estiman parámetros de sendos modelos estadísticos que establecen la probabilidad con la que ciertas palabras son susceptibles de traducirse por otras, así como las posiciones más probables que tienden a ocupar las palabras de la lengua destino en función de las palabras correspondientes de la frase origen. El atractivo de estas técnicas radica en que el desarrollo de un sistema para un par de lenguas dado puede hacerse de manera muy automática, con una muy reducida necesidad de trabajo experto por parte especialistas en lingüística.

8.8.1 **Historia de la Traducción Automática**

La aspiración de obtener artilugios mecánicos que sirvan para superar las barreras lingüísticas viene de antiguo. En el siglo XVII se habla de la utilización de diccionarios mecánicos (basados en códigos numéricos universales) para superar las barreras del lenguaje, dentro de un movimiento a favor de la creación de una "lengua universal" no ambigua, basada en principios lógicos y símbolos icónicos, que permitiese comunicarse a toda la humanidad. Este empeño precede por bastante tiempo a la propia existencia del ordenador. Por ello, se puede entender que desde el momento en que un ordenador estuvo disponible en la década de 1940, la traducción automática pasó a convertirse inmediatamente en una de las aplicaciones estrella de la informática.

Desde entonces, ha dado tiempo a realizar numerosos experimentos, pequeños y grandes, así como inversiones institucionales e industriales sustanciosas. Un referente obligado para conocer con más detalle la evolución de la traducción automática es el académico británico John Hutchins, cuya bibliografía puede, por suerte, ser consultada libremente en Internet. En esta breve reseña de la TA vamos a seguir el esquema simplificado de Johnatan Slocum, que aborda la historia de la TA por décadas. A sus cuatro décadas hasta 1985 vamos añadir dos más: seis décadas.[14]

[14] http://www.foroswebgratis.com/tema-que_es_in_traductor_en_l%C3%ADnea-86650-691986.htm

8.8.2 Sistemas De Videoconferencia

La videoconferencia es una herramienta eficaz para las organizaciones para comunicarse directamente con los socios y clientes. Las organizaciones con varias ubicaciones suelen utilizar la videoconferencia para realizar reuniones sin incurrir en gastos de viaje. Tandberg y Polycom ofrecen múltiples opciones para la realización de videoconferencias. Estas empresas proporcionan a las organizaciones el hardware, software, los servicios y la capacitación que hacen que la videoconferencia sea una parte integrada de la organización. Aunque Tandberg y Polycom utilizan tecnologías de videoconferencia similares, las empresas ofrecen diferentes soluciones de software y hardware.

Tandberg

Tandberg es parte de Cisco Systems, y utiliza una red fiable con sistemas de seguridad redundantes para garantizar una videoconferencia confiable. Tandberg ofrece sistemas de hardware inmersivos, personales y para espacios de usos múltiples conectados por un servidor de comunicaciones de vídeo. Estos sistemas también utilizan sistemas de audio y vídeo de alta definición. Además, Tandberg proporciona control de llamadas, administración, servicios de medios, servicios técnicos y de consultoría, así como soporte de periféricos y accesorios.

Polycom

Polycom también ofrece videoconferencias en alta definición. El hardware de Polycom soporta configuraciones de espacios de usos múltiples y configuraciones personales en un dispositivo de escritorio o móvil. Este sistema también permite la colaboración universal de video, recursos de vídeo, gestión de la virtualización, así como acceso y seguridad universales. Los productos y servicios de Polycom también pueden comunicarse en tiempo real con otros componentes que utilizan configuraciones compatibles de vídeo-conferencia. Además, Polycom ofrece soluciones de conferencia de voz y video con la capacitación, el apoyo administrativo y la certificación que se requieran.

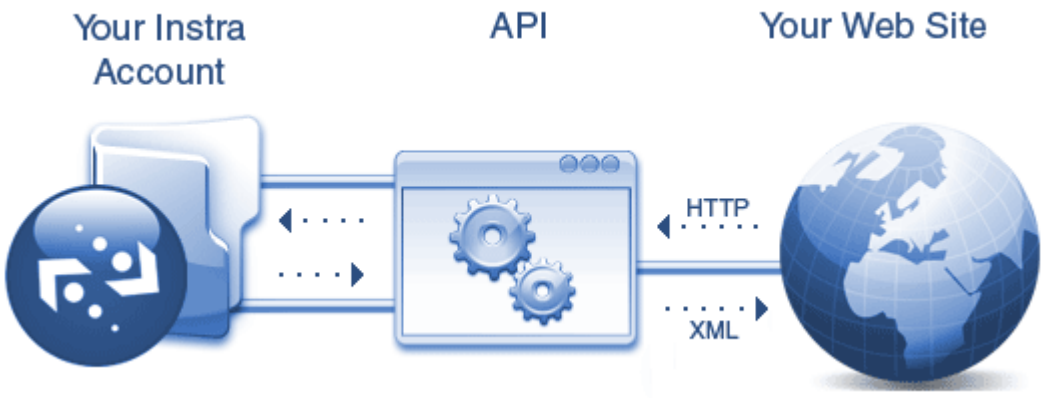
Semejanzas

Tandberg y Polycom se dirigen a una base de clientes similar. Ambas empresas usan tecnología de captura de última tecnología que proporciona señales de video y audio claras. Además, el software utilizado por ambas compañías tiene funciones de zoom que se centran de forma automática en las personas que hablan. Además, Tandberg y Polycom utilizan la triangulación de voz y software de reconocimiento facial para centrarse en una persona específica. Las empresas también ofrecen protocolos de seguridad altamente sofisticados para asegurar que el contenido de la conferencia de vídeo llegue a su destino previsto.

Diferencias

Una diferencia principal entre Tandberg y Polycom se relaciona con el software y hardware que se utiliza para operar los sistemas. Tandberg utiliza una única plataforma de hardware, software y un control remoto. Esto reduce la curva de aprendizaje del sistema y reduce al mínimo la capacitación necesaria. Polycom, por otra parte, ofrece una variedad de soluciones de hardware y software. Los sistemas Polycom también soportan configuraciones avanzadas que trabajan con varios sistemas operativos.[15]

API



Una API es una interfaz de programación de aplicaciones (del inglés API: Application Programming Interface). Es un conjunto de rutinas que provee acceso a funciones de un determinado software.

Son publicadas por los constructores de software para permitir acceso a características de bajo nivel o propietarias, detallando solamente la forma en que

[15] http://www.ehowenespanol.com/comparacion-sistemas-videoconferencia-hd-tandberg-polycom-info_307857/

cada rutina debe ser llevada a cabo y la funcionalidad que brinda, sin otorgar información acerca de cómo se lleva a cabo la tarea. Son utilizadas por los programadores para construir sus aplicaciones sin necesidad de volver a programar funciones ya hechas por otros, reutilizando código que se sabe que está probado y que funciona correctamente.

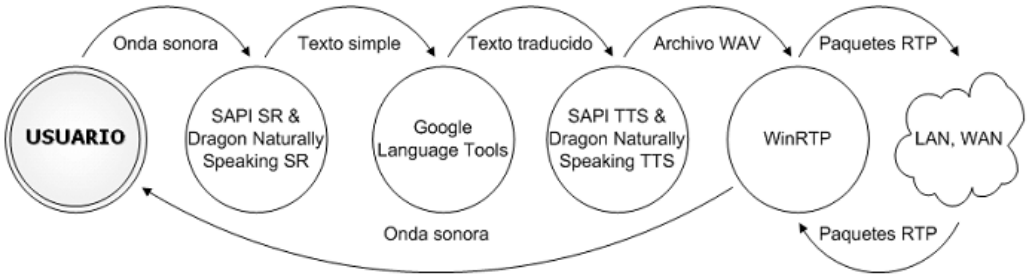
Interfaz de programación de aplicaciones. Conjunto de constantes, funciones y protocolos que permiten programar aplicaciones. Una buena API facilita la tarea de desarrollar aplicaciones, ya que facilita todas las piezas y el programador solo tiene que unirlas para lograr el fin que desea. Podríamos traducir como interfaz de programación entre aplicaciones, hace referencia a ciertos servicios y librerías que permiten acceder a procesos entre componentes de software. Dicho de otra forma, es una manera de abstracción que ofrece acceso a un conjunto de funciones de uso general, para asi evitar que haya que volver a programar todo desde cero cada vez que se utiliza.

En términos de aplicaciones web, cuando nos referimos a una API, por lo general estamos hablando de bibliotecas que ofrecen funcionalidades de acceso a los diferentes servicios. En (Staff)todas las aplicaciones web que lograron cierto éxito han publicado alguna API para operar con su servicio.

Reseña:

Los API es una interfaz gráfica para la programación de aplicaciones graficas este proporciona la funcionalidad necesaria para definir todos los elementos y operaciones que se usaran en el desarrollo. Es la interfaz de programación que te

permiten modificar o unir sin tener que empezar desde cero el programa. Esta es una maravillosa herramienta ya que te facilita todas las piezas y solo debes unir las piezas y formarlas no tienes la necesidad de crear o empezar desde cero una aplicación. (Serrata, 2009)



Fuente: Propia

Implementación

Métodos de Reconocimiento de voz Tres son los métodos que han marcado la historia del reconocimiento de voz; ellos son: “Alineamiento temporal dinámico”, “Modelos ocultos de Markov”, y “Redes neuronales”. Cada uno de estos métodos se aborda en los puntos siguientes.

Alineamiento temporal dinámico El concepto de “Alineamiento temporal dinámico” (conocido como DTW, del inglés Dynamic Time Warping) se ha empleado para obtener la distorsión o diferencia entre dos palabras. Muchas veces una palabra puede no pronunciarse siempre a la misma velocidad o bajo las mismas condiciones del ambiente o del mismo locutor, es necesario entonces, ajustarla a un patrón para interpretar correctamente la información.

