UNIVERSIDAD DON BOSCO.
FACULTAD DE INGENIERIA.
ESCUELA DE COMPUTACION

Guía de Referencia Técnica para la Implementación de un cuarto de equipos y servidor Web basado en plataforma Microsoft Windows, orientado a impartir cursos virtuales en la Web, de la facultad de ingeniería de la Universidad Don Bosco.

Presentado por:
Roberto Andrés Alvarenga Sandoval
Asesor:
Ing. Raúl Martínez Rivas
Lector:
Melvin Carias

CIUDADELA DON BOSCO
MAYO DE 2008

Guía de Referencia Técnica para la Implementación de un cuarto de Equipos y servidor Web basado en plataforma Microsoft Windows, Orientado a impartir cursos virtuales en la Web, de la Facultad de ingeniería de la Universidad Don Bosco.

Extracto

INDICE.

I. Marco Teórico.

Introducción.

Actualmente, el interés por mantener una comunicación digital esta en auge, esto se vuelve en un ir y venir de la información, como la conocemos en estos días; por medio de dispositivos de ultima generación que cada vez son mas sorprendentemente pequeños y muy poderosos en manejo de información. Que pueden ser artefactos unitarios independientes o bien formar parte de una PC como herramienta de consulta de información.

Esta comunicación se realiza por una cantidad mas variada de formas de conectividad, donde existe la tradición en el cable de comunicación y la novedad que los medios que utilizan el aire como medio de conexión.

Todos estos beneficios de la informática moderna, se basan siempre en una simple estructura de comunicación que es conocida como “Cliente – Servidor”, siendo esta segunda entidad la mas robusta y de alta importancia por ser fuente de la información, en el momento que el cliente solicite los datos.

Para poder aprovechar estos recursos, se hace necesario utilizar la herramienta de Referencia al momento de implementar una solución enfocada a solicitudes efectuadas desde la red más popular, Internet. Tanto para un servidor como el espacio físico que estará ubicado. Enfocado no solo desde el punto de vista arquitectónico, que muchas veces es a lo que se le da mayor importancia, sino desde el punto de vista de ingeniería. Y es esta ingeniería de diseño lo que puede hacer la diferencia entre unas instalaciones adecuadas para este equipo y las capacidades, de acuerdo a necesidades identificadas.

Teniendo en cuenta esta necesidad, en este documento se enumeran los objetivos que orientan a desarrollar una Guía de Referencia Técnica para la implementación de un cuarto de equipos y servidor web enfocado a la UDB. Además se establecen

los alcances y limitaciones que se esperan desarrollar en dicha guía. Como también se explica la metodología a utilizar.

II. Antecedentes.

En este apartado se ha investigado la existencia de documentos tanto nacionales como internacionales referentes al tema de elaboración de una guía de referencia técnica para la implementación de cuarto de equipos y servidores computacionales, que desde ahora en adelante los abreviaremos GRT y CE respectivamente, así como también la producción investigativa de universidades salvadoreñas, siendo estos últimos los más representativos dentro de la parte nacional.

2.1 Trabajos Realizados por Universidades Nacionales.

Para conocer la existencia de trabajos referentes elaboración de una GRT para la implementación de cuarto de servidores y servidores computacionales, se realizó una investigación bibliográfica en las principales universidades metropolitanas, encontrándose que la producción investigativa acerca del tema es escasa, las investigaciones son orientadas a temas específicos de diseño o guías de diseño orientadas al manejo de cuartos y servidores ya instalados o bien sobre uno de los muchos servicios que estos recintos ofrecen; a continuación se detalla por universidad los documentos referentes al tema de diseño en instituciones de salud.

2.1.1 Universidad Don Bosco.

- “Desarrollo de una herramienta de simulación para el análisis y estudio de una cola con múltiples servidores, aplicada a una entidad bancaria “: Refiere a información y aplicación para simular aspectos de transito de solicitudes de servicios en perfil de cola para servidores dedicados al sistema financiero, con el fin de mejorar los niveles de atención a los clientes.

- “Estudio de Factibilidad sobe la Implementación del Sistema Operativo Linux como Alternativa para Servidores de Red en la Empresa Salvadoreña”: Propuesta al los sistemas operativos de licencia libre y su potencial de manejo para diferentes clases de servidores dentro de la empresa privada de El Salvador.

- “Herramienta para el Análisis de Variables Aplicadas al Marketing, Utilizando Servidores OLAP y Minería de Datos”: Describe la creación de una herramienta informática con base a una investigación de campo, para facilitar las múltiples tareas de los seres humanos en el desempeño de sus profesiones, todo basado en el análisis de datos de arreglos de información tridimensionales de gran volumen, para una mejor toma de decisión.

2.1.2 Universidad Centroamericana José Simeón Cañas.

- “Interfaz CGI para servidores Web y sistemas de administración de bases de datos” Relata como debe ser una interfaz de comunicación, a nivel de aplicación para codificación de la información en el momento de ser enviada y en donde deben estar disponibles tanto en variable de entorno o entradas estándar.

2.1.3 Universidad de El Salvador.

- “Diseño e Implementación de una Intranet con Servicios Chat, Forum de Discusión, Correo electrónico, Servidores de Archivos y a nivel de propuesta, Los servicios de voz y datos sobre protocolos de Internet”: La investigación refleja un diseño y metodología para implementar una red interna con todos los servicios promedio, equiparables a Internet, además hace un diagnostico

del uso actual de la red instalada en el recinto así como también un análisis de costo benéfico de la ínter conectividad.

2.1.4 Universidad Tecnológica.

- "Diseño de un manual de procedimientos para la administración de la Unidad Central de los servidores de cómputo del centro nacional de registros": El documento trata sobre los conceptos que encierran los manuales y definiciones generales de administración, además de incluir una serie de procedimientos para la correcta administración de este centro computacional.

- "Elaboración de una Guía Técnica para Establecer comunicación entre Servidores Remotos Bajo SCO UNIX": Este escrito presenta bases de requerimientos básicos de software, hardware y sus respectivas metodologías para implementación y el correcto establecimiento de la comunicación entre servidores.

2.2 Principales Organismos normalizadores Internacionales.

Se ha investigado la elaboración bibliográfica de entidades normalizadoras internacionales, referentes la implementación de cuarto de servidores y servidores computacionales, construcción, ambientes, instalaciones vitales, dimensionamiento, para tener una base en la cual se sustentarán los criterios de diseño y normas que se utilizarán en la elaboración de GRT para la Implementación de un cuarto de equipos y servidor Web basado en plataforma Microsoft Windows orientado para impartir cursos virtuales en la Web, de la facultad de ingeniería de la Universidad Don Bosco.

2.2.1 Los Estados Unidos de Norte América

Este país cuenta con numerosas instituciones federales y asociaciones encargadas de elaborar Referencias y estándares, otras se encargan de elaborar manuales de

diseño y guías, para instalaciones informáticas, algunas de esas instituciones se muestran a continuación:

2.2.1.1 University of Florida Telecommunication Standards

Universidad del estado de Florida, que persigue con esta guía de referencia creada en Abril del 2005, poder asistir a profesionales en materia de telecomunicaciones que redactan documentos referente a las comunicaciones, para que sean elaborados bajo la norma CSI Format, que obedece a la organización y especificación de materiales en la división 27, Comunicaciones.

2.2.1.2 National Fire Protection Association

Fue creada en 1896, esta es una asociación independiente y voluntaria exenta de impuestos y no lucrativa, la misión de la NFPA es reducir los riesgos de incendios y otros peligros. Esta es una asociación que publica códigos y estándares basados en las normativas de la ANSI[1], lo cual garantiza la imparcialidad de sus publicaciones. Las publicaciones de la NFPA se pueden clasificar en cuatro categorías: Construcción de edificios y seguridad de vida, ingeniería eléctrica, protección contra los incendios e ingeniería química, y protección contra los incendios en general.
La normativa que nos compete en nuestro documento es: NFPA 75 Standard for the Protection of Electronic Computer/Data Processing Equipment, 2003 Edition.

2.2.2 Republica de Colombia

Este país en especial su capital bogota, la alcaldía posee su manual de políticas referentes al manejo de las infraestructuras destinadas a la conectividad.

[1] American National Standards Institute.

2.2.2.1 Alcaldía Mayor de Bogota D.C.

“Manual de Políticas. Políticas Generales y lineamientos para la administración de infraestructura de tecnología de conectividad.” Documento que establece referencia con lineamiento básico que deben tenerse en cuenta para la administración y gestión de los diferentes componentes de infraestructura de tecnología a nivel de Red eléctrica, Rede de cableado estructurado, Centros de computo, Equipos de conectividad LAN / WAN y enlaces de comunicaciones, Equipos de seguridad perimetral y sistemas de voz.

2.2.3 Documentos Internacionales.

2.2.3.1 The Computer Engineering Handbook

Libro basado en la recopilación de escritos específicos sobre todos los temas actuales del área de computación, en el se contiene un apartado especial llamado “Computer System and Achitecture” (Computadora: Sistema y arquitectura) este a su vez contiene “Server Computer Architecture” (Arquitectura De Computadora De Servidor) donde se detallan lineamientos básicos y de gran peso para el acceso a la web y servidores de gran poder.

2.2.3.2 Windows Server System Reference Architecture

La propuesta de WSSRA se basa en el suministro de pautas de diseño de escenarios empresariales y una infraestructura basada en Windows segura y reproducible, simulada en un ambiente de pruebas, con el objetivo de prevenir costos altos y una implementación más rápida de la solución, con menores niveles de riesgos.

III. Definición del Problema.

Un Servidor es un software que proporciona servicios de diversos tipos, a usuarios o computadoras que lo solicitan, normalmente de forma aleatoria que permite la simultaneidad de las peticiones.[2]

El termino Servidor también es interpretado para el conjunto de equipo computacional, que se encuentra compartido en una red informática que es el encargado de ejecutar el software que proporciona los servicios a los usuarios que lo requieren.[3]

Conceptualmente, Servidor es un sistema informático compuesto de un robusto hardware de actualidad, que brinda gran velocidad en procesamiento de información y un software que controla la parte material del servidor para interpretar las solicitudes entrantes y las operaciones de respuesta las cuales ejecuta a gran velocidad de manera simultanea.

En el día a día, la necesidad de acercar la información, requiere equipos dedicados a suplir esta necesidad, Un servidor es una muy buena opción para mantener esta información, segura y accesible. Este tipo de equipo necesita un adecuado espacio físico con requerimientos básicos para albergar adecuadamente estos datos de múltiples niveles de importancia y garantizar su integridad. En base a un pequeño sondeo en busca de un documento que reuniese componentes básicos para implementar un cuarto de equipos y servidor dentro del medio informático de nuestro país, no se pudo localizar un escrito similar que sirviera de referencia para esta necesidad. Esto obliga a que al iniciar un proyecto de montado de CE y servidor computacional, demande una unidad de investigación para reunir los conocimientos fundamentales para determinar el proceso a seguir y los aspectos sensibles a tener en consideración. Esto se traduce, en ocasiones, como inversiones de tiempo y

[2] Definición Servidor. www.definicion.org
[3] Definición Servidor www.wordreference.com

dinero, además esta acción debe ser repetida por cada entidad que tenga la necesidad de montar un núcleo de información similar a lo descrito previamente.

Existen muchos tipos de servidores en el medio de la informática, los principales y de mayor aplicación son: Servidores de aplicaciones, que funcionan como un intermediario entre la aplicación que se desea utilizar y el usuario, servidores FTP que permiten servir cualquier tipo de archivo a través del protocolo de Transferencia de Ficheros (File Transfer Protocol), Servidores de Correo electrónico, que son basados en el SMTP (Simple Mail Transfer Protocol) para la transmisión de mensajes mas detallados con origen y destinatario, Servidores Proxy, utilizados para el control, filtrado y modificación de sitios web y el Web Server que asiste a las peticiones de un cliente cuando solicitan un sitio web por medio del protocolo Http (Protocolo de Transferencia de HiperTexto), siendo estos quizás los mas importantes entre varios tipos de servidores.

Obedeciendo a los diferentes propósitos que tengamos para la información que deseamos compartir, existe uno o varios tipos de servidores que se adecua a nuestra necesidad. A estas entidades de servicio debe protegérseles debido al tipo de información que estas manejan, ya sea Operacional, Sensitiva o restringida. La seguridad con que contaran estos recintos debe estar dentro de los siguientes lineamientos: Acceso físico y lógico, uso del área de equipos, Medidas de seguridad físicas, Registro de modificaciones del área y medidas de contingencia.

IV. Justificación

La información concisa, puntual y actualizada es útil en los momentos en que se decide desarrollar nuevos proyectos de cualquier índole.

Una guía de implementación de un CE y servidor web, que incluya información precisa basada en casos reales de aplicación y disponibilidad de materiales, proveedores y equipos, en El Salvador, tomando en cuenta las condiciones locales, y las proyecciones que la universidad tenga para un futuro, resulta ser una referencia de gran valor al momento de la planificación detallada de un proyecto similar.

Todo lo anterior, respaldado con normativas internacionales específicas y autores reconocidos de mayor experiencia en el diseño y análisis de las instalaciones para comunicaciones y equipos informáticos.

Esta GRT requiere que sea aplicable a las capacidades de alojamiento físico en espacios disponibles dentro de los edificios existentes en el campus I y II de la Universidad Don Bosco, para la instalación de los equipos computacionales y suministros básicos que un CE precisa; o bien una ubicación externa a la UDB estime conveniente, a la vez se orientara sobre la disponibilidad de marcas y modelos de equipos informáticos que posean los proveedores y representantes de empresas informáticas internacionales, acá en El Salvador. Todo esto orientado a la proyección pedagógica e inversión en tecnología de la información que la UDB planee desarrollar para el cumplimiento de su misión y visión.

V. Objetivos.

5.1 Objetivo General.

Elaborar una GRT, que sirva de recomendación para la implementación de un cuarto de equipos con los lineamientos necesarios para dimensionar, evaluar y preparar un adecuado recinto para servidores informáticos y el procedimiento de montado de un servidor web para la emitir dictamen sobre marcas, estilos y capacidades de los diferentes modelos de servidores, con el objetivo de brindar el servicio de cursos en línea de la universidad Don Bosco.

5.2 Objetivos específicos.

5.2.1 Detallar las principales características físicas, métricas, diseño y estructura de servidores, demanda de recursos eléctricos y de comunicación a tomar en cuenta al momento de seleccionar el hardware para el equipo informático que será la entidad Servidor.

5.2.2 Definir los aspectos básicos que un CE debe poseer, relacionados a: Área promedio requerida para albergar equipos considerados, Control de acceso físico, uso general del área de equipos, Medidas de seguridad material, y Registro de modificaciones del área, suministro de electricidad ininterrumpida, medidas de prevención de incendios, control de temperatura interna del CE, Red de datos.