DTW está basado en la comparación todas las plantillas referencia resultado de anteriores entrenamientos contra plantillas compuestas de vectores de parámetros, calculados a partir de los distintos segmentos en que fue dividida la señal de entrada.

Para hacer la comparación se calcula la distancia mínima entre la referencia y la entrada, y finalmente se escoge la plantilla que entregue la menor distancia. Los reconocedores de habla basados en DTW son fáciles de implementar y muy efectivos para Vocabularios.

El desarrollo del software fue por prototipado. Para implementarlo se buscó un lenguaje que además de ser compatible con las bibliotecas SAPI y WinRTP, fuese de un nivel lo más cercano posible al sistema operativo para obtener un mejor rendimiento.

Por estas razones, se optó por implementar el prototipo en Microsoft Visual C++ .NET accediendo directamente a las APIs de Windows. Cabe destacar que no se emplearon funciones propias de .NET tales como MFC (Microsoft Foundation Classes) y herramientas para servicios web.

La aplicación comienza con el cuadro de diálogo. El usuario debe ingresar un nombre y elegir el modo de reconocimiento de voz que necesite. El nombre de usuario es necesario para asociar al locutor con el modo de reconocimiento escogido de esta forma, mientras más sesiones de entrenamiento ejecute el locutor, mejor será el reconocimiento.

Toda la información extraída acerca de su voz se guarda en un perfil creado con su nombre de usuario, que a la vez, es su identificador principal. Al hacer clic en Aceptar un mensaje informará si el perfil existe en el sistema o si ha creado uno. Es el menú de las dos opciones de traducción. Si por ejemplo el locutor escoge Inglés, entonces todo el texto reconocido se traducirá de inglés a español.

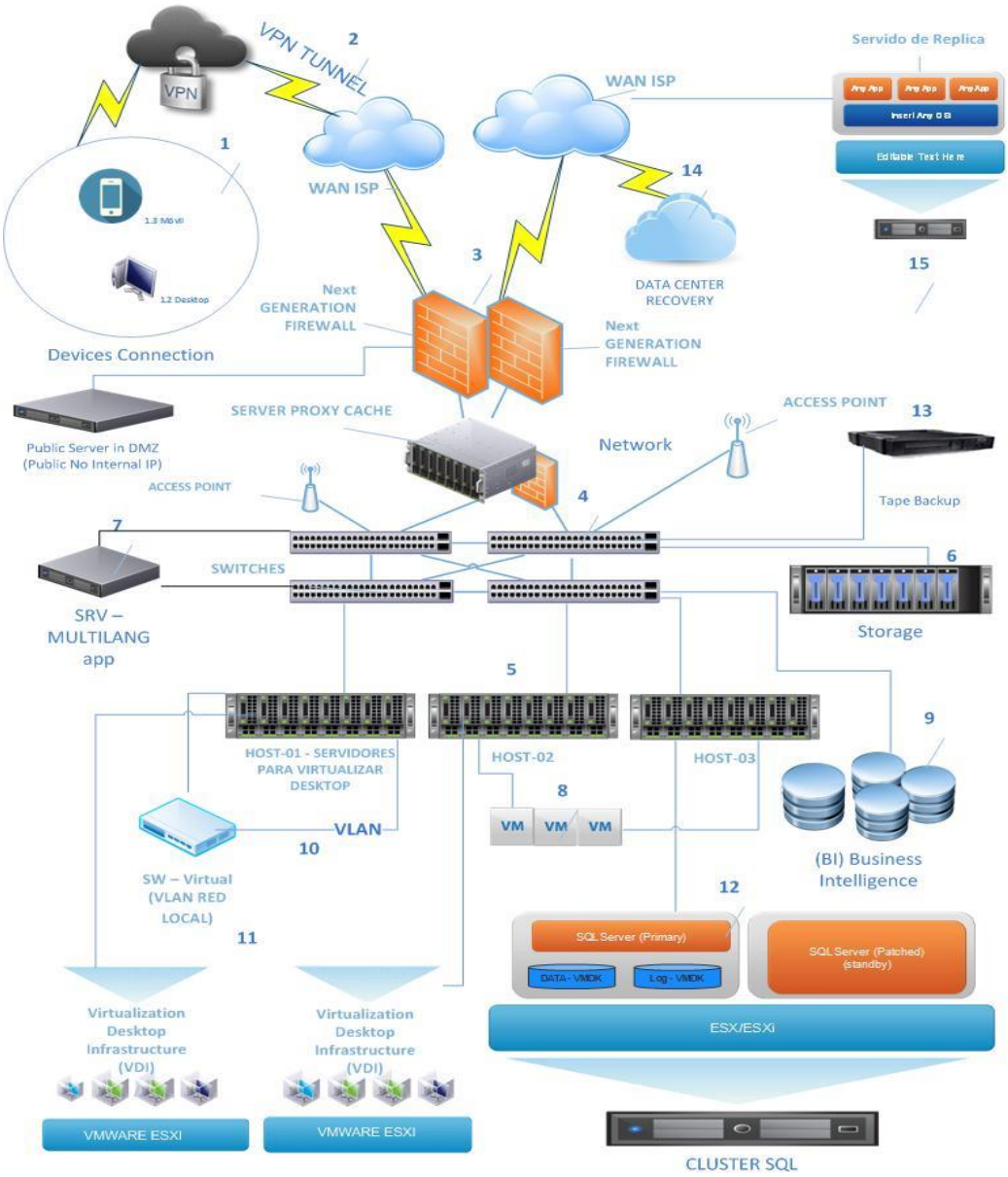


Gráfico 1; Fuente: Propia

CONCLUSION

El Centro De Capacitación tiene alrededor de 1 sucursal, la misma se apoya en los sistemas de gestión de información para realizar sus procesos implementar sus cursos en línea. Al carecer de un sistema de continuidad de negocio para los sistemas de información.

Para lograr sus objetivos de ser una empresa competitiva, decidieron embarcarse en el proyecto de implementar un traductor en línea en tiempo real para impartir sus cursos sin importar ninguna barrera, el cual les permitirá tener sus cursos un 98.9% disponible.

Este sistema permite a la organización mayor velocidad y rentabilidad en sus procesos de negocio, aprovechando las nuevas tecnologías, podrán involucrarse en nuevos proyectos de movilidad para sus canales de distribución, asociados y a clientes finales. Anteriormente, debido a las fallas del sistema, se realizaban procesos manuales y afectaba la comunicación al impartir sus cursos, creando frustraciones en los usuarios porque tenían que realizar procesos repetitivitos, los cuales, retrasaban a los usuarios para impartir sus clases. Debido a esta situación, las operaciones vitales eran afectadas.

Con la implementación de un traductor en línea y una continuidad de negocio, todos estos procesos frustrantes serán erradicados, aumentando la productividad, y situando al Centro De Capacitación en una posición competitiva frente al mercado global.

Glosario de Términos

- **Alta disponibilidad:** Según Laudon (2.004)

Alta disponibilidad se refiere a herramientas y tecnologías, incluyendo recursos de hardware de respaldo, que permiten a un sistema recuperarse rápidamente de una caída.

- **Aparamenta Eléctrica**

Es el término que se aplica al conjunto de aparatos de conexión, soporte, mando, medida y protección, así como a las conexiones, envolventes y soportes destinados a la producción, transporte, distribución y transformación de la energía eléctrica. Puede ser para instalación exterior o interior, y protegidos por envolvente metálica o no protegidos o abiertos.

- **Java Script**

Es un lenguaje ligero e interpretado, orientado a objetos con funciones de primera clase, más conocido como el lenguaje de script para páginas web, pero también usado en muchos entornos sin navegador, tales como node.js o Apache CouchDB.

- **Router**

Es un dispositivo de red, comúnmente hardware especializado, que envía paquetes de datos entre redes de computadoras.

- **Switch**

Es un dispositivo de red de computadoras que se utiliza para conectar dispositivos entre sí en una red informática mediante la realización de una forma de conmutación de paquetes.

- **Encriptar**

Encriptar es la acción de proteger información para que no pueda ser leída sin una clave. Sinónimos de Encriptar: cifrar, codificar.

- **Backup**

Se refiere a la copia y archivo de datos de la computadora de modo que puede utilizar para restaurar el original después de una eventual pérdida de datos.

Siglas y abreviaturas

AHJ: autoridad con jurisdicción

ANSI: Instituto Nacional Estadounidense de Estándares

AWG: Calibre de alambre estadounidense

CCTV: circuito cerrado de televisión

CCA: El Código Eléctrico Canadiense

CER: sala de equipos comunes

CPU: unidad central de procesamiento

CSA: Asociación Canadiense de Normas Internacionales

DSX: Señal digital de conexión cruzada

EDA: Área de distribución de equipos

EIA: Electronic Industries Alliance

EMI: Interferencia electromagnética

EL ccsme: sistema de gestión de la energía

EPO: Emergency Power Off- sistemas de corte de emergencia

FDDI: FiberDistributed Data Interface

HC: conexión cruzada horizontal

HDA: área de distribución horizontal

HVAC: calefacción, ventilación y aire acondicionado

IC: conexión cruzada intermedia

IDC: Aislamiento contacto de desplazamiento

LAN: red de área local

MC: conexión cruzada principal

MDA: área de distribución principal

NEC: Código Eléctrico Nacional

NEMA: Asociación Nacional de Fabricantes Eléctricos

NEXT: Diafonía de extremo cercano

NESC: Código Nacional de Seguridad Eléctrica

NFPA: Asociación Nacional de Protección contra Incendios

NOC: Network Operations Center – Centro operativo

OC: portadora óptica

PAC: Precision Air Conditioning / Aire Acondicionado de Presicion

PBX: PrivateBranch Exchange

PCB: Placa de circuito impreso

PDU: Unidad de distribución de energía

PVC: cloruro de polivinilo

RFI: la interferencia de radiofrecuencia

RH: Humedad relativa

SAN: Red de área de almacenamiento

SDH: jerarquía digital síncrona

SONET: Red óptica síncrona

STM: modelo de transporte síncrono

TIA: Asociación de la Industria de Telecomunicaciones

TGB: Barra de Puesta a tierra

TR: sala de telecomunicaciones

TVSS: Supresores de sobretensión transitoria

UL: Underwriters Laboratories Inc

VRLA: Válvula regulada de plomo-ácido

UPS: Fuente de alimentación ininterrumpida

UTP: Par trenzado sin blindaje

WAN: Red de área amplia

ZDA: Área de distribución de la zona A Ampere

° C: Grados Celsius

° F: Grados Fahrenheit

ft: Pies

Gb/s: Gigabit por segundo

Hz: Hertzios

kb/s: Kilobit por segundo

kHz: Kilohercios

km: kilómetro

kPa: kilopascal

kVA: kilovoltamp

kW: kilovatio

lbf: libra-fuerza

m: Metros

Mb/s: Megabit por segundo

MHz: Megahertz

Mm: Milímetro

Nm: Nanométrica

BIBLIOGRAFIA

Libros especializados:

(MoacirGadotti, Siglo XXI 2003, Perspectivas actuales de la educación)

• Fernando Andrés Arevalo Jiménez – “Como Escoger e Implementar una VPN”.

•Microsoft – “Seguridad de red privada virtual de Microsoft” (Documento Estratégico).

•Microsoft– “Windows NT Server”.

4Toro López, Francisco J. (2013) Administración de proyectos de informática. ECOE EDICIONES.

Aguilar, Luis (2012), Computación en la Nube: estrategias de cloud-computing en las empresas.

ALEGSA. (1998-2013). Definición de Virtualización a Nivel sistema Operativo.Santa Fe, Argentina: ALEGSA.

Aroche, S. F. (s.f.). Maestros del web. Recuperado el 8 de abril de 2011, de http://www.maestrosdelweb.com/editorial/cloud-computing-nueva-era-de-desarrollo/

Aroche, S. F. (s.f.). Maestros del web. Recuperado el 8 de abril de 2011, de http://www.maestrosdelweb.com/editorial/cloud-computing-nueva-era-de-desarrollo/

BIBILIOGRAFÍA

Brodkin, J. (2009). with Long History Of Virtualization Behind It, IBM Looks To The Future.IBM.

Capelli, E. (2011). Normas de la Empresa. Santo Domingo RD: EC S.A.

Carr, N. (2008). The Big Switch.

CEI-RD. (2010). Firma de un convenio de cooperación Interinstitucional con la AIRD el 07-12-10. Santo Domingo, Republica Dominicana: CEI-RD.

Cloudcomputingla. (10 de 08 de 2010). Cloudcomputingla.com/. Recuperado el 10 de 02 de 2011, de http://www.cloudcomputingla.com/

Daniel Peña Valenzuela y Juan David Bazzani Montoya (2013) Aspectos Legales de la Computación en la Nube. Universidad Externado de Colombia.

Díaz", I. D. (1966). Mensaje del Director General: Dr. Rafael Isa Isa. Santo Domingo: IDCP.

Documentos

Dordoigne, José (2011) DORDOIGNE Recursos Informáticos Redes informáticas - Nociones fundamentales. Ediciones ENI.

Enciclopedia libre de Internet.

http://blog.stikom.edu/vivine/files/2010/11/Identification-of-a-companys-suitability-for-the-adoption-of-cloud.pdf

http://es.slideshare.net/clickpsicomadrid/elearning-concepto-ventajas-e-inconvenientes-grupo-8-presentacin-colaborativa

http://es.wikipedia.org/wiki/Red_privada_virtual

http://mlearning2012.blogspot.com/p/ventajas-y-desventajas.html

http://olaretta.com/index.php?option=com_content&view=article&id=62&Itemid=94&limitstart=3

http://www.abcdatos.com/tutoriales/sistemasoperativos/windowsnt20002003.html

http://www.cisco.com

http://www.cybercursos.net

http://www.denoe.es/test/wp-content/uploads/estructura-cloud-computing.png

http://www.ehowenespanol.com/comparacion-sistemas-videoconferencia-hd-tandberg-polycom-info_307857/

http://www.foroswebgratis.com/tema-que_es_in_traductor_en_l%C3%ADnea-86650-691986.htm

http://www.microsoft.com

http://www.ovislinkcorp.es

http://www.pdf-search-engine.com/pptp-pdf.html

http://www.univalle.edu.co/~telecomunicaciones/trabajos_de_grado/informes/tg_FernandoArevalo.pdf

http://www.wikipedia.org

http://yessedik.blogspot.com/2012/07/u-learning-ventajas-y-desventajas.html

IBM. (2007). History and Heritage. Unites States: IMB.

J, R. (2005). Cibersociedad, Tecnologia de la Informacion y La Comunicacion. Consultado en octubre 8, 2010 en http://www.cibersociedad.net/archivo/articulo.php?art=218.

John, Rothon (2012), Cloud Computing Explained: Implementation Handbook for Enterprises.

Josep Lluís Cano (2007) BUSINESS INTELLIGENCE: COMPETIR CON INFORMACIÓN.

Junta de castilla y León. (2010). Observatorio Regional de la Sociedad de la Información. Recuperado el 03 de 11 de 2011, de La tecnología como servicio: http://issuu.com/orsicyl/docs/cloud_computing?mode=a_p

Key, G. H. (2010). Comunicado de Prensa de Gartner.

Marker, G. (2007). Informatica hoy, Cloud Computing: Ventajas y Riesgos de la Nube. Consultado en Octubre 2007 en http://www.informatica-hoy.com.ar/la-nube/Cloud-Computing-Ventajas-y-riesgos-de-la-Nube.php.

Microsoft, C. (2011). Virtualization 101. USA: Microsoft Corp.

Microsoft. (2011). Infrastructure Planning and Desing. USA: Microsoft Corp.

Microsystem, S. (2010). Guia para el Cloud Computing Consultado en noviembre 10, 2010.

NIST. (2009). Disponibilidad de tecnologias de infrormacion t comunicacion en los hogares, consultado en Octubre 23, 2010.Estados Unidos: INEGI.

Página Web oficial de Cisco Systems. Compañía mundial líder en la fabricación de equipos para Internetworking. Dentro de sus productos cuenta con equipos concentradores de túneles L2F, L2TP yIPSec. Desarrolla sistemas operativos (IOS) para sus enrutadores y switches que capacitan a los mismos para crear y terminar túneles.

Página Web oficial de Microsoft Corporation. Fuente de información sobre los protocolos

Páginas Web

PPTP y L2TP sobre computadores instalados con sistemas operativos Windows NT, Windows 2000 Server, Windows XP y Windows 2003 Server.

Profesor loayza, http://www.galeon.com/histedudistan/

Recuperado: revisado el 27 may 2014, http://es.wikipedia.org/wiki/Educaci%C3%B3n_en_l%C3%ADnea

Rolf A. de By, R. A. (2000). Principles of Geographic Information Systems. Netherlands: International Institute for Aerospace Survey and Earth Sciences.

Salazar, C. (2008). Cibermundos, La TIC como herramienta a la gestión empresarial. Consultado en septiembre 23 en http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html.

Salesforce. (2008). Multitenancy. San Francisco.

Schroeder. (1992). Administracion de Operaciones.Mc Graw Hill.

SearchDataCenter.com. (2012-2014). Virtualizacion. TechTarget, S.A.

Sitio Oficial de la empresa Ovislink fabricante de dispositivos de red.

Sitio Web donde se pueden descargar documentos referentes a tecnologías de redes y otras.