5.2.3 Explicar los medios de comunicación y capacidades de transmisión que deben ser instalados para cumplir con el flujo de la información estimada.

5.2.4 Determinar la mecánica de montaje y puesta en funcionamiento del servidor web para completar el trayecto de los datos.

VI. Alcances.

La GRT contará con todos los requerimientos mínimos necesarios que facilitaran la implementación de un CE, alojamiento, ensamblaje e implementacion de un servidor web, estas exigencias podrán ser aplicadas a un diseño que involucre las instalaciones de la universidad o bien una nueva ubicación externa que la UDB designe adecuada; donde se gozaran de las condiciones mínimas que un CE debe poseer, definidas anteriormente en la nuestra justificación.

Específicamente la GRT de implementación constara de 4 etapas:

- Se determinará las características de equipo, especificación de propiedades físicas y capacidades del conjunto de hardware, para establecer los requerimientos de espacio; recursos eléctricos, comunicación y seguridad, que deben ser instalados en la habitación del servidor.
- Se definirán las características mínimas que esta habitación debe poseer en los sentidos de seguridad material, manejo de espacio interior, Acceso de personal y dispositivos.
- Se precisarán las vías de transmisión de los datos, como enlaces de comunicación, capacidades que esta deba poseer y la disponibilidad de brindar este servicio por parte de las compañías de telecomunicación basados en la ubicación geográfica del servidor web.
- Se concretarán los lineamientos a seguir para iniciar operaciones de servicio web, su conexión y configuración, además de la asistencia técnica necesaria por parte del proveedor.
- Se proporcionaran diagramas arquitectónicos básicos de vista de planta y frontal del CE para recomendar la distribución de todos los componentes de suministro eléctrico, red de datos y distribución de equipos.

VII. Delimitación.

No se incluirán detalles específicamente estéticos. Esto significa que, a pesar de facilitar lineamientos generales en cuanto a los espacios mínimos necesarios y algunas recomendaciones de posicionamiento respecto a otros espacios, conexiones, relaciones y dependencias eléctricas o de comunicación; no se darán indicaciones contundentes en cuanto a la localización específica de los diferentes equipos y demás cualidades de aspecto visual agradable.

Se limitara a dar lineamientos de montado de CE y servidor web, no se entraran en detalles de manejo de la información o de creación de respaldos y recuperación de datos, ni de servicios derivados de un servidor web.

La información presentada en la GRT, los procedimientos de montado de CE y del servidor web, estarán únicamente vinculadas a la tecnología de actualidad que exista en el tiempo y espacio de realización de esta Guía.

El software recomendado para la implementación del servidor, estará estrechamente y únicamente relacionado a su puesta en funcionamiento, no se profundizara en detallar recomendaciones para el modelo de manejo de los datos que se implemente en una fase final.

VIII. Limitaciones.

- Fundados en un pequeño rastreo sobre Información de precedente para proyectos de CE y Servidores realizados a nivel nacional, que sirva como referencia para la elaboración de una GRT para un centro de educación superior, es muy poca o casi invalidada debido a su antigüedad.

- La única información existente es muy restringida al acceso público, ya que figura dentro del medio de la empresa privada.

IX. Proyección Social

La educación nacional, a todos sus niveles, principalmente la educación superior, ha sido uno de los tantos campos que la computación ha venido a revolucionar, debido, principalmente, a los medios de comunicación informáticos y a la facilidad que estos brindan para hacer llegar la información a muchos lugares fuera de los recintos o centros de estudio.

La Universidad Don Bosco, como institución participe de las ventajas que brinda la tecnología de la computación e interesada en facilitar la adquisición de conocimientos para sus alumnos, apuesta a estas bondades para conservar la visión de mantener una calidad educativa y humana superior al promedio nacional, esto hace que la institución este en constante búsqueda para mejorar los medios de cómo trasmitir los conocimientos y esta muy bien comprobado que el Internet es un medio muy viable a todo nivel.

Es difícil cuantificar la proyección del beneficio social de este documento, sin embargo, esta herramienta, al ser utilizada como referencia de implementación, permite que se planifiquen mejor los proyectos, sin perdidas de tiempo, recursos y dinero que suceden frecuentemente a la hora de diseñar, por bibliografías contradictorias, o que no se adaptan a las realidades del país.

Con la intención de precisar un beneficiado directo de este proyecto, podríamos señalar a: La creciente comunidad de la Universidad Don Bosco, ya que un informe que contenga directrices concernidas a la preparación de equipo informático para almacenamiento y manejo adecuado de la información, formas seguras de compartirla, protección a estos datos tanto física como lógica y estimaciones de crecimiento a futuro de volúmenes de datos y equipo; se traduce en una gran disposición de los conocimientos de manera inmediata y sin restricción de horarios, además de reducir los problemas de transmisión de conocimientos y documentación de los cursos impartidos en la Universidad.

X. Marco Histórico.

A nivel internacional, se pueden mencionar normativas y referencias ejemplares a seguir, debido a su trayectoria en la ingeniería de las comunicaciones, electrónica y computación. Nos remontamos específicamente a las regiones como Norteamérica y Europa.

10.1 Norteamérica.

- **IEEE**. Instituto de Ingeniería Eléctrica y Electrónica. Esta institución fue fundada el 1ero de Enero de 1963. Es una organización internacional sin fines de lucro y una organización profesional para el avance de tecnología relacionado a la electricidad, aunque actualmente incluye una gran diversidad de disciplinas. Una de las referencias que se aplica al tema aquí tratado son los estándares para la tecnología de la información. Telecomunicaciones e intercambio de información entre sistemas de servidores.
- **Microsoft**. compañía fue fundada en 1975 por William H. Gates III y Paul Allen, se han dedico inicialmente a desarrollo de software para computadoras personales, en la actualidad Microsoft provee de soluciones completas en la gran mayoría de necesidades en el extenso campo de la computación. Una de las referencias que compete en nuestra temática es el Windows Server System Reference Architecture. Que trata sobre recomendaciones para soluciones específicas de sistemas de almacenamiento, manejo y transferencia de información basado en servidor.
- **ACM**. Association for Computing Machinery, es una organización internacional científica y educativa dedicada al avance de las ciencias, arte y aplicaciones de la tecnología de la información desde 1947. Lideres en recursos de y para profesionales en computación que se desempeñan en las variadas áreas de la tecnología de la información. Además de trabajar en la interpretación del impacto de la información en la sociedad. Con sede en Nueva York. Actualmente la ACM contiene un documento que se relaciona en la seguridad

de servidores, este es el Server scaling with network-attached secure disks, que trata sobre la seguridad de los datos, mediante arreglo de discos de expansión controlada y discos de alta seguridad.

10.2 Europa.

- **CEPT**. The European Conference of Postal and Telecommunications Administrations fue establecida en 1959 por 19 países, el se expandió a 26 durante los primeros diez años. Los miembros originales fueron los controladores del monopolio postal y administradores de telecomunicaciones.
- **ETSI**. The European Telecommunications Standards Institute (ETSI) desde 1949 es una organización independiente y sin fines de lucro que tiene por misión producir estándares de telecomunicaciones para la actualidad y para el futuro. El instituto europeo de los estándares de las telecomunicaciones (ETSI) es oficialmente responsable de la estandardización de las tecnologías de información y de comunicación (ICT) dentro de Europa. Estas tecnologías incluyen telecomunicaciones, la difusión y áreas relacionadas tales como transporte inteligente y electrónica médica.

XI. Marco Teórico.

La GRT para la Implementación de un CE y servidor Web, es un documento que contiene la descripción de procedimientos que deben seguirse para la realización de diseños y evaluación de instalaciones para cuartos de equipos y servidores computacionales.

La GRT esta basada en una serie de estándares, criterios y normativas internacionales, las cuales le dan la pauta para la aplicación en un ambiente educativo de nivel superior, lógicamente, se hace un trabajo analítico antes de tener La GRT plasmada, ya que se tiene que adaptar a las necesidades locales.

Un estándar o normativa, se puede entender, como el conjunto de reglas y definiciones que especifican como llevar a cabo un proceso o la producción de un producto. Los estándares o normativas se establecen por consenso y se aprueban por un cuerpo reconocido para su uso común y repetido, enfocados en alcanzar un resultado óptimo dentro de un contexto dado.

También, una La GRT suele contener ejemplos de los procesos de diseño y protocolos de evaluación en base a los criterios establecidos.

Por lo tanto, la GRT es un documento que facilita las acciones de diseño de un CE y servidor Web, y a la vez brinda una herramienta para la evaluación, control y vigilancia de los mismos.

La estructura a nivel macro de una GRT es la siguiente:

- Identificación o Carátula. Se detalla el nombre de la guía.
- Índice o Contenido. Se muestra el contenido de la guía, así como sus sub contenidos en cada uno de los temas a desarrollar.
- Introducción. Exposición del documento, áreas de aplicación e importancia.

- Objetivos del Manual. Explicación del propósito que se pretende cumplir al realizar los procedimientos.
- Conceptos. Conceptos de carácter técnico que se emplean en el desarrollo del contenido, los cuales por su significado o grado de especialización requieren una explicación o ampliación de su significado.
- Desarrollo del contenido del documento. Exposición detallada del contenido de la GRT, especificando los diferentes aspectos de cada tópico.
- Glosario de términos. Términos usados en el desarrollo la GRT.

Cada una de las áreas desarrolladas tendrá un análisis general basado en los siguientes pasos:

- Normas, criterios y estándares de Ingeniería para el diseño de instalaciones.
- Y montado de servidor web En esta parte se hará una mención de las normas a considerar para el diseño.

- Desarrollo del procedimiento.
  Presentación por escrito, en forma narrativa y secuencial, de cada una de las operaciones que se realizan en un procedimiento, explicando en qué consisten, que aspectos se tienen que tomar en cuenta, etc.

- Ejemplos de Aplicación del documento
  Pequeños ejemplos hipotéticos del procedimiento, fácilmente reproducible en otras situaciones relacionadas al tema.

XII. Metodología.

En el desarrollo del la GRT se utilizará diversos recursos, referidos a continuación:

12.1 Investigación Bibliográfica.

Esta previsto realizar una investigación bibliográfica, tomando en cuenta aquellos libros o documentos que atañen al tema de diseño la Implementación de un CE y servidor Web, siendo estos escogidos por su calidad y respaldo internacional.

12.2 Investigación en tesis.

Se tomarán de referencia ciertas tesis de Universidades nacionales identificadas por sus atributos de contenido y que estén acordes al tema la Implementación de un CE y servidor Web.

12.3 Investigación en la Internet.

Se realizará búsquedas de documentación y estándares de organismos internaciones de renombre, que se refieran a la Implementación de un CE y servidor Web.

XIII. Contenido.

Dentro de este apartado, se definen las fases en que se desarrollara el documento sobre la temática propuesta, iniciando por definir una solución apropiada a la necesidad informática, modelar la infraestructura del CE, sus conexiones de recursos de información y eléctrico, además de el montado general de el servidor y su seguridad lógica.

CAPITULO I Solución.

- Definición de Solución informática.
- Características de equipo y espacio preciso.
- Evaluación de opciones de solución.

CAPITULO II Infraestructura.

- Ubicación Física.
- Conexiones y demanda eléctrica.
- Infraestructura de Pisos, Paredes y Techo.
- Consideraciones ambientales internas.

CAPITULO III Conexiones.

- Racks
- Cableado.
- Dispositivos de interconexión.

CAPITULO IV Seguridad Física.

- Acceso Físico
- Seguridad Física de la infraestructura.

CAPITULO V Montado de Servidor.

- Hardware
- Dispositivos de almacenamiento.

CAPITULO VI Seguridad Lógica.

- Seguridad virtual (Firewall's)
- Administración de Seguridad.
- Servicios de aplicaciones Web Aplicaciones

CAPITULO VII Guía de Referencia Técnica para montado de Servidor Web. (Extracto)

CAPITULO VIII Conclusiones, Observaciones y Recomendaciones

CAPITULO IV Anexos

CAPITULO I. Solución Informática.

De acuerdo con las necesidades de colocar a disposición pública la información educativa de la Universidad Don Bosco, para poder impartir cursos virtuales en la web, todo de manera segura, escalable y con una alta disponibilidad de la información, se comienza definiendo una serie de requerimientos en equipos informáticos que albergaran la carga de datos y el procesamiento de solicitudes de datos, a todo este proceso de selección y definición de equipos nos entregara lo que llamaremos nuestra solución informática.

1.1 Definición de necesidades.

Como mencionábamos anteriormente, definiremos nuestros tres principales requerimientos para la obtención de una solución informática eficaz de acuerdo a las necesidades planteadas con anterioridad.

1.2 Alta Disponibilidad de la información.

La alta disponibilidad de la información se logra al minimizar los puntos de fallos únicos en los equipos encargados de brindar el servicio de procesamiento de solicitudes, almacenaje y manipulación de los datos.

A continuación, notaremos como colocar características de alta disponibilidad de la información, en cada uno de los componentes que serán parte de nuestra solución de servidor web.

Fuentes de poder: Fuentes de poder que permitan el suministro de energía eléctrica al sistema informático, de forma compartida en la carga eléctrica, en caso de que una de las dos falle, la segunda asume el 100% de la carga eléctrica en distribución, o bien si una es apagada para dar mantenimiento, el servidor continuará operativo mientras se conecta la segunda fuente.

Procesadores: Unidades que soporten tolerancia en fallos por medio de configuraciones de múltiples procesadores para brindar procesamiento de la información de manera ininterrumpida.

Memoria: Los componentes computacionales deben soportar tolerancia de fallos por medio de "cambio en caliente"[4] para poder seguir operantes mientras se da mantenimiento a la unidad que presento el error.

Almacenaje directo: La unidad de almacenaje debe soportar cambio en caliente de discos defectuosos, otra opción es poder configurar arreglos RAID 1 como espejo de la información para que entre en operación mientras se le da revisión al arreglo principal.

Adaptadores de Red: estos dispositivos de comunicación, deben proveer la disponibilidad de soportar Teaming para el mejor balance de distribución de transmisión de datos en la red.

Tarjetas de Expansión: Todas deben soportar cambio en caliente

[4] Cambio en Caliente o "Hot Spare" componente de hardware que se encuentra en espera del fallo de su(s) equivalente(s) para entrar en acción y asumir el rol del faltante.

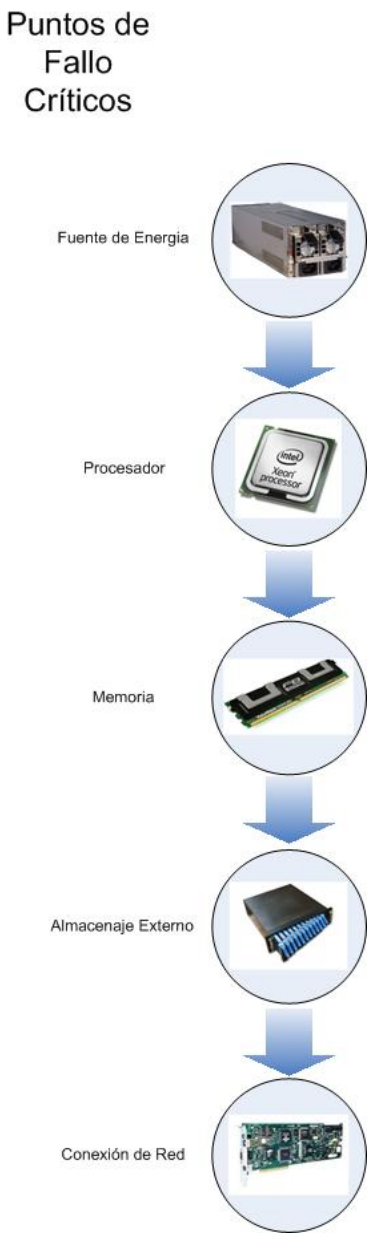


Fig. 1.1 Diagrama típico de elementos funcionales para el cumplimiento de consultas a servidor, donde cada dispositivo representa un punto de fallo único y posible ruptura de secuencia de información.

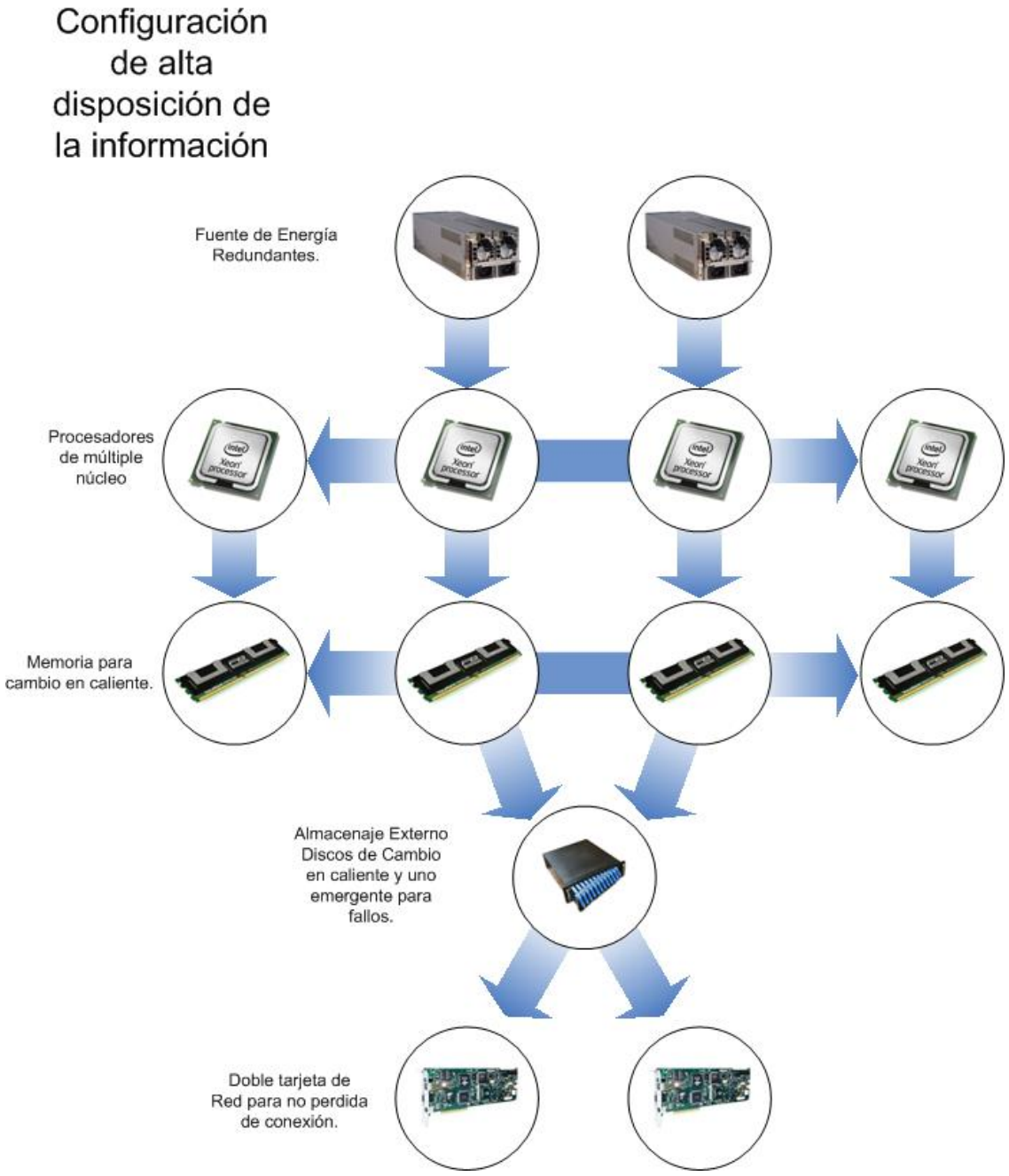


Fig. 1.2 Configuración de alta disponibilidad de la información, donde se mitigan los puntos de fallo únicos, se brindan opciones de caminos a seguir para responder en circunstancias extremas a una solicitud.

1.3 Seguridad de equipos y datos

La seguridad de equipos será alcanzada por medio de un conjunto de garantías que se da a cada una de las partes, lógicas y físicas, involucradas en la contención y manipulación de los datos.

Ahora veremos como lograr seguridad de equipos y datos en cada uno de los componentes físicos y virtuales que serán parte de nuestra solución de servidor web.

1.3.1 Uso de Contraseña.

Para dispositivos que se les pueda activar un password desde la configuración de BIOS[5].

1.3.2 Deshabilitar disketera.

Los dispositivos a adquirir deben tener la capacidad de poder desconectar la disquetera y no poder arrancar de diskets, CD o unidades de memoria flash con puerto USB[6].

1.3.3 Herramientas de administración de seguridad.

Software de protección donde se pueda utilizar SSL sobre conexiones HTTPS[7].

1.3.4 Administración remota.

Si se utiliza administración remota, debe ser posible otorgar diferentes niveles de autoridad para diferentes usuarios.

[5] BIOS: Es el bloque de instrucciones grabadas en la memoria de solo lectura ver glosario.
[6] USB: Universal Serial Port, ver Glosario
[7] HTTPS: HyperText Transport Protocol Secure, ver Glosario.

1.3.5 Controladores de arreglo de discos seguros por contraseña.

Si se implementa arreglos RAID[8] para el servidor, el software de configuración debe contar con la posibilidad de configurar password, para evitar cambios no autorizados.

1.3.6 Cifrado.

Si la información que el servidor maneje, va a ser transmitida por medio de redes públicas y esta sea información sensible, debe ser posible cifrar los datos. (SSL[9])

[8] RAID: Redundant array of inexpensive drives, ver Glosario.

[9] SSL: Secure Sockets Layer ver Glosario

Fig. 1.3 Detalle de los factores importantes que nos brindan seguridad a los equipos informáticos y el manejo de la información de estos.

1.4 Escalabilidad

Propiedad de todo un sistema, una infraestructura de red o un proceso de información, que indica habilidad para manejar el crecimiento continúo de demanda de procedimientos de manera fluida, o bien preparado para hacerse expandirse sin perder calidad en los servicios ofrecidos.

A continuación veremos como lograr escalabilidad en cada uno de los componentes críticos que serán parte de nuestra solución de servidor web.

Procesador: la clave para la escalabilidad del procesador es la velocidad de este, el número de ellos y la memoria cache. Una manera de asegurarnos la escalabilidad del procesador es configurar el servidor con la máxima capacidad de procesadores para el escogido, esto para asegurarnos del buen manejo de la carga asignada. Pero la opción mas atractiva es disponer un arreglo de procesadores que posean la tecnología hyper-threading[10], para no saturar de espacios disponibles de procesador y en un futuro configurar mas procesadores para mejorar el desempeño del mismo.

Memoria: Para adquirir escalabilidad es preciso tener memoria de ultima generación, y una cantidad que logre manejar el volumen solicitudes a entrar, de 2.0 a 4.0 GB de preferencia memoria FBD[11] (Fully Buffered DIMMs)

Direct Attached Storage[12] (DAS): Número de ranuras para discos, velocidad de rotación, diseño de LUNs, velocidad de transferencia, I/O Cache.

[10] HYPER-THREADING Característica de los procesadores Pentium que toma un chip físico y simula dos lógicos.
[11] FDB: Tecnología de memoria que permite incrementar la confianza, velocidad y densidad en los sistemas. Ver Glosario.
[12] DAS: Discos contenidos en un gabinete computacional, conectado directamente al CPU. Ver Glosario

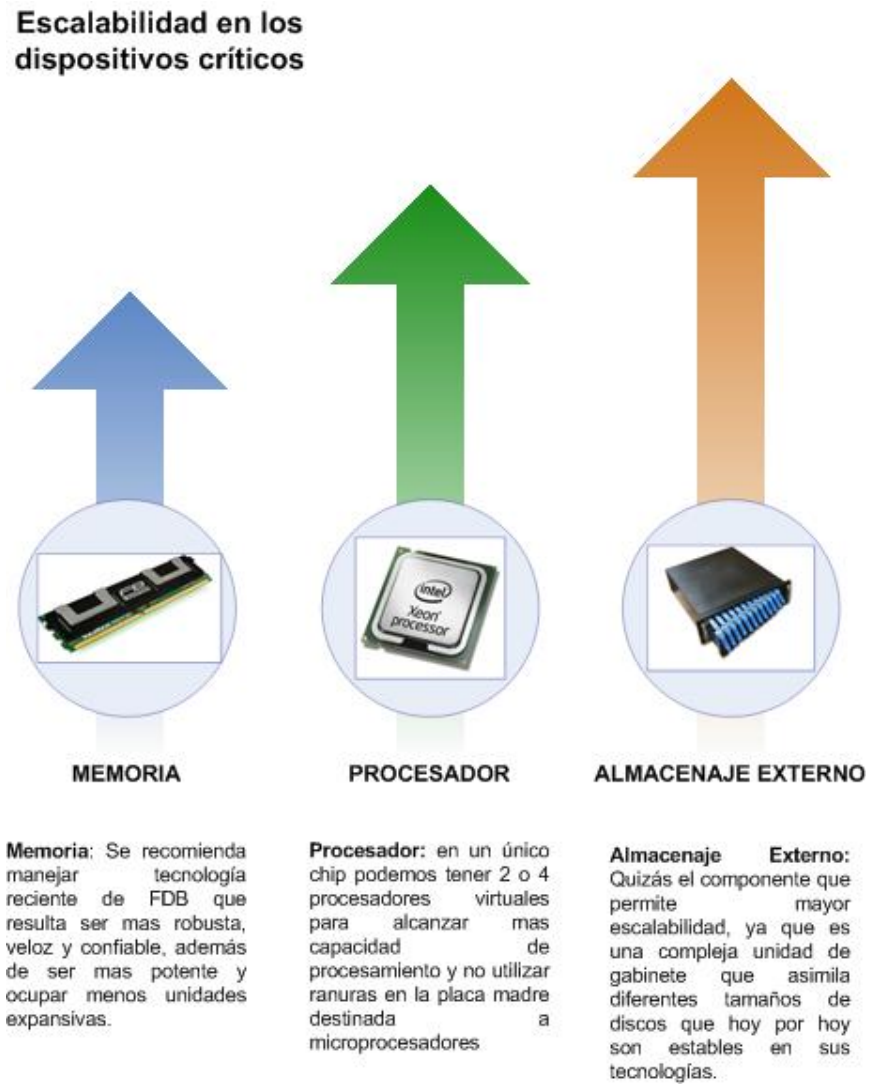


Fig. 1.4 Escalabilidad representada según prioridad de posibilidad en elementos críticos del servidor Web.

1.5 Características de equipo

El perfil de la solución informática de acuerdo a los análisis anteriores, que nos permitiría cumplir con las necesidades propuestas se extractarían en la siguiente tabla.

Las marcas de equipos de TI, con presencia acá en el país representadas por compañías de larga trayectoria y presencia regional, tenemos a Heweltt packard y DELL estas marcas han experimentado avances importantes no solo en tecnologías

tradicionales, sino en tecnologías nuevas de servidores tales como blade servers, discos de fibra, almacenamiento de datos centralizados entre otros.

Las compañías que reúnen las características que un proveedor debe poseer en cuanto a presencia nacional, conocimiento de la línea del negocio y soporte técnico, tenemos a Grupo RAF representado la marca DELL, EDP/Sigma que representan a HP y Tecnasa.

Característica / Equipo	**Requerimiento Mínimo**	**Requerimiento Medio**	**Requerimiento Optimo**
Cantidad de Procesadores	1	2	3 - 4
Velocidad de CPU	2.33GHz[⌂]	3.0 GHz[⇮]	2.66 GHz[†]
Memoria	1 GB	2 GB	Mayor a 2 GB
Discos de almacenamiento	2 Discos	4 Discos	6 Discos
Tecnología de configuración HDD	SCSI RAID Hotswap	SCSI RAID Hotswap	SCSI RAID Hotswap
Capacidad de Discos de almacenamiento	36 GB	73 GB	146 GB
Tarjetas de Red integradas	1	2	2 con Teaming[14]
Puertos PCI	1	1 PCI - X y 1 PCI	3
Unidades en Rack	1 U	2U	2U – 4U
Fuentes de Poder	1	2 en Redundancia	2 en Redundancia

Tabla 1. Características de equipo en cuadro comparativo de mínimo – medio - óptimo.