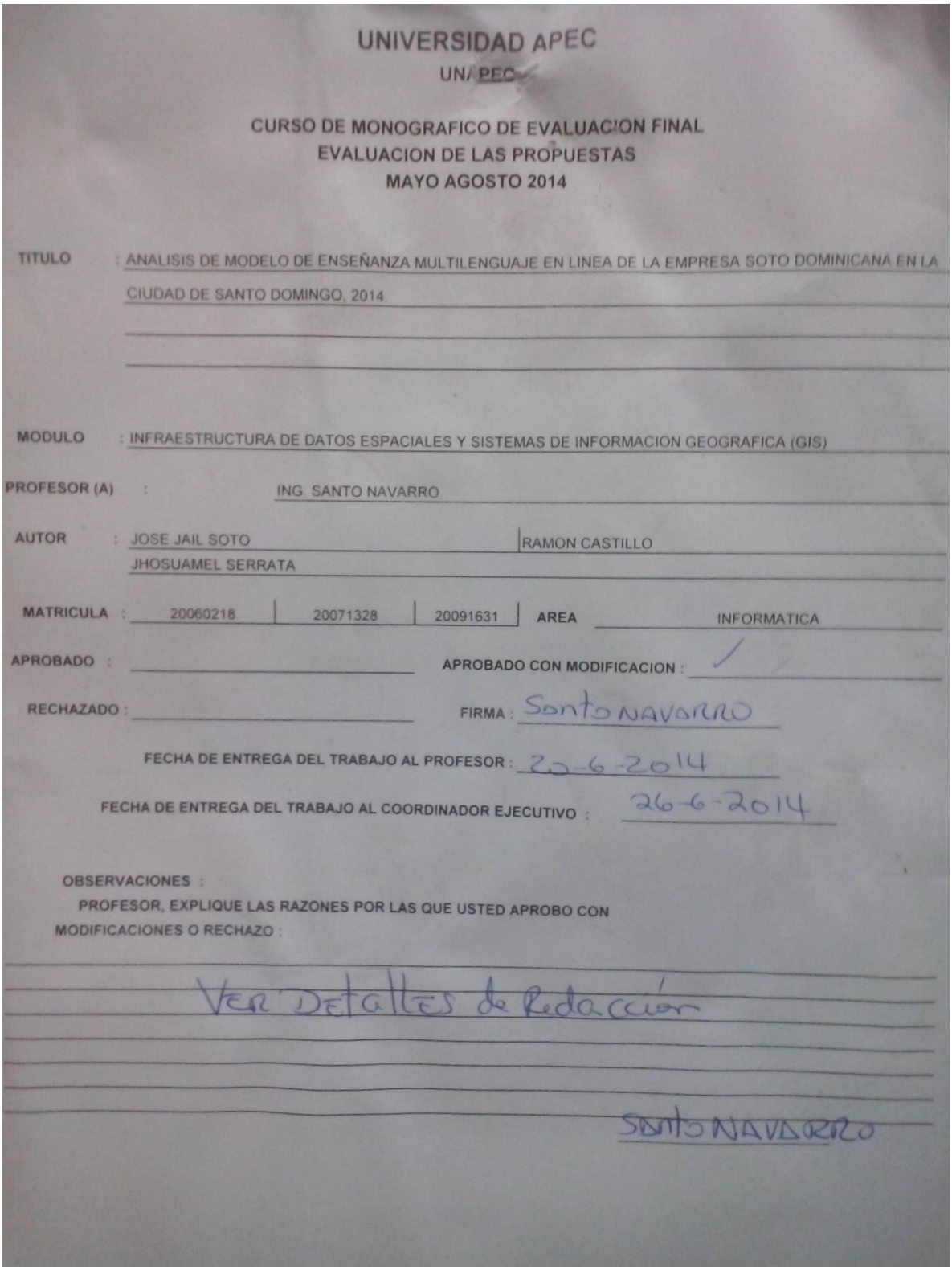
Sullivan, F. &. (2009). Primer informe regional sobre el modelo Cloud.

Torres Viñals, Jordi (2011) Empresas en la nube: Ventajas y retos del Cloud Computing. Libros de Cabecera.

Turban, E., King, D., Lee, J., & Viehland, D. (2013). Building E-Commerce Applications and Infrastructure.Prentice Hall, pp. 27.

A N E X OS

Anexo #1: Anteproyecto



UNIVERSIDAD APEC

UNAPEC

CURSO DE MONOGRAFICO DE EVALUACION FINAL
EVALUACION DE LAS PROPUESTAS
MAYO AGOSTO 2014

TITULO : ANALISIS DE MODELO DE ENSEÑANZA MULTILENGUAJE EN LINEA DE LA EMPRESA SOTO DOMINICANA EN LA CIUDAD DE SANTO DOMINGO, 2014.

MODULO : INFRAESTRUCTURA DE DATOS ESPACIALES Y SISTEMAS DE INFORMACION GEOGRAFICA (GIS)

PROFESOR (A) : ING. SANTO NAVARRO

AUTOR : JOSE JAIL SOTO | RAMON CASTILLO
JHOSUAMEL SERRATA

MATRICULA : 20060218 | 20071328 | 20091631 AREA INFORMATICA

APROBADO : _____ APROBADO CON MODIFICACION : ✓

RECHAZADO : _____ FIRMA : Santo NAVARRO

FECHA DE ENTREGA DEL TRABAJO AL PROFESOR : 20-6-2014

FECHA DE ENTREGA DEL TRABAJO AL COORDINADOR EJECUTIVO : 26-6-2014

OBSERVACIONES :
PROFESOR, EXPLIQUE LAS RAZONES POR LAS QUE USTED APROBO CON MODIFICACIONES O RECHAZO :

Ver Detalles de Redacción

SANTO NAVARRO

Decanato de Ingeniería e Informática
Escuela de Informática

"Análisis de modelo de enseñanza multilenguaje en línea de la empresa SOTO DOMINICANA en la Ciudad de Santo Domingo, 2014."

Sustentantes:

José Jail Soto	**2006-0218**
Ramón Castillo	**2007-1328**
Jhosuamel Serrata	**2009-1631**

Asesor:
Ing. Santo Rafael Navarro

Anteproyecto de la Monografía para Optar por el Título de:
Ingeniero en Sistemas de Computación

Distrito Nacional, República Dominicana
2014

“Análisis de modelo de enseñanza multilenguaje en línea de la empresa SOTO DOMINICANA en la ciudad de santo domingo, 2014.”

INDICE

SELECCIÓN DEL TÍTULO Y DEFINICIÓN DEL TEMA

Análisis para la implementación de un modelo de Continuidad de Negocios y Recuperación de Desastres en la empresa Soto Dominicana", Santo Domingo R.D. 2014.

1.1 DEFINICIÓN DEL TEMA

En este trabajo de grado se desarrolla la implementación de un modelo de continuidad de negocios y recuperación de desastres. Esta estructura apoyará a la empresa a tener un sistema de alta disponibilidad en su operación tecnológica y recuperarse en un tiempo reducido, ante cualquier eventualidad.

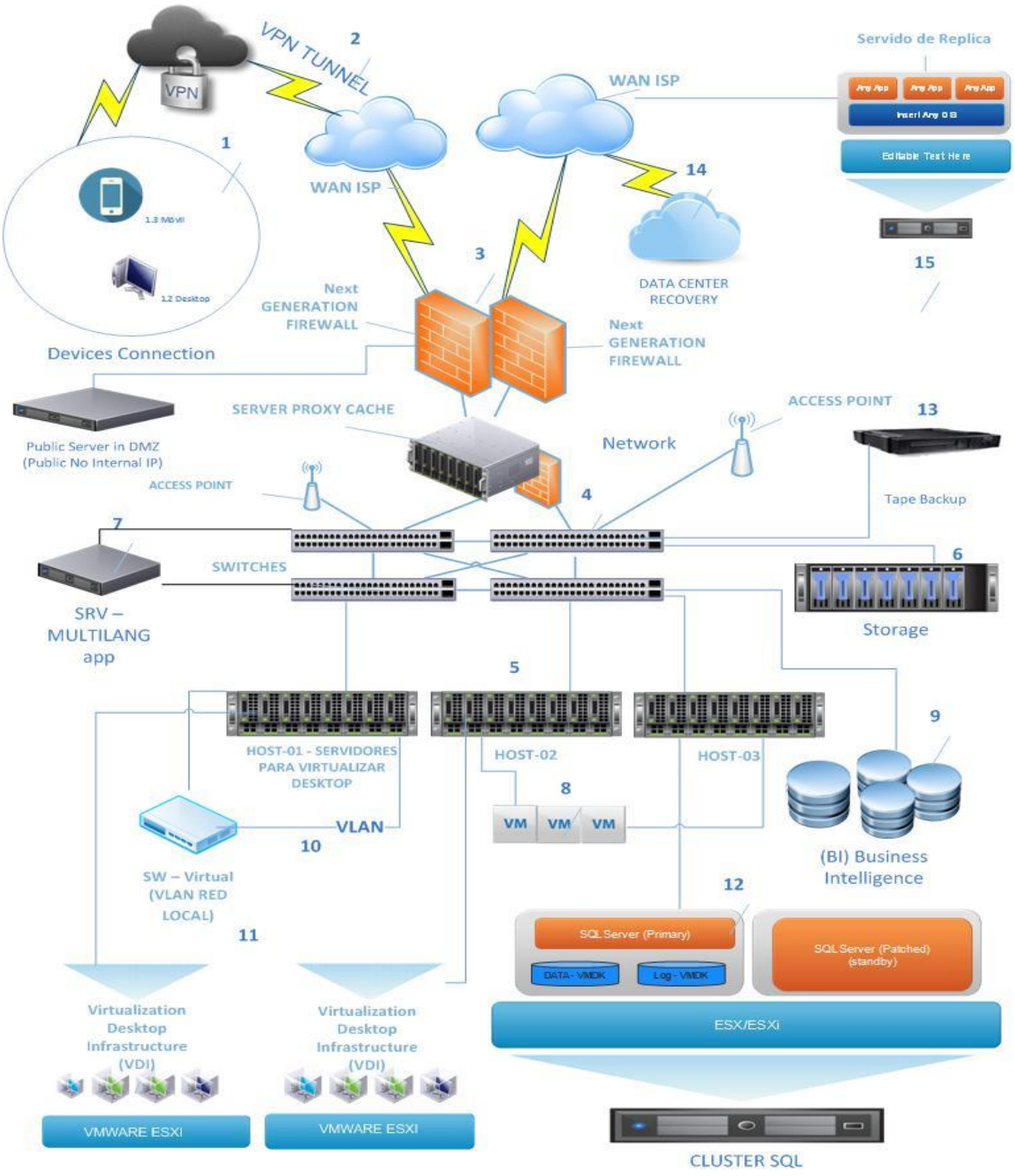


Gráfico 1; Fuente: Propia

1.2 ORGANIZACIÓN DE CONTENIDOS

Esta investigación estará dividida en capítulos, de la manera siguiente:

CAPITULO 1 - Define la Empresa y a que está dedicada. Explica la misión de la misma en el mercado y a quién va dirigida. Explica también la visión de la empresa, hacia donde quiere llegar y conseguir la total satisfacción de los clientes. Además de los objetivos.

CAPÍTULO 2 -Se desarrolla una investigación de los tipos de enlaces privados, su historia y evolución al pasar de los años.