[1] Dual-Core Intel Xeon Low Volt 5148
[2] Dual-Core Intel Xeon 5100
[3] Quad-Core Intel Xeon 5300
[4] Teaming: Adaptadores de red múltiples, ver Glosario

Detalle	DELL		RAF		EDP/SIGMA	
Rack	PowerEdge 4120 Rack Enclousure	$4,764.00	PowerEdge 4120 Rack Enclousure	$3,141.00	Rack HP 10642 42U	$2,977.13
Servidor Web	PowerEdge 1950	$3,290.00	PowerEdge 1950	$4,257.00	HP DL380G3	$4,068.21
DAS	PowerVault 220S Disk Storage Enclosure	$3,758.23	PowerVault MD 1000 SAS/SATA	$3,853.00	PowerVault 220S Disk Storage Enclosure	$3,156.30
UPS	UPS - Battery Back-Up Power	$1,376.89	Tripplite 5KVA	$1,920.00	UPS APC Smart-UPS RT 5000VA	$3,515.00
Switch administrable	Dell Powerconnect 6024	$2,471.00	Delink Corporate 24 Modelo DGS-3324SR.	$3,781.00	HP ProCurve Switch 2848	$3,342.92
Consola de control	1U Console Tray w/Touchpad, Keyboard & 15inch Flat Panel 1UKMMR	$1,553.99	1U Console Tray w/Touchpad, Keyboard & 15inch Flat	$1,979.00	1U Console Tray w/Touchpad, Keyboard & 15inch Flat	$1,603.17
Servicios de instalación e implementación		$3,189.31		$4,000.00		$ 6,356.18
TOTAL		**$20,403.42**		**$22,931.00**		**$25,018.91**

Tabla 2. Comparación de precios por equipos y proveedor.

Luego de la revisión y evaluación cuantitativa y cualitativa de las ofertas recibidas de los proveedores (DELL, RAF y EDP/SIGMA), se considera recomendable la oferta de RAF con base a los criterios expuestos a continuación:

1.6 Criterios Económicos

Hay una opción de precios más bajos que los ofrecidos por RAF, pero la calidad de los equipos o servicios no llenaba de manera óptima el requerimiento de esta solución informática.

El plan de pagos ofrecido por RAF es de crédito a 30 días por el 50%, y crédito a 60 días por el resto. Dado que los plazos previstos para tener implementadas las soluciones son menores a 60 días, el segundo desembolso estará condicionado al cumplimiento satisfactorio de parte del proveedor.

1.7 Criterios Técnicos

Los equipos ofertados por RAF resultaron ser los más ajustados a nuestros requerimientos, equilibrando precios y calidad.
La oferta de servicios de soporte y garantía de RAF (24x7x365), tiene la ventaja de contar con un equipo capacitado disponible localmente, lo que supone una mejor y más rápida respuesta ante cualquier necesidad de soporte técnico, sin los contratiempos y gastos adicionales de traer técnicos especializados del exterior.
Las soluciones sugeridas para este proyecto, ya han sido implementadas por RAF en otras compañías locales, por lo cual ya cuentan con experiencia previa comprobada en proyectos similares.
La marca de los equipos ofertados por RAF es DELL, lo que garantiza respaldo regional, tomando en cuenta que RAF instala equipos en todo El País y la región siendo representante directo de esta marca.

1.8 Microsoft como selección de plataforma de software.

Microsoft ha alcanzado un muy alto nivel de desarrollo en sistemas operativos para configuraciones de alta disposición de la información, actualmente desarrolla una herramienta montada en sistema operativo, capas de brindar redundancia entre servicios de servidor de datos; a la vez establece los lineamientos a seguir para enriquecer una alineación que garantice la máxima disposición de los datos ante múltiples activaciones de puntos de falla, lo cual es común entre el medio informático sin interrupción de los servicios.

Esta herramienta, anteriormente se incorporaba en las primeras liberaciones de versiones del Microsoft Windows Server 2003, donde se podía montar un cluster de replicación en configuración activo – pasivo o activo – activo con ciertas limitantes de control sobre los servidores. Microsoft Windows Compute Cluster Server 2003 R2, no solo proporciona control de una configuración física de redundancia de servidor,

sino también sostiene los servicios como operativos individuales y monitoreo al detalle de esta prestación, es decir, si alguno de los servicios que se están prestando desde el cluster de servidor, hacia la red, llegase a fallar o a no ser activado; el monitoreo de Microsoft Windows Compute Cluster Server 2003, ofrece el levantamiento individual del servicio que se presta. Además de crear y configurar un servidor virtual que es el principal ante la red y los clientes se conectan directamente a el; En caso que uno de los dos servidores se diera de baja por problemas internos, el segundo entra a soportar la carga de la demanda de información, sin tener que efectuar ningún cambio para los clientes, siendo una transición transparente para ellos. Por estas características de redundancia en configuración, amplio desarrollo de los productos que proveen, representación del fabricante en el país, soporte a sus aplicaciones a nivel mundial, generación de documentación de respaldo y asesoría en proyectos de esta clase, es que se recomienda a Microsoft como la mejor opción para la adquisición de la plataforma de software.

1.8.1 Recomendación de configuración de Cluster.

En el caso que se considere una configuración de Cluster, para la solución informática para este instituto de educación superior, únicamente debe considerarse un precio doble de servidor, ya que se necesitaría uno adicional para la creación de Cluster, y aumentar los gastos de Servicios de instalación e implementación, para la configuración de cluster Server dentro de nuestra solución informática.

Todas las empresas listadas tienen la capacidad de brindar este tipo de asesoría y es un procedimiento de complemento en configuración, pero debe ser especificado que se necesita con anticipación antes de dar inicio a la configuración general, ya que existe tanto hardware como software que debe ser instalado y probado antes de poner en producción nuestro servidor.

CAPITULO II. Ubicación Física, Conexiones y demanda energética, Infraestructura de Pisos, Paredes y Techo. Consideraciones ambientales.

2.1 Generalidades Demanda energética.

Instalaciones para poner a tierra equipo de tecnología de la información.

De acuerdo con el "Information Technology Industry Council", el 90% de los problemas con los ETI[15], son relacionados a los equipos informáticos y a la infraestructura que los contiene, solo el 10% de los problemas son relacionados al servicio eléctrico. Importante también saber que el 75% de los problemas que se dan relacionados a las instalaciones que alojan los equipos informáticos, es debido a realizar una apropiada instalación a tierra, el factor único y más importante factor para el funcionamiento de los sistemas de ETI.

La intención de poner a tierra correctamente todos los equipos de TI, está ligada a mantener una baja impedancia y evitar los siguientes incidentes con presencia de baja y alta frecuencia.

Baja frecuencia < 100 Hz

Choques eléctricos
Daño a equipos por voltajes transitorios.

Alta frecuencia > 100 Hz

Contaminación o corrupción de datos
Corriente en los conductores de tierra

[15] Equipos de Tecnología de la Información.

Recomendaciones para procedimientos de presencia de corrientes objetables en conductores a tierra.

- Descontinuar uno o más polos a tierra que se les detecte corrientes de ruido en las líneas, únicamente con la recomendación que no pueden ser eliminados todos los polos a tierra, caso fuera que con un único polo a tierra persista el ruido eléctrico en las líneas, es necesaria una revisión de la red eléctrica para su reimplementación.

- Interrumpa la continuidad del conductor o la vía de interconexión al polo tierra.

- Cambiar la ubicación física de las conexiones a tierra, fortaleciendo el aterrizaje

2.1.1 Importancia del ambiente eléctrico.

El ambiente eléctrico para computadoras incluye sus fuentes de energía, el sistema a tierra y las interfaces eléctricas con las líneas de comunicaciones, sistema de aire acondicionado y los sistemas de seguridad industrial. También incluye el sistema de luminarias y otros equipos ubicados en la sala de computadoras.

Además se evalúan características de los pisos de sala de computadoras, para maximizar el uso de espacio para conexiones eléctricas, de datos y sistemas de ventilación, además considerar algún tipo de mueble útil dentro de la sala y a la vez evitar las descargas electrostáticas.

El ambiente eléctrico adyacente a la sala de computadoras, también debe considerarse, ya que las perturbaciones eléctricas se propagan a través de

conductores, tuberías, conductos metálicos y partes estructurales del edificio o por medio de radiación electromagnética, como en el caso de ondas de radio.

Ningún equipo es inmune totalmente a las interferencias y perturbaciones, sin embargo la sensibilidad puede variar de un equipo a otro y de un tipo de perturbaciones a otro. Las interferencias o perturbaciones de alta energía pueden causar fallas catastróficas o mal funcionamiento en algunos componentes. Las perturbaciones menores tal vez no dañen los equipos, pero pueden corromper las señales de lógica y causar errores en los datos o señales de control.

La utilización de computadoras o equipos con componentes electrónicos digitales crece continuamente, en todos los ambientes profesionales inimaginables, el fallo de estos sistemas de computadoras puede afectar actividades criticas dentro de una empresa.

2.1.2 Características de la energía eléctrica a estar disponible.

La corriente eléctrica proporcionada por los proveedores, para la red publica, puede estar disponible en muchas variaciones de voltajes y configuraciones de fase. La configuración preferida y la selección lógica dependen del tamaño del sistema y equipo utilizado. En vez de intentar la adaptación de un equipo de procesamiento de datos a un sistema antiguo de alimentación energética, es preferible instalar un cableado exclusivo para el equipo electrónico sensible que tenga un voltaje adecuado y mínimo de interacción con otros elementos de la infraestructura del edificio.

La frecuencia de la energía eléctrica suministrada en Estados Unidos, y la mayor parte de los países de Latinoamérica es de 60Hz. Acá en El Salvador la frecuencia de la línea no es la optima, por lo que muy a menudo se presentan problemas en los sistemas de computadoras, tales como daños físicos en discos duros al ser

desalineados magnéticamente por una variación eléctrica muy dramática, quemado de fusibles en periféricos, daño en fuentes de voltaje, Una de las reacciones que se pueden tener por una variación de tensión, y que esta sea dada con tendencia a la baja, es por naturaleza el aumento de la corriente, esto genera calentamiento en las líneas de transmisión y por ende, la activación de las protecciones de los equipos informáticos, en caso que no este dimensionado correctamente estas medidas de prevención, se pueden dañar elementos internos protectores o de los equipos informáticos, entre otros. De la misma forma, fuentes independientes de potencia como plantas eléctricas a base de motor diesel o motores eléctricos no tienen la estabilidad que ofrece una central eléctrica, para ser tomadas como una medida de fuente de energía continua y sostenida, este tipo de fuentes independientes únicamente es recomendable, como medidas de contingencia, para cortes de energía prolongados y dentro de condiciones ideales de mantenimiento y carga seleccionada en configuración de soporte, ya que se considera como una fuente aislada de energía, los lineamientos de selección de una adecuada planta generadora de electricidad se describen en el apartado 2.5.1 de este capitulo.

Los límites en los cuales se espera que la fuente de voltaje pueda variar sin tratamiento especial es aproximadamente -13% a + 5.8% El voltaje de línea no debiera variar más allá de -10% a + 3% del valor nominal.

Estos límites permiten esperar resultados confiables. El voltaje nominal de línea es una designación conveniente para esta clase de voltaje.

Las mediciones de voltaje de línea pueden variar de una ubicación a otra, así como, la hora del día ya que las cargas cambian. Cuando se habla de 110V, 115V, o 117V se esta hablando de 120 V

2.1.3 Tierra de Referencia Cero de un sistema.

La expresión “Tierra del sistema” utilizada en esta sección 2.1.3, se refiere a un cable aislado , separado y que tiene aislante color verde o verde con bandas amarillas, que esta conectado a tierra y se instala para computadoras y equipos que cuentan con microprocesadores.[16]

Este conductor de conexión a tierra también es un conductor adicional para la seguridad, lo cual se ilustra en esta figura.

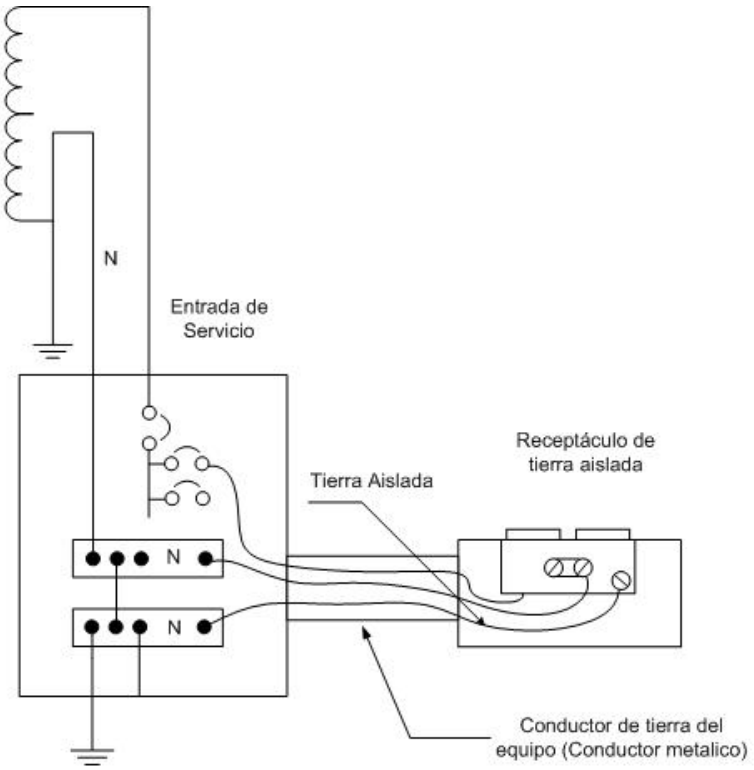


Fig. 2.1 Receptáculo de la tierra aislada, especifica, libre de ruidos. También muestra la tierra del equipo como conducto metálico.

[16] NEC 250.119 Identification of Equipment Grounding Conductors

El propósito de este sistema es presentar un sistema “libre” de ruidos, de referencia cero para todas las fuentes de alimentación de corriente directa y en los sistemas informáticos.

La sección 250-146(d) y la sección 384-20 de Código Eléctrico Nacional (NEC) permiten que un conducto de puesta a tierra de equipo se instale desde un punto de unión neutro/tierra (equipo de servicio) terminal X_o de una fuente derivada separadamente hasta el equipo, o a los receptáculos aislados a tierra para el equipo. Este conductor de tierra aislada, debe instalarse con los conductores de circuito, el conductor neutro u el conductor de tierra de seguridad y podrá pasar a través del tablero o panel de control como se describe en las dos secciones arriba citadas y en la sección 250-96(b)

El conductor de tierra del sistema no debe ser conectado al conducto de distribución secundarios por los cuales se desplaza, sino que solo termina en los bloques de terminales “aislados” en el cable aislado principal de tierra u otra “tierra aislada” o receptáculo, en la tierra aislada (lógica) del equipo y en el punto único de unión de la fuente de energía.

La tierra de seguridad también debe de instalarse y conectarse con objetivos de seguridad; es decir que el caso de un toma duplex aislado, el contacto de forma circular se debe conectar a la terminal flexible aislada de tierra en la parte posterior del receptáculo.

El tornillo que sostiene la cubierta delantera del receptáculo se conecta a tierra de seguridad por medio de los sostenedores del montaje y la caja metálica donde se monta el receptáculo. Si se usa una caja plástica se debe considerar un conductor de tierra de seguridad y este debe extenderse junto con el conductor de fase, el neutro y los conductores de tierra aislados. Además, deben fijarse a los sujetadores de montaje del receptáculo para conectar a tierra la lámina frontal.