CAPÍTULO3-Se inicia con la historia de la virtualización, un nuevo concepto de virtualización de escritorio, cual es la demanda que existe hoy día de este nuevo concepto. Se dan la Estimaciones, estadísticas y las ventajas que posee al ser implementada en compañías.

CAPÍTULO4-- Este capítulo tratará sobre la disponibilidad en los centro de datos, Según lo establecido por el estándar TIA-942, de la Asociación para la Industria de las Telecomunicaciones (TIA, por sus siglas en inglés).

CAPITULO5-En esta parte vamos a mostrar ampliamente la evaluación de las normas, recomendaciones y estándares internacionales actuales, para garantizar

el diseño de infraestructura tecnológica que permita alta disponibilidad en la gestión y administración de datos.

CAPÍTULO 6-Una de las parte clave de un centro de datos y una plataforma de educación a distancia es la seguridad, en este capítulo explicaremos los diferentes tipos de seguridad que requiera esta tecnología y así mismo que tipo de seguridad esta emplea.

CAPÍTULO 7 - Se realizará un estudio sobre los resultados y beneficios económicos de esta implementación.

CAPITULO 8- Se inicia con la historia de educación en línea, cuales son los desafíos y fronteras también sus características ventajas y desventajas.

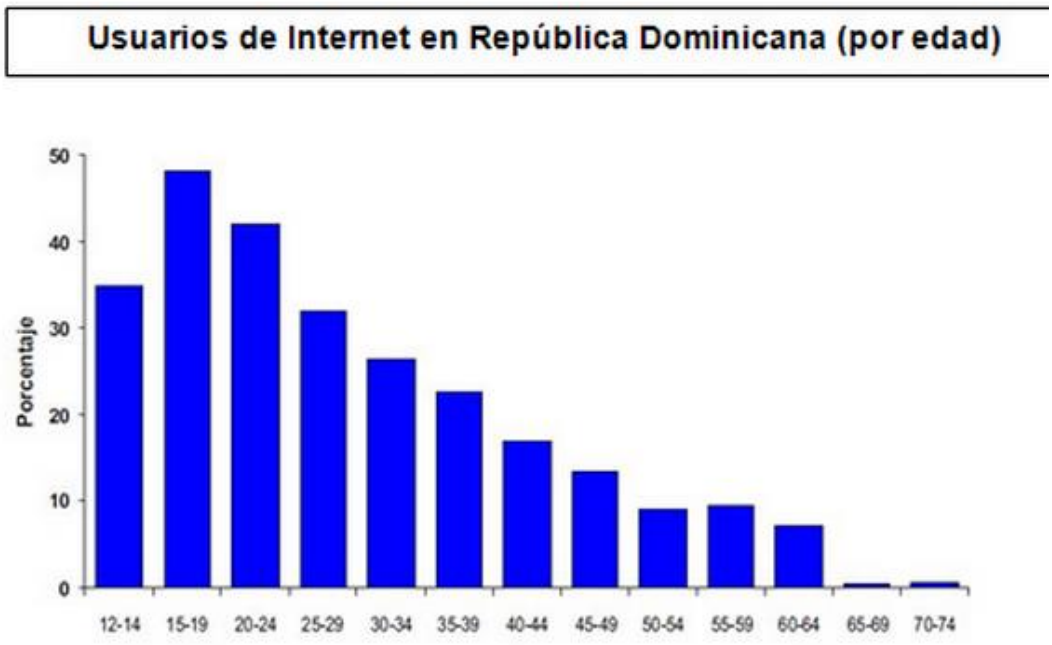
CAPÍTULO 9- Se realizará las conclusiones de la investigación.

2. PLANTEAMIENTO DEL PROBLEMA

La empresa SOTO DOMINICANA, tiene por mandato de ley la responsabilidad de impulsar el desarrollo de los Recursos Humanos que laboran en el área financiera del Estado. Para cumplir con su misión la empresa SOTO DOMINICANA ha desarrollado diversas capacitaciones en materia fiscal a nivel nacional, sin embargo, por razones presupuestaria no ha podido extender su presencia en todo el país.

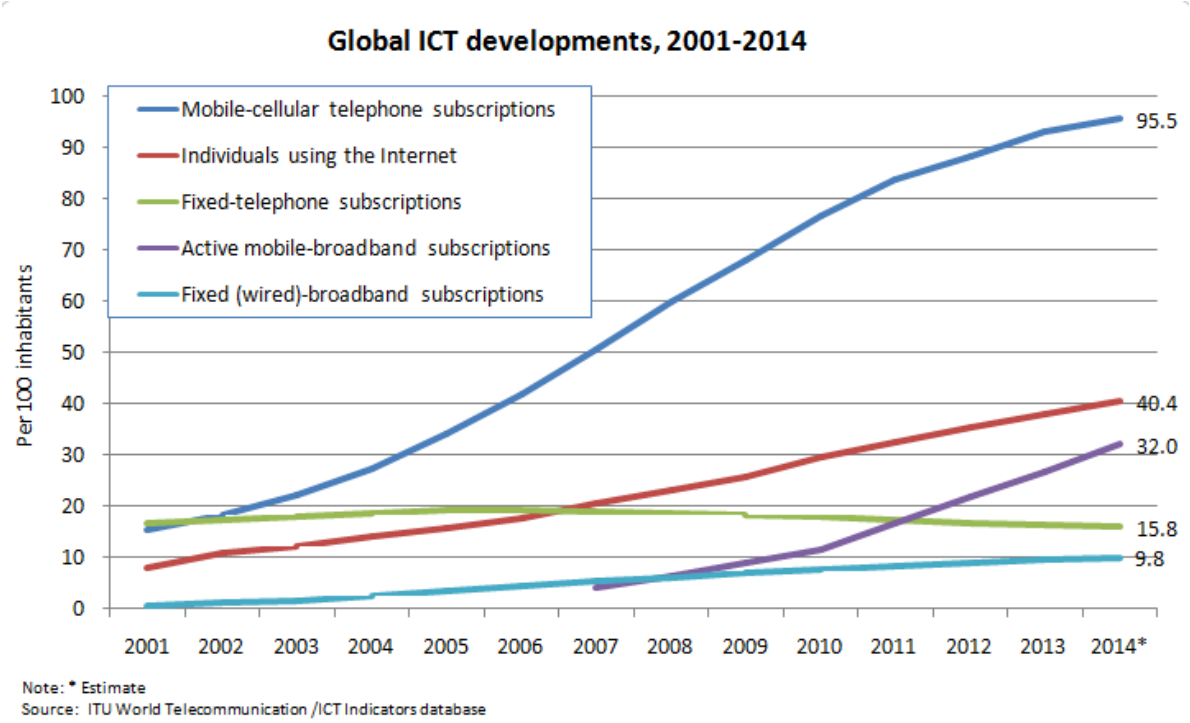
Un estudio demuestra que todo el que estudió en una **universidad en la República Dominicana** entre el 2004 y 2005, aproximadamente, conoció y vivió de mala manera el proceso tortuoso de ir en horas de la madrugada para obtener el registro de las asignaturas a estudiar en un determinado cuatrimestre, pues los procesos de selección de materias, aunque se utilizaban computadoras en muchos casos, había que hacerlo de manera presencial. Sin embargo, en las principales **universidades dominicanas,** los estudiantes universitarios ya se inscriben a través de internet, revisan sus notas y también reciben las actualizaciones y correos electrónicos para enviar las informaciones por esta vía y que no tengan que estar haciendo largas filas para procesos cotidianos.

Otro estudio realizado en nuestro país en el año 2007 demuestran que el listado nominal de votantes de 18 y 29 años que utilizan internet es de 1, 154,256 usuarios.



Fuente: Oficina Nacional de Estadísticas. Encuesta Nacional de Hogares de Propósitos Múltiples (ENHOGAR)2007

En el mismo orden se muestran estadísticas sobre disponibilidad y uso de tecnologías de Información y Comunicación. En las Américas, casi dos de cada tres personas utilizará Internet a finales de 2014, lo que representa la segunda mayor tasa de penetración después de Europa. En Europa, la penetración de Internet alcanzará el 75 por ciento (es decir, tres de cada cuatro personas) a finales de 2014 y será la más alta a nivel mundial. Un tercio de la población de Asia y el Pacífico estará en línea a finales de 2014 y cerca del 45 por ciento de los usuarios de Internet totales procederán de esta región.



Fuentes: ITU Statistics (http://www.itu.int/ict/statistics) Global ICT developments, 2001-2014

A raíz de lo anterior, una de las grandes problemáticas es la convergencia de los dispositivos de los clientes para tener acceso a la plataforma en línea, ya que hasta ahora solo está enfocado para trabajar con PC, dejando un lavo la revolución de los dispositivos móvil. Otro aspecto fundamental es el mal diseño a nivel de infraestructura de las bases de datos. No obstante la seguridad juega un papel importante y en el levantamiento información que obtuvimos de la entrevista al departamento de TI de la empresa Soto Dominicana, nos dimos cuenta que no poseen una dmz (Zona Desmilitarizada) para publicar los servicios web teniendo altas vulnerabilidades a nivel de seguridad.

Una limitante de la capacitación en línea es la barrera del idioma, que impide que las formaciones ofrecidas por la empresa Soto Dominicana puedan expandirse sin ninguna frontera, tenemos un caso de estudiantes que pertenecen Haití donde manejan el idioma ingles y francés más que el español, siendo esto una debilidad del sistema de capacitación actual que no posee traducciones en tiempo real para satisfacer la demanda de estos sectores.

Por otro lado, los sistemas de información y equipos informáticos tienen sistema operativo descontinuados por los fabricantes como el caso de windowsxp, altos problemas de seguridad por una mala planificación en la infraestructura tecnológica, descentralización de los procesos internos entre departamentos que tienen flujos de trabajo compartidos.

OBJETIVOS DE LA INVESTIGACIÓN

3.1 OBJETIVO GENERAL

Implementar un sistema basado en un nuevo método de enseñanza en línea, que incorpore un traductor en tiempo real para permitir a los clientes tomar curso a distancias sin importar el idioma.

Implementar un método de enseñanza mediante un sistema multilenguaje en línea que Permita al usuario tomar entrenamientos y capacitaciones sin importar las barreras que se presenten a nivel de idiomas

3.2 OBJETIVOS ESPECÍFICOS

- Implementar un nuevo sistema de traducción en tiempo real para la capacitación en línea.

  - Describir la arquitectura para el diseño del ambiente de virtualización de servidores y escritorios.
  - Centralizar todo los sistemas virtualizados y datos de la empresa.
  - Segmentar el tráfico en VLANs (Virtual LAN Área Network) para dividir el acceso de la red corporativa y la red de estudiante.
  - Aprovechar los recursos de hardware para minimizar el impacto del consumo eléctrico.
  - Utilizar la inteligencia de negocio (BI) para la administración y análisis de los datos existente de la empresa.
  - Ofrecer nuevas alternativas tecnológicas con virtualización de escritorio para remodelar los laboratorios con tecnología de punta.
  - Ahorrar espacio y energía eléctrica en el data center, centralizar la administración de los servidores, contar con una imagen del sistema que pueda ser recuperada ante cualquier cambio que se haga en los servidores.
  - Mantener la encriptación e integridad en la comunicación cliente-servidor
  - Realizar replicación de los servicios críticos de la empresa para continuidad del negocio en caso de falla.

- Realizar copias de seguridad tantos en cintas como en la nube para salvaguardar la información fuera de la empresa garantizando que en caso de cualquier desastre en la empresa la data este segura.
- Mantener las bases de datos de la plataforma virtual siempre en línea aplicando modelos de alta disponibilidad y tolerancia a fallos.
- Brindar al cliente el acceso a los servicios y capacitaciones de la empresa tomando en cuenta la revolución de los dispositivos móviles.

4. Justificación de la investigación

4.1 Justificación teórica.

¿Alguna vez te has preguntado cuantas capacitaciones en línea no pudiste tomar por que no estaban en tu idioma?. Nuestra propuesta se basa en esta parte como romper la barrera del idioma en la formación a distancia. Tomando como base la aplicación de la teoría, análisis y diseño de nuevas tecnologías como Virtualización, Cloud Computing y plan de continuidad de negocio.

4.2 Justificación metodológica.

Para llevar a cabo el desempeño de los objetivos de esta investigación se emplearan diversas técnicas y herramientas que permitan concretizar el análisis de un sistema basado en un nuevo método de enseñanza en línea, que incorpore un traductor en tiempo real y la infraestructura tecnológica que la soporte.

4.3 Justificación práctica.

La utilización de tecnología en nuestros tiempos se ha convertido en un recurso indispensable para las empresas y el diario vivir de las personas. El objetivo principal de nuestro proyecto A raíz de lo anterior, realizar un diseño de infraestructura acorde a las exigencias tecnológicas que permita a la institución crecer en el tiempo, sin tener que invertir todos los años en actualización de su infraestructura tecnológica, esto permite que proyectemos la institución a 10 años y ahorremos en el consumo de energía eléctrica, compra de PC y servidores, contratos de consultorías y adquisición de software, igualmente l nuevos UPS centrales para futuros laboratorios.

Los Sistemas de información y equipos informáticos para la Red Administrativas tienen problema de Actualización de sistema operativo, Seguridad lógica y no tienen una intranet que ayude a realizar procesos internos de forma más centralizadas y con controles en las informaciones que se manejan.

.

Solución a la adquisición de varios servidores. La cual implica una alta inversión económica por el coste de las instalaciones físicas, utilización de electricidad, así como la formación que debe recibir el personal encargado del mantenimiento de los mismos, siendo estos gastos sólo una parte pequeña del coste total. Y es por esta razón que la Virtualización y optimización de recursos es tan importante. La Virtualización esconde las características físicas de un ordenador a los usuarios, aplicaciones o ambos.

Disponibilidad, las características prosperadas que poseen los sistemas de Virtualización nos proporcionan la posibilidad de concordar opciones de alta disponibilidad para recuperación de desastres. Podemos configurar nuestros sistemas para que en el caso de que una máquina falle, automáticamente se levante en otro host en el mismo estado, sin que el usuario se dé cuenta del inconveniente.

Facilidad de backup, en un entorno virtualizado, con las herramientas necesarias de backup, se puede configurar tanto los trabajos de backup como de replicación de forma que la recuperación de desastres sea cuestión de minutos.

Flexibilidad, podemos crear tantas máquinas virtuales como el hardware de nuestro servidor nos permita, y con las exclusivas características que necesitemos en cuanto a almacenamiento, CPU, memoria RAM, etc. También tendremos la posibilidad de modificar dichos recursos en cuanto nos sea necesario de una forma muy fácil y eficaz.

Desubicación, si tenemos diversos servidores Host (los servidores físicos que albergan las máquina virtuales), podemos mover las máquinas virtuales entre los otros Host sin que el usuario se percate de ello, con las máquinas en caliente.

Independencia del hardware, nuestras máquinas virtuales sólo necesitan un ambiente en donde ejecutarse, el cual es independiente de la marca y el hardware de nuestro servidor físico.

Menor consumo energético, al tener menos equipos derrochamos menos energía.

5. Métodos y Técnicas de Investigación

5. TIPOS DE INVESTIGACIÓN

Para el desarrollo del trabajo de grado se utilizarán los siguientes tipos de investigación:

a) **DESCRIPTIVA**: Las investigaciones de tipo descriptiva, llamadas también investigaciones diagnósticas o investigación estadística, Consiste en la caracterización de un hecho o situación, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento es decir indicando sus rasgos más peculiares o diferenciadores. Este método de investigación será utilizado en el desarrollo del trabajo para identificar los factores que involucra la implementación de continuidad de negocios basado en la nube también se emplearan técnicas específicas en la recolección de información u datos como son las entrevistas, observación y cuestionario, que ayudaran a facilitar datos para la investigación.

b) **EXPLICATIVA**: es aquella que tiene relación causal, no sólo persigue describir o acercarse a un problema, sino que intenta encontrar las causas del mismo. Este tipo de investigación será utilizado en todo el proceso para definir cada problema que pueda sobrevenir así detallando los pasos para la resolución de forma clara y precisa, mediante un análisis, síntesis e interpretación de la información recolectada.

c) **DOCUMENTAL**: Es una investigación que se realiza en forma ordenada y con objetivos precisos, con la finalidad de ser base para la construcción de conocimientos de investigación científica y se caracteriza por la utilización de documentos: dónde recolecta, selecciona y presentan resultados coherentes. Este método será utilizado en el trabajo de investigación, porque mediante este recolectamos una serie de información de la empresa SOTO DOMINICANA, el cual nos brinda una serie de factores que explica la implementación de continuidad de negocio basado en la restructuración del área de tecnología.

d) **ENTREVISTAS**: Esta técnica tiene numerosas ventajas para el trabajo educativo, social, cultural y científico. Este procedimiento es altamente valioso y útil para recabar informaciones actualizadas que probablemente no están disponibles en las publicaciones escritas. Este método será utilizado para la recolección o extracción de la información que se usara para el desarrollo del trabajo de investigación. estas entrevistas serán realizadas al personal

considerado necesario, esto incluye directores, supervisores, técnicos involucrados y personal administrativo.

6. MARCOS DE REFERENCIA

6.1 MARCO TEÓRICO

Vivimos un momento de revolución tecnológica, es decir, una aceleración de la transformación de las modalidades de organización del trabajo y de los medios de producción y una creciente progresión de la productividad global del trabajo social.**(amin, 2009)**

Cloud computing o computación en la nube es un nuevo paradigma que consiste en ofrecer servicios a través de internet. En los últimos años, este tipo de servicios se ha generalizado entre los principales fabricantes para formar parte de las opciones disponibles de su portafolio de servicios, e incluso en algunos casos para ser la forma predominante de los mismos.**(diaz, 2012)**

Un plan de continuidad de negocio es conveniente para todas las entidades, si bien en algunas, porque den servicio a un gran número de empresas o usuarios, por el sector de actividad o por otras razones, es absolutamente imprescindible, para evitar que en el caso de un problema grave la entidad haya terminado su actividad para siempre o sufrido un daño importante. Business continuity management es reconocido como una buena práctica profesional y es parte integral del buen gobierno de las organizaciones.**(Gaspar, 2004)**

La seguridad de la información en sí es de importancia creciente, en parte porque la propia información puede ser vial, y hoy día se trata, transmite y almacena en sistemas de información soportados por tecnología, y también es importante por los sucesos generales relacionados con la (in)seguridad en general: por todo ello las entidades han de contar con medios que puedan garantizar la continuidad de los sistemas y del negocio/servicio **(Gaspar, 2004).**

ISO 22301:

ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio. Esta ha sido creada en respuesta a la fuerte demanda internacional que obtuvo la norma británica original, BS 25999-2 y otras normas. Si usted cumple con los requisitos para obtener la certificación, su organización será reconocida a nivel global. ISO 22301 identifica los fundamentos de un sistema de gestión de continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio. Proporciona una base de entendimiento, desarrollo e implantación de continuidad de negocio dentro de su organización y le da la confianza de negocio a negocio y de negocio a cliente. Se usa para asegurar a las partes interesadas clave que su empresa está totalmente preparada y que puede cumplir con los requisitos internos, regulatorios y del cliente.

recuperado de :http://www.bsigroup.es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Continuidad-de-Negocio-BS25999/

6.2 MARCO CONCEPTUAL

Cloud Computing o computación en la nube: Se utiliza para definir a un sistema informático basado en internet que permite gestionar archivos y aplicaciones sin necesidad de instalarlas en la computadora. (Caccuri)

Platform as a Service: Plataforma como servicio (PaaS) es un modelo de computación en la nube a través del cual se entrega una plataforma informática para usuarios a través del Web. PaaS es de uso frecuente para el desarrollo, despliegue y hosting de aplicaciones. Ofertas de PaaS son Microsoft Azure, Force.com y Google App Engine.