2.1.4 Conexión confiable a tierra para equipos de cómputo.

El significado de punto único de conexión a tierra se ha establecido como estándar para realizar la conexión a tierra para equipo electrónico sensible.

Es de alta importancia colocar un punto único de referencia de tierra para lograr la confiabilidad de un equipo y una satisfactoria operación de todos los sistemas de cómputo.

La confiabilidad y operación de un sistema computarizado mejorara utilizando este método, la cual esta basada en el mantenimiento de un plano equipotencial para todos los equipos y así evitar diferencias riesgosas de voltaje que puedan afectar el buen funcionamiento del equipo electrónico. Es una realidad que algunos sistemas no operan si no se cuenta con esta técnica aplicada. La acometida del edificio debe ser la referencia inicial para el sistema de un solo punto a tierra.

Es aun más provechoso indicar un punto único de unión neutro (tierra) para el sistema de cómputo instalado, ya sea en el dispositivo de tratamiento de potencia del sistema o en el secundario del transformador reductor.

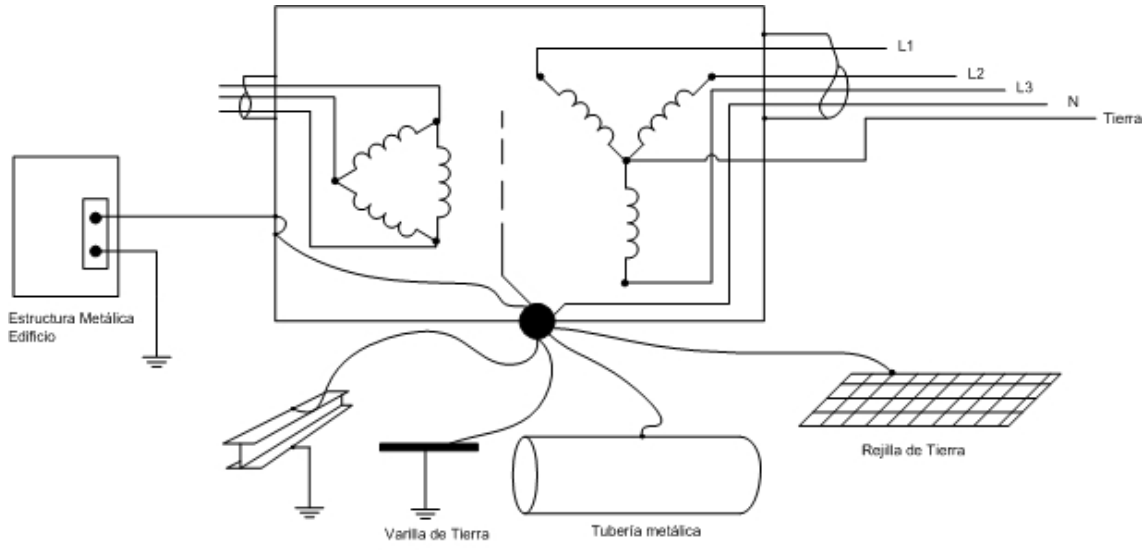


Fig. 2.2 Punto único de conexión a tierra para sala de computadoras

Siempre es necesaria la instalación de un transformador de aislamiento tan cerca del sistema de procesamiento de datos, como sea posible debido a la impedancia que presentan los conductores largos, lo que genera diferencias de potencial a lo largo del conductor y como consecuencia presenta ruidos eléctricos e interferencias que afectan los equipos electrónicos, en ultima instancia de daño de este transformador aislador por sobrecalentamiento debido a una baja tensión, se genera un cortocircuito, protegiendo el resto de líneas de cualquier ruido o armónico que pudiese pasar al resto del conductor de alimentación.

Esta fuente derivada separadamente aísla al sistema eléctrico de los ruidos en el sistema de alimentación eléctrica del edificio. Se recomienda que el sistema tierra del equipo electrónico de la sala de computadoras, que esta instalado en el secundario del transformador, se conecte al sistema de tierra del edificio. Esto se hace para establecer un cortocircuito entre los sistemas de tierra y mantener así todo el sistema al mismo potencial ante la eventualidad de descargas atmosféricas u otros efectos causados por corrientes tierra. El la figura 3, que es vista en la sección 2.1.6 que hace referencia a Requisitos del NEC, se muestra el secundario del transformador ubicado cerca del equipo de procesamiento de datos; el secundario se conecta a

tierra en un punto único y los equipos se conectan este punto, que puede estar ubicado en el transformador o en un tablero secundario.

En muchos casos el fabricante de los equipos electrónicos especifica un sistema “dedicado” a tierra, esto se refiere al sistema denominado tierra aislada, aclarado anteriormente. En sus instrucciones de instalación del sistema incluye diagramas para la conexión de los sistemas de tierra; la “tierra de seguridad” y la “tierra aislada” aunque solo incluyen una sola terminal eléctrica de conexión, en el chasis del equipo. Esta única terminal incluida en el equipo del fabricante es común para los circuitos de tierra (tierra de seguridad y tierra aislada) si ambos conductores se de estos dos sistemas se conectaran a esta terminal la conexión de “Tierra Aislada” se perdería completamente.

La tierra aislada es la tierra de referencia cero para la lógica digital y la mantiene libre de ruidos eléctricos. El propósito es mantener los equipos eléctricos sensibles y protegidos de los ruidos eléctricos producidos en los bucles de tierra y múltiples conexionas a tierra.

El calibre del cable es decisivo para los modernos circuitos electrónicos. El conductor de “Tierra del sistema” debe ser continuo, de calibre completo, con aislamiento y forro aislante color verde.
Cuando el forro aislante de color verde se usa para la tierra de seguridad, debe utilizarse aislamiento color verde con rayas amarillas para la “tierra del sistema”. Un solo “Calibre” significa un conductor de cobre de un calibre mínimo AWG #8 o del mismo calibre que los conductores portadores de corriente.

Los conductores de conexión a tierra especificados por el NEC pueden ser tan pequeños como 1/11 de la capacidad de los conductores de fase. La utilización de un conductor de conexión a tierra, de calibre adecuado y uniforme, aislado, separado y dedicado, puede aumentar el calibre del conducto y el costo del trabajo, pero es el

único método aceptable para asegurar la confiabilidad y el funcionamiento del moderno equipo electrónico computarizado.

2.1.5 Selección de calibre de cable.

La especificación del voltaje de neutro-tierra, que establece un voltaje inferior a 2 voltios pico a pico, puede ser difícil de obtener. Este voltaje resulta de la corriente que fluye en el conductor neutro y es el producto de ella y de la resistencia del alambre. El balance adecuado de las cargas polifásicas reducirá la corriente en el neutro.

La resistencia conocida de los alambres de cobre y aluminio la proporciona la tabla 9 del NEC[17], las unidades de resistencia en esta tabla son en ohms por cada 300 metros de alambre. Para calcular el calibre real del conductor neutro y lograr la especificación de 2 voltios de pico a pico, neutro-tierra, dados los factores de ajuste de voltaje del 80%, se puede utilizar la formula siguiente, esta es una formula empírica para el calculo aproximado del conductor neutro, y que se usa junto con la tabla 9 del NEC.

$$R = 1000 \div (I_{cb} \times L_m)$$

En donde:

L_m = Longitud máxima del alambre (en pies)

Icb = Capacidad de corriente de disparo para el interruptor de circuito.

R = Resistencia del conductor neutro en ohms por 300 metros de alambre

En el siguiente ejemplo se aplican estas herramientas para seleccionar el calibre del neutro: En un escenario se necesita seleccionar el cable neutro para un sistema

[17] Ver Sección de Anexos Tabla 9 NEC

computarizado que debe ubicarse a 20 m del tablero de distribución más cercano. Calculando el calibre del conductor neutro requerido para un circuito de 20 amperes, usando la formula dada anteriormente.

$$R = 1000 \div (Icb \times Lm) = 1000 \div (20 \times 65)$$
$$= 0.77 ohms / 30 m (1000 pies)$$

Usando los valores dados en la tabla 9-Z del código, efectiva en 0.85 PF, y utilizando un conducto de acero, seleccionamos un conductor AWG #8 o uno de aluminio del #6. Los conductores de aluminio no ofrecen seguridad en calibres menores de #4 dentro de un edificio, así que seleccionaremos un conductor de cobre de #8.

2.1.6 Requisitos del NEC

Las normas del Código se aplican por razones de seguridad, por ello es muy importante considerarlas en los ambientes de instalaciones de computadoras. El cumplimiento de ellas tendrá un efecto positivo en la operación del equipo, lo que no asegura de ninguna manera una instalación libre de ruido eléctrico, el cual causa un mal funcionamiento del sistema.
El ruido eléctrico es cualquier voltaje o corriente presente en un conductor, o un circuito, que no es la señal eléctrica deseada.

En todo tipo de instalación eléctrica para equipo computarizado es muy recomendable instalar un sistema derivado separadamente para la alimentación eléctrica [secciones 250-20(d) y 250-30]. Una “instalación de equipo computarizado” se refiere a cualquier instalación de computadoras o equipos electrónicas con base en microprocesadores. La figura siguiente muestra dos métodos para instalar un sistema derivado separadamente con el fin de proteger los equipos electrónicos en una sala de computadoras.

En este tipo de instalaciones en importante el control de la energía eléctrica y el ruido eléctrico, la temperatura del ambiente y la humedad.

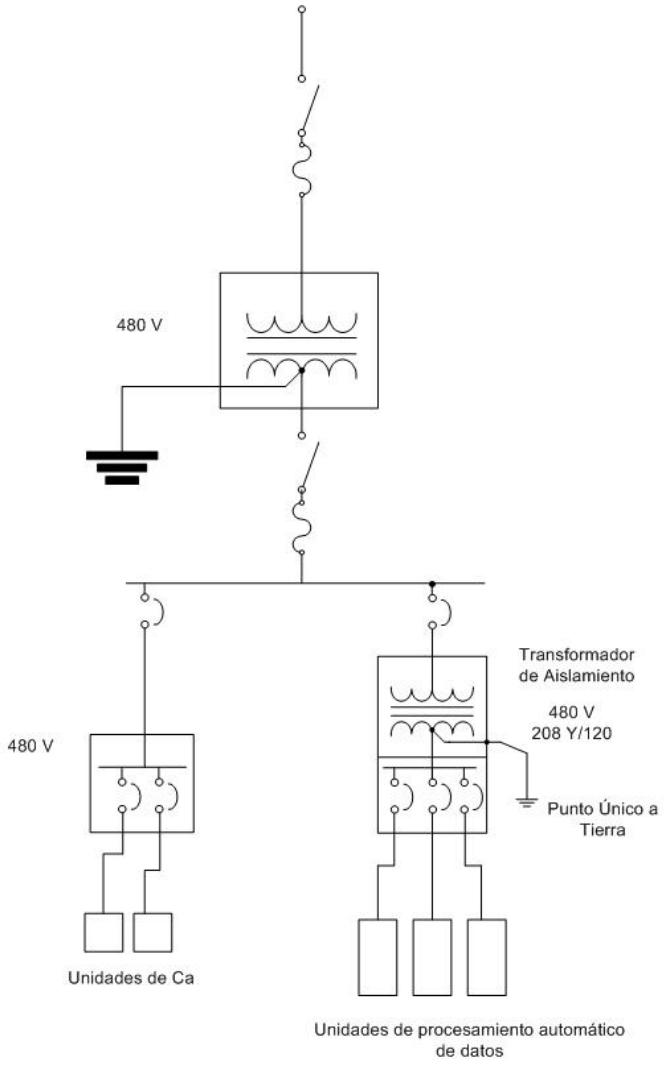


Fig. 2.3 Conexión básica aceptable para equipos de procesamiento de datos.

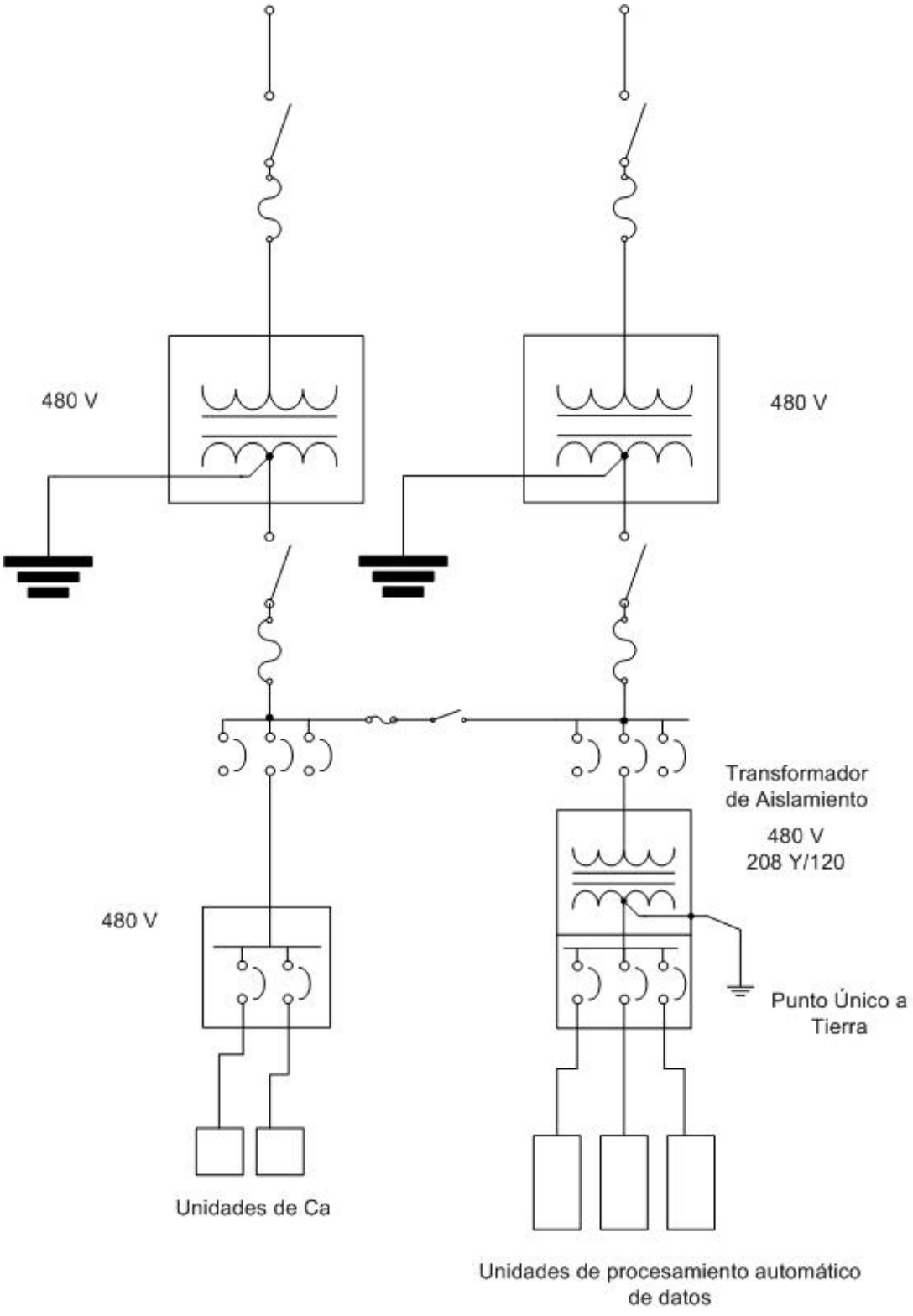


Fig. 2.4 Conexión optima aceptable para equipos de procesamiento de datos.