Recuperado de :http://searchdatacenter.techtarget.com/es/cronica/Computacion-de-almacenamiento-en-las-nubes-desde-A-hasta-Z

Cloud Backup: La copia de seguridad en nube es el concepto de enviar copias de sus datos a un servidor fuera de las instalaciones para el almacenamiento de copia de seguridad. Las empresas son poco propensas a adoptar cloudbackup de los datos pertinentes, como los problemas de seguridad y los temores sobre el almacenamiento de información crítica en la nube persisten. Varios servicios de copia de seguridad de nubes son prominentes Amazon S3, Asigra y Mozy de EMC.

Recuperado de:http://searchdatacenter.techtarget.com/es/cronica/Computacion-de-almacenamiento-en-las-nubes-desde-A-hasta-Z

VLANs: Es una división virtual de una red local en varias más pequeñas, pero sin salirse del entorno físico dela LAN. **(Lopez)**

LAN: Es un grupo de ordenadores conectados mediante un medio de transmisión compartido, normalmente un cable. Una LAN está limitada a un área local por las propiedades eléctricas de los cables utilizados para construirla y por el número relativamente pequeño de ordenadores que pueden compartir un único medio de transmisión.**(armiña, 2004)**

Firewall: Es un guardián que vigila los puertos de entrada y salida de su ordenador., este solicita una autorización cuando usted efectúa una operación corriente.**(CAPRANI, 2006)**

Host: Computadora que mediante la utilización de los protocolos TCP/ IP permite a los usuarios comunicarse con otros sistemas anfitriones de una red.**(Rendon)**

VPN: Permiten a las organizaciones tener conexiones enrutadas entre distintas oficinas o con otras organizaciones a través de una red pública a la vez que se mantiene la seguridad de las comunicaciones.**(Pérez, 2009)**

Virtualización: Es la manera en que un usuario utiliza un programa especial para instalar un nuevo sistema operativo dentro de ese programa, es como tener dos computadoras en una**(Valentín)**

SQLserver: Es una de las mayores inversiones de microfost y ha sido una pieza estrategica junto a los sitemas operativos. Es una plataforma para base de datos que se utiliza en el procesamiento transaccional en linea a gran escala, en las bodegas de datos y las aplicaciones de comercio electronico asi como tambien es una plataforma de inteligencia de negocios para soluciones de integracion, analisis y creacion de informes de datos. **(rivera)**

Clúster: Permiten asociar maquinas y servidores para que actúen de forma conjunta como una única instancia. La creación de un clúster va a permitir el balanceo de carga y la recuperación frente a fallos**. (editorial, 2004)**

Business continuity management:

Es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporciona el marco adecuado para construir y reforzar la capacidad de dar una respuesta efectiva que salvaguarde los intereses, la imagen y el valor de las actividades realizadas por la misma. Gaspar J. (2004).

6.3 MARCO ESPACIAL

La investigación será realizada en base a datos e informaciones obtenidas de la Empresa SOTO DOMINICANA, Gazcue, D.N. Santo Domingo.

6.4Marco Temporal

La investigación será realizada en un periodo aproximado de 4 meses en el periodo Mayo-Agosto 2014.

7. Métodos, procedimientos y técnicas utilizadas en la investigación.

7.1 Métodos

Las metodologías que se utilizarán para este trabajo de grado son:

A) Método Observación: Utilizaremos este método para llevar a cabo observaciones y diagnosticar el estado actual de la organización planteado anteriormente, además de las problemáticas que los aquejan, para de este modo lograr la implementación de los procesos virtuales en el modelo de continuidad de negocio basada en la nube en la empresa SOTO DOMINICANA.

B) Método Inductivo: Utilizaremos este método para llevar a cabo un registro, análisis y clasificación de los hechos observados.

c) Método Deductivo: Utilizaremos este método para observar lo anteriormente planteado, concluir y señalar la pluralidad problema planteado.

d) Método de Análisis y Síntesis: Se utilizara este método para identificar las partes que componen el problema planteado y de esta manera establecer la relación de causa y efecto entre los elementos del mismo.

7.2PROCEDIMIENTO

Luego de obtener las informaciones recolectadas mediante los métodos antes mencionados se realizarán las siguientes actividades:

- Definición conceptos generales, una base teórica para exponer los fundamentos y características de los temas. Esa base estará apoyada en libros técnicos y sitios web debidamente identificados.
- Análisis de todos los aspectos importantes en el flujo de información que operan por separado pero a la vez se relacionan como sistema.
- Análisis de la Infraestructura del sistema para la empresa SOTO DOMINICANA.
- Análisis del sistema o procesos contingencia actual de la para la empresa SOTO DOMINICANA.

- Desarrollar un nuevo método de modelo de enseñanza en con traductor en tiempo real.
- Desarrollar un modelo de Continuidad de Negocio y Recuperación de Desastres Basada en la Nube para la empresa SOTO DOMINICANA.

Finalmente se presentará un informe final del proyecto con las conclusiones y los resultados.

7.3 TÉCNICA

Las técnicas utilizadas para la recolección de información de este trabajo de grado serán:

La entrevista: Se utilizará esta técnica para la recolección o extracción de la información que será utilizada para el desarrollo del trabajo de investigación. Dichas entrevistas serán realizadas a todo el personal considerado clave o necesario, esto incluye directores, supervisores, técnicos involucrados y personal administrativo.

Caso de estudios: son herramientas que consisten en ejemplos reales en los que se presenta una historia positiva sobre los beneficios que un producto o servicio le han significado a determinados usuarios.

Artículos periodísticos: Es un texto que expresa la opinión que redacta el mismo público al cual es dirigido, con la finalidad de encontrar en el lector la formación de la opinión y el conocimiento del tema.

Documentos de investigación: Dan a conocer de un modo claro y preciso en lo posible, determinados conocimientos.

Informes técnicos: Método de análisis o para reportar aspectos técnicos del tema o problema específico y generar posibles soluciones.

8.0 TABLA DE CONTENIDO

- **DEDICATORIAS**
- **AGRADECIMIENTOS**
- **INDICE**
- **RESUMEN**
- **INTRODUCCION**

Capitulo 1. Información organizacional

1.1. ¿Quiénes somos?

1.2. Misión

1.3. Visión

1.4. Objetivos

1.5. Valores

1.6. Estructura organizacional

Capitulo 2. Conceptos Generales

2.1. Computación en la nube

2.2. Interoperabilidad datos y Aplicaciones

2.3. Portabilidad

2.4. Gobernabilidad y gestión

2.5. Medición y Monitoreo

2.6. SLA (traducir)

2.7. Virtualización de aplicaciones

2.8. Continuidad de negocios Tecnología de la Información (Siglas en Ingles IT)

2.9. Plan de recuperación de desastres (Disaster Recovery Plan, DRP)

2.10. Plan de continuidad de negocios (Business Continuity Planing, BCP)

2.11. Análisis de impacto del negocio (Business Impact Analysis, BIA)

2.12. Seguridad.

2.13. Riesgo y Cumplimiento

Capitulo 3. Sistema de continuidad de negocio

3.1. Sistema de continuidad basado en servicio

3.2. Sistema de continuidad basado en aplicaciones

3.3. Sistema de continuidad basado en la recuperación de desastres

3.4. Sistema de continuidad de respaldo basado en la nube

3.5. Sistema de continuidad de respaldo basado en almacenaje

3.6. Sistema de continuidad en servicios de seguridad

Capitulo 4. Infraestructura Tecnológica de la empresa

4.1. Centro de datos

4.2. Infraestructura virtual

4.3. Infraestructura de servidores

4.4. Infraestructura de comunicaciones

4.5. Infraestructura de red internacional

4.6. Estructura energética

Capitulo 5. Sistema de continuidad basado en la nube

5.1. Sistema de continuidad de negocio hibrido

5.2. Replicación

5.3. Alta disponibilidad

5.4. Software como servicio

5.5. Seguridad como servicio

RESULTADOS

CONCLUSION

BIBLIOGRAFIA

ANEXOS

Fuentes de Documentación

10.1 Primarias

Entrevistas en la empresa SOTO DOMINICANA para recolectar informaciones de sus sistemas.

10.2 Secundarias

Libros especializados:

ALEGSA. (1998-2013). *Definición de Virtualización a Nivel sistema Operativo.*Santa Fe, Argentina: ALEGSA.

Brodkin, J. (2009). *with Long History Of Virtualization Behind It, IBM Looks To The Future.*IBM.

Capelli, E. (2011). *Normas de la Empresa.* Santo Domingo RD: EC S.A.

Carr, N. (2008). *The Big Switch.*

CEI-RD. (2010). *Firma de un convenio de cooperación Interinstitucional con la AIRD el 07-12-10.* Santo Domingo, Republica Dominicana: CEI-RD.

Díaz", I. D. (1966). *Mensaje del Director General: Dr. Rafael Isa Isa.*Santo Domingo: IDCP.

IBM. (2007). *History and Heritage.* Unites States: IMB.