2.1.7 Dispositivos de tratamiento para las líneas que tienen conexión a tierra.

Cada instalación de ambiente computarizado debe recibir energía de su propia transformador dedicado, el cual debería, bajar el voltaje de 480 voltios de servicio trifásico, al clásico voltaje de una computadora, 208 y 120 voltios, sin embargo el transformador puede ser del tipo elevador o de una relación uno a uno, si es requerido, y el voltaje de salida debe concordar con los requerimientos del equipo. También puede ser simplemente un transformador de aislamiento que proporciona solo rechazo de cómo común y aislamiento ca.

Si se requiere, este transformador puede tener un blindaje Faraday para la atenuación de ruido en modo común, lo mismo que ser de voltaje constante para una mejor regulación de voltaje, o puede tener un acondicionador de ruido. La razón primordial de uso del transformador es proporcionar una fuente separada de energía en el punto más cercano posible al equipo y aislada de otras fuentes de energía del edificio. A continuación una figura de cómo es la mejor configuración para el equipo.

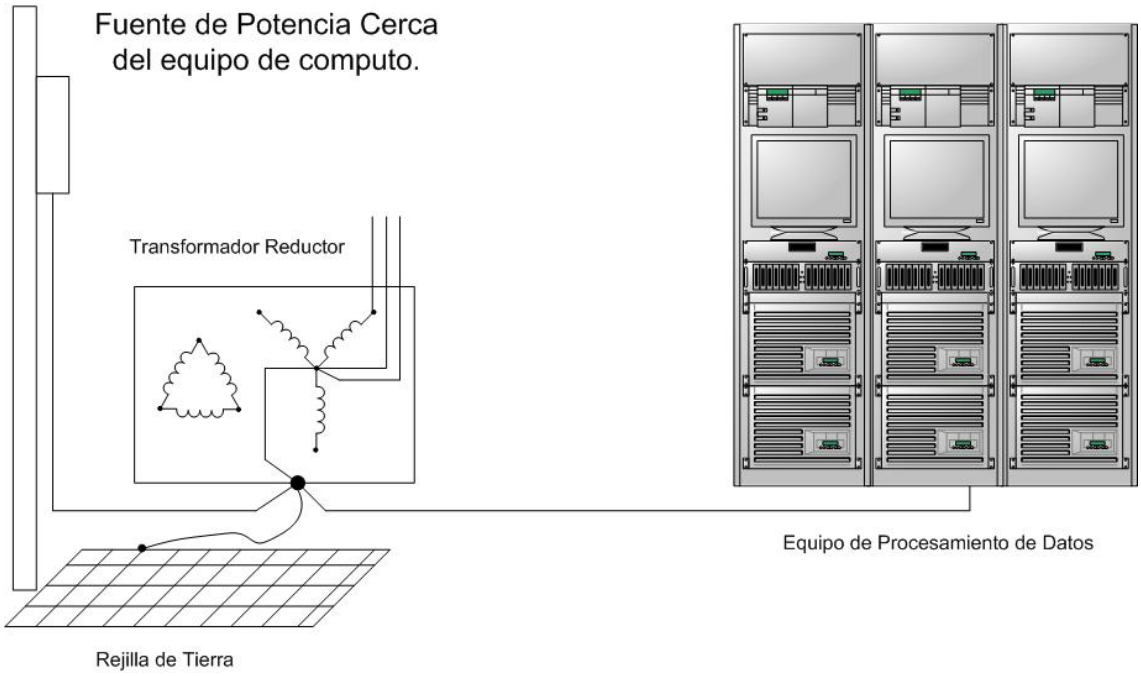


Fig. 2.5 Conexión en diagrama basico-equematico, que representa la protección hacia los equipos informáticos.

Un “Transformador dedicado” con aislamiento blindado, núcleo ferrorresonante y con derivación electrónica conmutada, es considerada como una fuente derivada separadamente y debe conectarse a tierra conforma a la sección 250-30 del NEC.

Un puente de unión, debe conectar la barra neutro, o la terminal X_0 del secundario del transformador, a los conductores de conexión de tierra o a la barra colectora de conexión a tierra. El calibre de este puente de unión no debe ser menor que el calibre del conductor del electrodo de tierra de la tabla 250 – 66 del NEC.

El conector conectado a tierra o la barra colectora neutro debe conectarse al sistema de electrodo de tierra del edificio con un “Conductor de electrodo de tierra”, calibrado de acuerdo con la tabla 250-66.
La sección 250-30(a) (3) establece que “el electrodo a tierra o de puesta a tierra” estará localizado tan cerca como sea posible y preferiblemente en la misma área donde el conductor de puesta a tierra se conecta al sistema.

El electrodo de tierra debe ser una barra de metal, efectivamente conectado a tierra, el cual forma parte de la estructura, de acuerdo a las secciones 250-50 y 250-52.

Si todos los elementos metálicos, soportes, de la estructura, tubería, refuerzos y rejillas de tierra están conectados entre si como lo establecen las secciones 250-50 y 250-52, esta configuración se convierte en el “sistema de electrodo de tierra”

2.2 Infraestructura de piso, paredes y techo.

2.2.1 Infraestructura de Piso, Generalidades.

Los pisos elevados en cuarto de servidores son muy importantes para todo centro de datos basados en la alta disponibilidad de la información, y con muy buena razón.

Para muchas instituciones, la presentación de su centro de servidores es una de las partes importantes de la infraestructura de la información.

Los cuartos de servidores y de datos sin los pisos elevados pueden ser percibidos como adaptados a condiciones muy limitadas o con menos intenciones de aprovechar todas las ventajas de las infraestructuras civiles alcanzables para el manejo de recursos que puede llegar a demandar una sala de datos.

El suelo elevado dentro del cuarto de servidores es desarrollado para proporcionar el siguiente:

- Un sistema de la distribución para el aire acondicionado frío.
- Pistas, conductos, y/o ayudas para cableado de datos.
- Conductos para Cableado de la energía eléctrica
- Espacio para una rejilla de tierra de cobre para poner a tierra del equipo.
- Una localización para evacuar el agua u otro tipo de tubería necesaria.

Las necesidades del aire acondicionado frío y de la distribución de energía contribuyen a la utilidad y reconocimiento de pisos elevados. Los operadores de estos centros de datos y el sitio del servidor son tomados en cuenta al momento de escoger el mejor diseño ya que se valora la flexibilidad que es proporcionada por los sistemas levantados del piso. Con respecto a requisitos de energía, el número de los circuitos por metro cuadrado, los centros de datos de hoy son mucho mayores que en el pasado. En la mayoría de los casos, es más fácil instalar y mantener los circuitos debajo del piso que los tradicionales de pared o techo. Aunque, una tendencia reciente es utilizar cableado de energía y datos como parte del sistema del gabinete. Esto reduce con eficacia las cantidades del cable a utilizar cuando de cuenta con una estructura de piso levantado, de tal modo que permite mayor espacio abierto dedicado a la distribución del aire. En pisos generales, elevados en el sitio del servidor es una opción fiable y práctica de diseño para la mayoría de las instalaciones.

2.2.1.2 Infraestructura de Piso, Diseño

Los pisos elevados en la mayoría de los centros de datos utilizan un patrón de la circulación de aire en el cual las corrientes de aire se refresquen y se calienten en un ciclo continuo de la convección. Bajo este ciclo de circulación de aire se requiere una configuración de piso elevada que forme un plano del suministro de aire. Una unidad de CRAC[18] empuja el aire caliente hacia la tapa, refresca el aire, y lo descarga debajo del piso. Los pisos elevados miden típicamente 18 pulgadas (46 centímetros) a 36 pulgadas (91 centímetros) del piso original del edificio hasta la tapa de los azulejos del piso elevado, que son apoyados por una estructura puesta a tierra por una rejilla.

Fig. 2.6 Fotografía de sección de piso elevado donde contiene espacios de ventilación, conducción de cableado y compartimiento de mantenimiento de soportes en vértices.

La presión estática del plano empuja el aire hacia arriba a través de los azulejos perforados del piso para refrescar los estantes. La mayoría de los salones de equipos, hace circular el aire frío de la fuente desde abajo y el aire caliente es evacuado por los extractores hacia afuera generado por la parte posterior de los estantes. Idealmente, el extractor de aire caliente se levanta al techo y vuelve a lo

[18] Aire Acondicionado de Cuarto de Computadores, por sus siglas en ingles, monitor y preservador de la temperatura en una sala de equipo informático. Ver Glosario Anexo.

largo de este de nuevo a los cierres de las unidades de CRAC para repetir el ciclo. Muchos centros de datos tradicionales arreglan filas de estantes en frente - posterior para no contribuir a la pronta mezcla de aire e ineficiencia del mantenimiento de la temperatura dentro de la habitación. El mezclarse del aire frío y caliente en los pasillos es muy ineficaz y pierde recursos y energía que se refrescan valiosos. Mientras que esta disposición puede trabajar con densidades de energía y cargas de calor más bajas, como el aumento de la densidad de energía y de la carga de calor, las temperaturas de la entrada del equipo comenzarán a levantarse (demostrado en la figura anterior) y a sobre calentar recursos críticos.

2.2.2 Infraestructura de Pared, Generalidades.

Al menos dos de las paredes del cuarto deben tener laminas de plywood de 20 Milímetros de espesor y de 2.4 metros de alto. Las paredes deben ser suficientemente rígidas para soportar equipo de comunicaciones y gabinetes para el mismo tipo de equipos, además de no permitir ningún tipo de ventilación natural como ventanas o aberturas no especificadas como ajenas al flujo de aire acondicionado. Las paredes deben ser recubiertas con pintura resistente al fuego, lavable, mate y de color claro para optimización de la iluminación dentro del recinto, que tiene que ser clara y no generadora de calor; para cumplimiento de esto con lámpara fluorescentes acorde al área decidida para la sala de datos.

2.2.3 Infraestructura de Techo, Generalidades.

Las características de techo interior, para un cuarto de servidores, según consulta realizada a proveedores de mantenimiento de equipos informáticos, se debe reflejar una sola cubierta sin ningún tipo de división de cielo falso o similares, únicamente las aberturas de iluminación selladas con el mismo material para dar uniformidad a la placa superior, esto con la intención que no se genere entrada de polvo de partes superiores de espacios entre el cielo falso y la parte sólida de la infraestructura del edificio. En el caso de que exista la posibilidad de filtración de líquidos sobre el cuarto de datos, debe instalarse una cubierta impermeabilizante de varias capas para absorber o desviar cualquier indicio de permeabilidad hacia el recinto.

2.3 Ubicación Física, Generalidades.

En esta sección tratamos los aspectos físicos de la ubicación de la unidad servidor, incluyendo las razones para la existencia de un cuarto dedicado a servidores y equipos que procesan datos, generalidades sobre lo que un cuarto de servidor debe contener, puntos dominantes al planear un cuarto del servidor, una lista de comprobación de instalación y algunas razones qué hace una instalación eficiente.

2.3.1 Ubicación Física, Aspectos de dimensionamiento por características de servidores.

En una instalación de solo uno o pocos servidores, se puede obtener gran beneficio de un cuarto dedicado a equipos de estas características. Estos pocos servidores pueden producir un ruido intolerable y una carga termal extra en un ambiente normal de oficina, además de las preocupaciones serias de seguridad que se presentan de un servidor desprotegido que sea fácilmente accesible por personas que transitan en la zona ya sean pertenecientes o no a la institución que utiliza el servidor.

Una configuración de varios servidores excede rápidamente el nivel de ruidos tolerable en un ambiente de oficina. Además, tal configuración de servidores impondrá una carga térmica substancial. Esta tipo de fenómenos generados por los equipos de procesamiento de datos dedicado es manejada más fácilmente por un cuarto dedicado con el aire acondicionado especializado y control de acceso directo donde requerir autenticación personalizada por cada ingreso de personal, permite que se restrinja el acceso y que se guarde un registro de los ingresos al área de los equipos dedicados al procesamiento de los datos.

Un cuarto de servidores contendrá generalmente no solamente a la configuración de servidores si no también discos, dispositivos de reserva, cables de interconexión, ventiladores y otro tipo de equipo relacionado a partes del correcto funcionamiento de la solución informática.

Aunque la administración de los servidores puede ser realizada remotamente, tiene sentido proporcionar una consola local dentro del cuarto de los servidores, permitiendo que los administradores realicen mantenimiento y la administración localmente.

2.3.2 Ubicación Física, Aspectos determinantes al escoger la ubicación física final.

Todos estos requerimientos deben ser ubicados dentro de una estructura que sea diseñada para poder brindar un ambiente adecuado de seguridad, temperatura y recursos que demandan estos equipos informáticos. Por ello brindarle un espacio seguro dentro de la infraestructura civil tiene un alto nivel de importancia, ya que la localización física del cuarto de servidores es crítica y debe tener prioridad para la localización del espacio cuando es posible.

Con sus requisitos del tamaño del centro de datos a disposición, explorar una posición que se considera para el cuarto, son los aspectos horizontales y verticales dentro de la infraestructura del edificio. Su localización se debe también situar centralmente en todos los ejes, esto reducirá al mínimo costos y longitudes de cableado a través del edificio.

Además se debe intentar permanecer alejado de los niveles del sótano y del piso superior, donde se corre el riesgo de inundación y de goteos o filtraciones de respectivamente ya sea por precipitaciones naturales o tuberías existentes en el edificio. Los cuartos de servidores deben de adecuarse las paredes exteriores para ejercer mejor control de la temperatura y de la humedad interna, especialmente si tienen ventanas, dado sea el caso es recomendable eliminarlas. Además de buscar locaciones que permitan el crecimiento del área superficial del cuarto de equipos informáticos.

Es primordial evitar las áreas adonde las tuberías funcionan directamente sobre el techo del cuarto del servidor, o las ubicaciones donde está arriba un cuarto de baño en el piso siguiente. Considere el redireccionar algunas vías de tuberías en caso necesario de riesgo de filtración no controlada. Asimismo, evite los sitios del edificio con alto tráfico peatonal, por razones de seguridad física de accesos y no considere ubicar su cuarto de equipos informáticos cerca del pasillo principal, del área de alimentación o de la otra área público accesible.

Debe de explorase las áreas adyacentes al cuarto del servidor y buscar los espacios alejados del funcionamiento de cableado eléctrico por problemas que pueden generar campos eléctricos o magnéticos grandes tales como ejes del elevador.

2.4 Consideraciones ambientales.

2.4.1 Consideraciones Ambientales, Generalidades

El número de proveedores de aire a temperatura adecuada, a instalar en cada local será un promedio de 2, lo cual puede variar por las dimensiones del cuarto de servidor o bien para garantizar que en caso de avería solo se estropee el 50%.
Estos locales están destinados a contener máquinas y no personas, por tanto se debe evitar la presencia de las mismas por espacios de tiempo prolongados. La mejor forma de resolver esto por diseño, es calibrar los termostatos de estos locales a una temperatura de 17ºC, que es ideal para minimizar tanto la fatiga mecánica como electrónica de los equipos, al tiempo que es lo suficientemente hostil como para garantizar la no presencia humana por espacios prolongados.
Al impulsar el aire frío por el falso suelo, permite distribuir frío mediante rejillas a los servidores en la granja de servidores y a los armarios con electrónica en el RP, por esta razón la distribución de la canalización por la que discurren los cables de datos y alimentación eléctrica, será perimetral en forma de U, ubicando los climatizadores en la abertura de la U. El acabado del suelo técnico será estanco, de tal modo que permita mantener el aire a sobre-presión debajo del mismo, que actuará como canalización de impulsión.

2.4.2 Consideraciones Ambientales, Área Superficial necesaria.

El cuarto del servidor debe contar con la suficiente área física disponible para sostener las piezas del servidor y permitir que se den cambios físicos de equipos, de acuerdo a las necesidades que la institución vaya sufriendo, con respecto a demanda de recursos informáticos. Incluyendo cambios en aire acondicionado y corriente eléctrica. El cuarto debe también tener espacio para equipo de reemplazo, tal como tarjetas adicionales de comunicación, ventiladores, discos para almacenamiento de datos y cintas para respaldo de datos. Al estimar incorrectamente estos requisitos de este tipo de habitaciones y sus funciones esperadas, podría forzarle mover una

instalación de servidor a un nuevo cuarto, lo que significa una interrupción seria en el servicio de datos para la compañía.

Ese movimiento también genera costos directos e indirectos; éstos incluyen los costos directos de adquirir, de construir, aprovisionamiento el nuevo cuarto del servidor y los costos indirectos que se presentan cuando el servidor en estado operativo o almacenaje restringido limitan el trabajo eficientemente y la capacidad de producción de la institución que se traduce responder con ineficacia a los usuarios.

Es importante que los medios de almacenaje y los contenedores de datos de respaldo no sean almacenados dentro del cuarto de servidores.

2.4.3 Consideraciones Ambientales, Ubicación de Datos de Respaldo.

Un incendio podría dañar el hardware y las medias de almacenamiento, haciendo el ejercicio de copias de respaldo totalmente inútil. Las copias de respaldo de los datos deben ser fuera del sitio operativo de los servidores, almacenado en gabinetes o cajas fuertes resistentes al fuego.

Cerciórese de que la energía que apoya el cuarto del servidor sea suficiente para las aplicaciones de hoy no justas pero para el crecimiento futuro en el servidor. Es penique sabio y libra absurda escatimar en correctamente equipar el cuarto del servidor. Tenga en cuenta la suficiente iluminación y enchufes eléctricos múltiples; hacer la esta derecha hace el mantenimiento y los realces más simples. Puede ser necesario equipa el cuarto del servidor del aire acondicionado dedicado de guardar el equipo del recalentamiento. Además, el equipo del servidor es sensible a la calidad del aire, así que es sabio asegurar la limpieza del edificio, que puede implicar el instalar de los filtros de aire.

2.5 Autonomía Eléctrica de Cuarto de Equipos.

2.5.1 Autonomía Eléctrica, Generalidades.

Los cortes de energía eléctrica planificados o no, interrumpen los servicios que brinda un cuarto de equipos de procesamiento de datos, centralizado para una comunidad de estudios superiores, así como los servicios y procesos administrativos y académicos llevados a cabo por las dependencias ubicadas dentro del campus.

El sistema eléctrico de respaldo permitirá la alimentación de las cargas esenciales para el funcionamiento de todos los equipos esenciales para el procesamiento de la información, por un tiempo limitado de tiempo mientras se incorpora la fuente auxiliar de suministro conformada por una planta eléctrica independiente de la fuente de suministro normal.

Esto podría obligar a interrumpir los servicios corporativos como correo, página Web, sistema de consultas, entre otros, así como el acceso a Internet para el resto de institución, debido a cortes de energía eléctrica prolongados y no planificados que afectan a la misma. Por esto es necesario contar con una independencia eléctrica que le brinde una alternativa de alimentación para dar continuidad a los servicios.
Esta situación implica un gasto significativo en el presupuesto que se plantea en este documento con la intención de cubrir todos los requerimientos de un cuarto de equipos debe reunir, para su funcionamiento optimo, caso contrario afectaría la productividad y rendimiento al interrumpir todas las actividades académicas, administrativas y de extensión. Adicionalmente, el efecto negativo sobre los servicios y procesos influye en una pérdida de la imagen corporativa de la Institución ante los estudiantes, grupos sociales y privados que se tienen puesta la atención en la entidad.

2.5.2 Lineamientos de la Autonomía Eléctrica para cuarto de equipos.

Como se mencionaba en el apartado 2.5.1 la planificación, análisis e implementación de un sistema ininterrumpido de energía eléctrica, basado en un generador eléctrico por combustión, sugiere una extensión muy amplia para ser incluida como una sección de esta GRT, por ello brindamos los lineamientos y objetivos que se deben perseguir al momento de desarrollar esta necesidad critica.

Basándonos en los siguientes objetivos ineludibles podemos definir una clara justificación, recursos necesarios y resultados esperados que variaran de la situación actual.

2.5.2.1 Objetivos de la autonomía eléctrica para cuarto de equipos.

- Asegurar la disponibilidad de los servicios informáticos brindados por el centro de datos en un 99.99%.
- Proteger la plataforma tecnológica de los cortes de electricidad no planificados.
- Asegurar la continuidad de los servicios que ofrece el cuarto de equipos y todas las necesidades de procesamiento y consulta de información.
- Cumplir con los requerimientos de seguridad y prevención de incidentes relacionados a la falta de energía eléctrica dentro de la habitación de las computadoras.

2.5.2.2 Situación Actual

En el Capitulo I “Solución Informática” por el momento, los servicios informáticos son asegurados en caso de corte de energía eléctrica, cualquiera sea su causa, por la existencia de un equipo UPS, de 50kVA, con autonomía de unas 45 minutos aproximadamente, Sin embargo, la experiencia del comportamiento del servicio

eléctrico nacional, nos indica que una cantidad considerable de los cortes supera este período de tiempo.

2.5.2.3 Situación Deseada.

Se requiere que los servicios informáticos de todo tipo, brindados por la institución de educación superior, por medio de su CE, tengan disponibilidad los 365 días del año y que ante un eventual o planificado corte del servicio de suministro eléctrico sea capas de mantener las aplicaciones que se están utilizando, credenciales de usuarios que usan el sistema en la actualidad y la capacidad de crecimiento necesaria para soportar, con parámetros de calidad adecuados, inclusión de nuevos servidores al CE, equipos desarrolladores de las aplicaciones, sistemas administrativos, sistemas de Control de estudio, educación a Distancia, Servicios de bibliotecas digitales, mensajería, bases de datos, y usuarios que se incorporan en el mediano y largo plazo.

Para ello es necesaria la transición desde la plataforma actual hacia una plataforma mejorada que cumpla como mínimo los siguientes criterios:

2.5.2.4 Justificación autonomía eléctrica para una institución de educación superior.

Una institución de educación superior con el animo de cumplir su rol social, de formación intelectual, producción de conocimientos, facilitación y guía, búsqueda de soluciones a los problemas sociales, mediador entre las teorías predominantes del saber y su aplicación práctica en las actividades humanas, debe contar con una plataforma de apoyo adecuada que brinde todas las herramientas necesarias para facilitar la ejecución de dichas tareas.

La implementación de una plataforma tecnológica confiable y robusta, soportada en las Tecnologías de Información, con garantía de funcionamiento adecuado a las necesidades de obtención, procesamiento y producción de conocimientos, necesaria para la realización de sus actividades básicas dentro de la sociedad, permitirá a la institución de educación superior el cumplimiento de su misión y visión.

2.5.2.5 Experticia inicial, definición de demanda energética y posibles etapas del proyecto de autonomía eléctrica.

Para la primera etapa se requiere de la asesoría de expertos a fin de obtener el informe técnico de la evaluación y cálculo de las cargas esenciales, llevar a cabo el levantamiento de la información, realizar la ingeniería conceptual y básica para el diseño de los sistemas eléctricos y la fuente auxiliar de suministro eléctrico y las memorias descriptivas. Con este informe técnico se puede diseñar la licitación para el suministro e instalación del sistema de generación de emergencia.

Etapa 1: Evaluación y cálculo de cargas esenciales de las instalaciones, ingeniería conceptual y básica necesarias para el diseño de los sistemas eléctricos, ingeniería conceptual y básica necesarias para el diseño de una fuente auxiliar de suministro de energía eléctrica conformada por una planta generadora accionada por combustión interna. Incluyendo ubicación, sistema de transferencia automática, sistema generador, protecciones, especificaciones de reserva de combustible y tiempo de autonomía, insonorización y manejo de escapes de la combustión. Informe técnico para la implantación del proyecto.

Etapa 2: Implantación del proyecto mediante las obras civiles y eléctricas requeridas para la instalación y puesta en marcha de la planta eléctrica, su reserva de combustible y otros componentes.

La forma recomendada para la contratación de los recursos es por medio de licitación publica o con proveedores invitados basados en las experiencias demostradas para con la universidad en ocasiones pasadas.

2.5.2.6 Productos y Servicios de autonomía eléctrica para el Cuarto de Equipos.

En conclusión, se puede concluir que los productos que deben resultar de este proyecto son:

1. Memoria descriptiva de la instalación eléctrica propuesta.
2. Memoria de cálculos y mediciones.
3. Memoria de tablas de cargas esenciales: críticas y de emergencia.
4. Memoria de especificaciones de suministro e instalación de materiales y equipos y de construcción de obras eléctricas y civiles asociadas.
5. Diagrama con el sistema de acometidas propuestas y de la planta de suministro propuesta.
6. Cómputos métricos con estimación de costos por suministro de materiales y equipos.
7. Suministro e instalación de una planta eléctrica accionada por combustión interna y su reserva de combustible.
8. Obras civiles y eléctricas asociadas a la instalación.
9. Sistema de sonorización y manejo de escapes de la combustión.

En conclusión, el resultado que se busca de este proyecto es que, una vez instalado el sistema de alimentación de emergencia y puesto en marcha, asegurará que los servicios informáticos que se derivan en, administrativos y corporativos ofrecidos, sean prestados ininterrumpidamente, lo cual se traduce, en un ahorro significativo en el presupuesto de la institución de educación superior, optimización de la resolución de peticiones de procesamientos o consultas de información y mejora en la calidad de la educación que ofrece la institución.

CAPITULO III. Determinación de conceptos de Rack, Estructura de Cableado cuarto de Servidores y dispositivos de interconexión de comunicaciones.

3.1 Generalidades de Gabinetes para equipo de procesamiento de datos.

3.1.1 Características de diseño de gabinetes para equipo de procesamiento de datos.

La construcción y diseño de un rack está limitada principalmente por el peso que debe soportar. Además, se suelen situar sobre falsos suelos, que también tienen limitación en el peso que pueden soportar. Generalmente se fabrican en acero o en aluminio. Algunos modelos incorporan una puerta frontal de cristal. Útil para evitar que se accione el equipamiento por accidente. Otros tienen una bandeja extraíble de 1U donde se aloja un teclado y un monitor TFT abatible.

En algunos casos el rack esta encerrado en un armario con puerta de cristal, además de tener ventilación/refrigeración, con eso se consigue aislar el ruido que puedan provocar.

3.1.2 Estándares de Gabinetes para equipos informáticos.

Dentro de los gabinetes para equipos informáticos y de comunicaciones, tenemos dos estándares que son descritos en la normativa EIA. Existe los gabinetes de 19 pulgadas y los estándares para terremotos.

3.1.2.1 Gabinetes de 19 Pulgadas

La Asociación de Industrias Electrónicas (EIA[19] por sus siglas en ingles) estableció el estándar EIA-310 para asegurar compatibilidad física entre los estantes, los estantes encapsulados, y el equipo diseñado para montarse en estantes.

[19] Electronics Industries Association. (EIA)es una organización comercial nacional que incluye el espectro completo de los fabricantes de los E.E.U.U. La asociación es una sociedad de asociaciones y de las compañías electrónicas y de alta tecnología que misión está promoviendo el desarrollo de mercado y la competitividad de la industria de alta tecnología de los E.E.U.U.

La principal intención del estándar es asegurar compatibilidad y flexibilidad dentro del centro de datos.

EIA-310 define la unidad del estante (U) a ser el espacio vertical usable para un pedazo de equipo montado en estante. La U es igual a 1.75 pulgadas o 4.445 cm. Si un estante se describe para ser 10U, significa que hay un espacio vertical interior físico de 17.5 pulgadas de disponible para el montaje del equipo.

Fig. 3.1 Imagen de definición de 1U. Equivalente a 4.445 cm. Y espacio utilizable dentro de un gabinete.

EIA-310 se utiliza por todo el mundo para el equipo diseñado para ser montado en estante de 19 pulgadas.