J, R. (2005). *Cibersociedad, Tecnologia de la Informacion y La Comunicacion.* Consultado en octubre 8, 2010 en http://www.cibersociedad.net/archivo/articulo.php?art=218.

Key, G. H. (2010). *Comunicado de Prensa de Gartner.*

Marker, G. (2007). *Informatica hoy, Cloud Computing: Ventajas y Riesgos de la Nube.* Consultado en Octubre 2007 en http://www.informatica-hoy.com.ar/la-nube/Cloud-Computing-Ventajas-y-riesgos-de-la-Nube.php.

Microsoft. (2011). *Infrastructure Planning and Desing.* USA: Microsoft Corp.

Microsoft, C. (2011). *Virtualization 101.* USA: Microsoft Corp.

Microsystem, S. (2010). *Guia para el Cloud Computing Consultado en noviembre 10, 2010.*

NIST. (2009). *Disponibilidad de tecnologias de infrormacion t comunicacion en los hogares, consultado en Octubre 23, 2010.*Estados Unidos: INEGI.

Rolf A. de By, R. A. (2000). *Principles of Geographic Information Systems.* Netherlands: International Institute for Aerospace Survey and Earth Sciences.

Salazar, C. (2008). *Cibermundos, La TIC como herramienta a la gestion empresarial.* Consultado en septiembre 23 en http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html.

Salesforce. (2008). *Multitenancy.* San Francisco.

Schroeder. (1992). *Administracion de Operaciones.*Mc Graw Hill.

SearchDataCenter.com. (2012-2014). *Virtualizacion.* TechTarget, S.A.

Sullivan, F. &. (2009). *Primer informe regional sobre el modelo Cloud.*

Turban, E., King, D., Lee, J., & Viehland, D. (2013). *Building E-Commerce Applications and Infrastructure.*Prentice Hall, pp. 27.

Aguilar, Luis (2012), Computación en la Nube: estrategias de cloud-computing en las empresas.

John, Rothon (2012), Cloud Computing Explained: Implementation Handbook for Enterprises.

4Toro López, Francisco J. (2013) Administración de proyectos de informática. ECOE EDICIONES.

Daniel Peña Valenzuela y Juan David Bazzani Montoya (2013) Aspectos Legales de la Computación en la Nube. Universidad Externado de Colombia.

Torres Viñals, Jordi (2011) Empresas en la nube: Ventajas y retos del Cloud Computing. Libros de Cabecera.

Dordoigne, José (2011) DORDOIGNE Recursos Informáticos Redes informáticas - Nociones fundamentales. Ediciones ENI.

Josep Lluís Cano (2007) BUSINESS INTELLIGENCE: COMPETIR CON INFORMACIÓN.

ANEXO #2:

ENCUESTA

Somos estudiantes de la Universidad Acción Pro Educación y Cultura (UNAPEC) y estamos realizando un levantamiento de información sobre el sistema multilenguaje del Centro De Capacitación, Por Favor Contestar a las siguientes preguntas.

Aspectos Generales

Sexo

a) Masculino

b) Femenino

Edad

a) 18-25 años

b) 26-35 años

c) 36-45

d) Mas de 45

Nivel de Estudio:

a) Primarios

b) Secundarios

c) Técnico

d) Grado

e) Postgrado

1. Si fueras a tomar un curso en línea, por ejemplo, para capacitación Profesional, de los siguientes idiomas ¿Cuál Elegirias?

a) Francés

b) Portugués

c) Mandarín

d) Ningunos de los anteriores

2. ¿Consideras que un traductor en línea facilitaría el aprendizaje del mismo?

a) Si

b) No

c) Tal vez

3. En los últimos 24 meses, ¿Cuántos cursos en línea has dejado de realizar por tener limitaciones con el idioma?

a) 0

b) 1

c) 2

d) 3

e) 4

f) más de 5

4. Organiza en orden de prioridad del 1-3, porque consideras importante tener un traductor en línea, siendo el 1 la razón más importante.

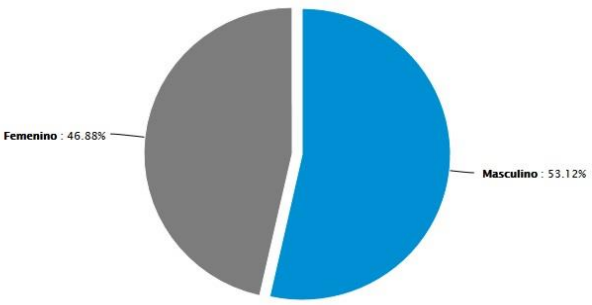
a) evade las fronteras de aprendizaje por tener limitaciones del idioma

b) Fácil forma de utilizarlo

c) Flexibilidad de alcance del programa

Resultados

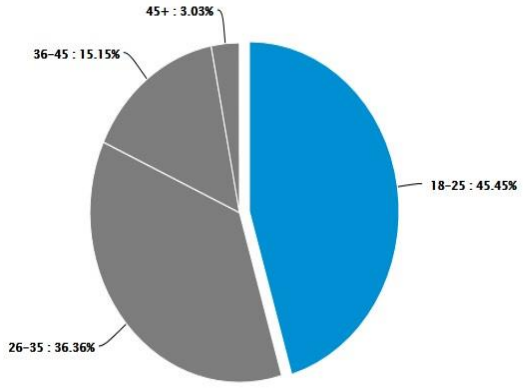
Sexo:



Answer	Count	Percent	20%	40%	60%	80%	100%
1. **Masculino**	17	53.12%					
2. Femenino	15	46.88%					
Total	32	100%					

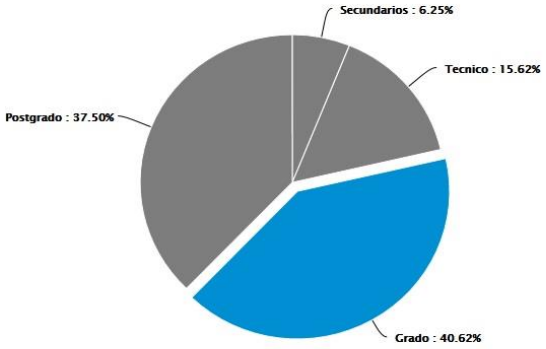
Mean: 1.469 Confidence Interval @ 95%: [1.293 - 1.644] Standard Deviation: 0.507 Standard Error: 0.090

Edad:



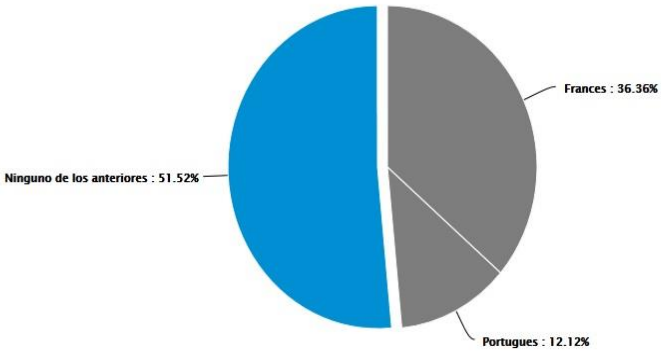
Answer	Count	Percent	20%	40%	60%	80%	100%
1. 18-25	15	45.45%					
2. 26-35	12	36.36%					
3. 36-45	5	15.15%					
4. 45+	1	3.03%					
Total	33	100%					

Nivel de Estudio:



Answer	Count	Percent	20%	40%	60%	80%	100%
1. Primarios	0	0.00%					
2. Secundarios	2	6.25%					
3. Tecnico	5	15.62%					
4. Grado	**13**	**40.62%**					
5. Postgrado	12	37.50%					
Total	32	**100%**					

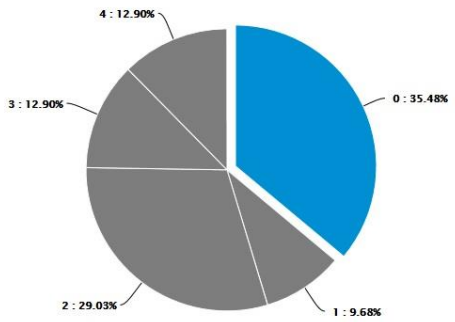
Si fueras a tomar un curso en linea , por ejemplo, para capacitacion profesional, de los siguientes idiomas, ¿cual elegirias?



Answer	Count	Percent	20%	40%	60%	80%	100%
1. Frances	12	36.36%					
2. Portugues	4	12.12%					
3. Mandarin	0	0.00%					
4. Ninguno de los anteriores	**17**	**51.52%**					
Total	33	**100%**					

Mean: 2.667 Confidence Interval @ 95%: [2.179 - 3.154] Standard Deviation: 1.429 Standard Error: 0.249

En los ultimos 24 meses, ¿cuantos cursos en linea has dejado de realizar por tener limitaciones con el idioma?



	Answer	Count	Percent
1.	0	11	35.48%
2.	1	3	9.68%
3.	2	9	29.03%
4.	3	4	12.90%
5.	4	4	12.90%
6.	5+	0	0.00%

Organiza en orden de prioridad del 1-3, porque consideras importante tener un traductor en linea, siendo el 1 la razon mas importante.

	Average Rank		1	2	3
1.	Evade las fronteras de aprendizaje por tener limitaciones del idioma	1.74			
2.	Facil forma de utilizarlo	2.32			
3.	Flexibilidad de alcance del programa	1.94			

Data Table

1.	**Evade las fronteras de aprendizaje por tener limitaciones del idioma**	**14**	**45.16%**	**11**	**35.48%**	**6**	**19.35%**
2.	Facil forma de utilizarlo	5	16.13%	11	35.48%	15	48.39%
3.	Flexibilidad de alcance del programa	12	38.71%	9	29.03%	10	32.26%