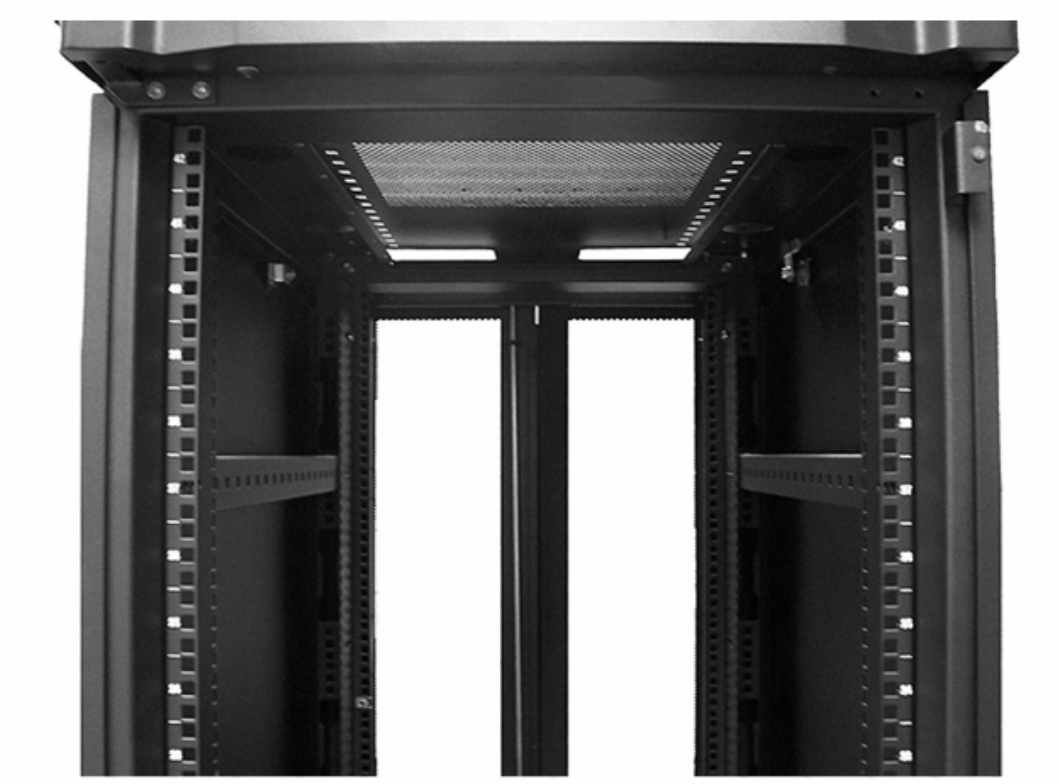


Fig.3.2 Gabinete de 42 U, con paneles frontales, puertas traseras y refuerzos antisísmicos, gabinete tradicional en la región centro americana.

Hay varios tipos de carriles de montaje verticales para el equipo estándar. Éstos incluyen las perforaciones rectangulares para las tuercas (prisioneras) de la “jaula” y las tuercas del clip, o los agujeros redondos, con o sin hilos de rosca.

Fig.3.3 Tuercas prisioneras especiales para gabinetes de equipos informáticos para el montado de la estructura y servidores que van desde 1 U hasta 5 U.

El estándar de 19 pulgadas, define las dimensiones importantes para los estantes, los encapsulados, y el equipo para montado en estante.

Por ejemplo, EIA-310 define la abertura mínima de la estructura entre los carriles esta debe ser de al menos 450 milímetros (17.72 pulgadas). Para proveer el espacio adecuado para los equipos de medida para chasis de gabinete.

La anchura entre los centros de los agujeros de montaje del equipo es 465 ± 1.6 milímetros (18.31 pulgadas ± 0.063). cada una de las medidas seguidas del ± indican los posibles márgenes de error que son admisibles para poder montar los equipos de manera segura.

La anchura mínima del recinto para proporcionar la separación para los paneles delanteros del equipo y las placas frontales de los biseles es 483.4 milímetros (19 pulgadas).
En la siguiente figura se indican precisamente las medidas y puntos de inicio y fin de estos datos.

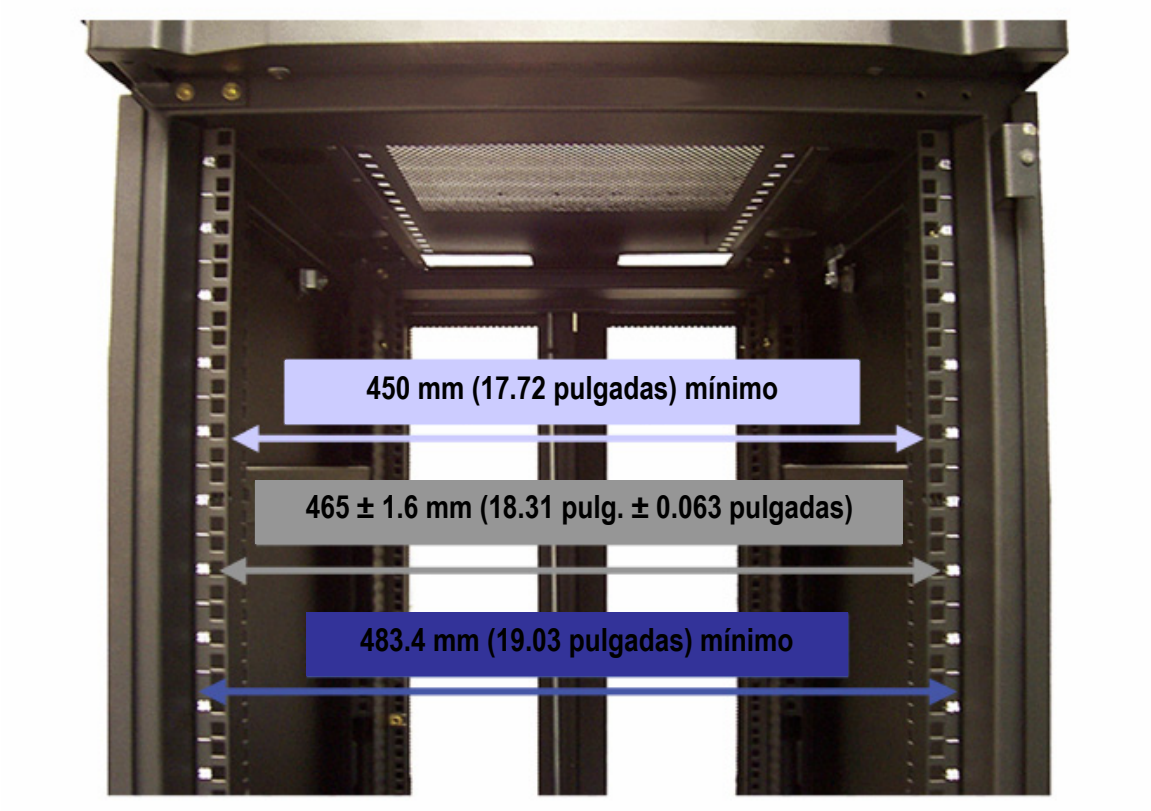


Fig.3.4 Medidas interiores y exteriores de Gabinete de 42 U, con sus márgenes de error permitidos por la norma EIA 310

La mayoría de los gabinetes encapsulados ahora utilizan perforaciones rectangulares y las tuercas de la jaula, aunque las diferentes necesidades de las instituciones o empresas requieren los agujeros roscados o no roscados a través de los agujeros rectangulares.

Las perforaciones rectangulares más comunes con las tuercas de la jaula soportan varios tamaños y tipos del hilo de rosca. Si los hilos de rosca de una tuerca de la jaula sufren daños, la reparación es tan fácil como sustituir la tuerca de la jaula. Ya que la tuerca de la jaula “flota” en su montaje, la tuerca tiene cierta libertad de moverse, lo que hace la alineación de la tuerca y del perno más fácil. La tendencia para los estantes abiertos del marco, es haber roscado los agujeros. Hay muchos tamaños del hilo de rosca, pero #12-24 es el tamaño más común del hilo de rosca. La ventaja principal de los agujeros roscados puestos directamente en

el estante es que el despliegue es rápido, puesto que no hay tuercas de la jaula a la instalación.

3.1.2.2 Gabinetes de con estándar para terremotos.

El código de edificio uniforme (UBC[20] por sus siglas en ingles) y Eurocode especifican cómo los recintos se deben empernar al piso en localidades donde hay un riesgo elevado para los terremotos.
El sistema de elaboración para equipo de red (NEBS[21]) y los estándares europeos del instituto de los estándares técnicos (ETSI) tienen requisitos más rigurosos que el UBC y el Eurocode, especifican anclar al piso los gabinetes y las estructuras reforzadas del marco para los recintos.

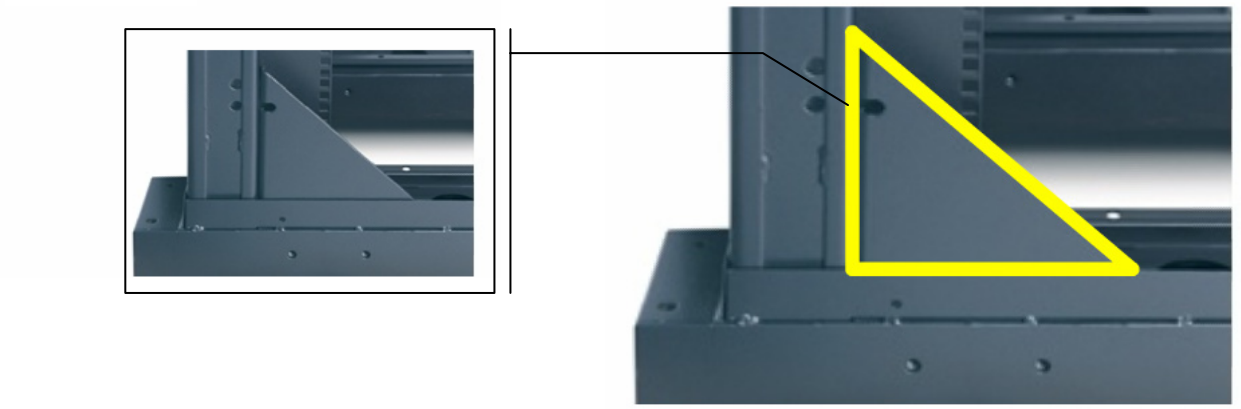


Fig. 3.5 Refuerzo inferior de soporte para protección contra sismos, para brindar más solidez al gabinete que contiene equipo informático definido en la norma EIA 310

A Continuación se muestran las imágenes de un gabinete diseñado para la prevención de daño al equipo en una zona sísmica. Los gabinetes con estándares para terremotos, se refuerzan especialmente con la intención de proteger el equipo

[20] **El consejo internacional de código**, una asociación dedicada a la seguridad de edificios y la prevención de incendios, desarrolla códigos usados para construir edificios residenciales y comerciales, incluyendo hogares y escuelas. La mayoría de las ciudades, los condados y los estados de los E.E.U.U. que adoptan códigos eligen los códigos internacionales desarrollados por el consejo internacional del código.
[21] **Network Equipment Building System**, NEBS es un sistema de requisitos técnicos con un propósito básico: para hacer los interruptores de la red a prueba de balas. El estándar fue desarrollado internamente en los laboratorios de Bell.

contra terremotos. En dirección a certificar la seguridad del equipo y del personal, las instalaciones sísmicas del recinto deben conformarse con los estándares regionales, tales como NEBS o ETSI. La mayoría de los centros de datos y de telecomunicaciones que no están en zonas del alto riesgo, utilizan estándares menos rigurosos como el UBC o el Eurocode, más bien que los estándares más terminantes del NEBS o de ETSI [22].

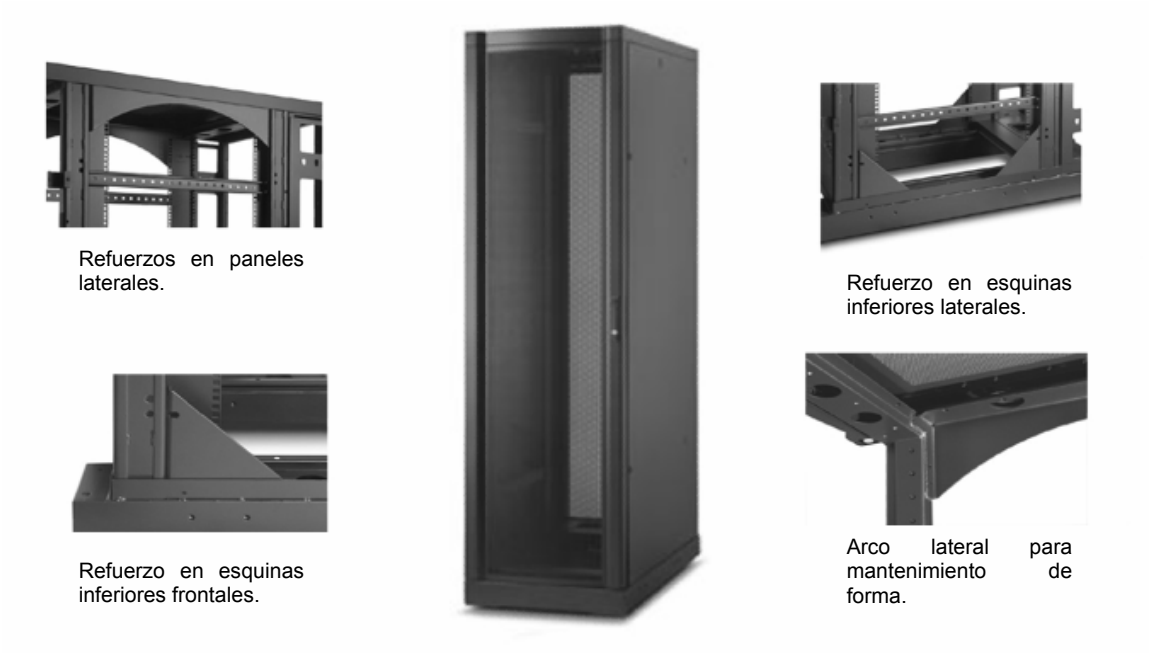


Fig. 3.6 Gabinete con múltiples refuerzos laterales para protección contra sismos.

3.1.2.3 Gabinetes Abiertos: 2 postes y 4 postes.

El estante abierto existe en dos tipos básicos: Dos postes y Cuatro postes.

El marco de dos postes es usado como un estante que tiene la capacidad de sostener equipo que puede ser montado delantero o de centro.
Se utiliza típicamente para los equipos no pesados en ambientes de TI.

[22] **European Telecommunications Standards Institute** (ETSI) o Instituto Europeo de Normas de Telecomunicaciones es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

A pesar que el gabinete de dos postes tiene un relativamente precio bajo, no ofrece ningún tipo de seguridad, ningún control en la circulación de aire, capacidad baja de carga de peso y estabilidad baja.

Dependiendo del fabricante, los accesorios comunes que el estante puede incluir son las bandejas, organizadores verticales de cable, soportes para la distribución de energía, y los kits que permiten que varios estantes sean ensamblados juntos.

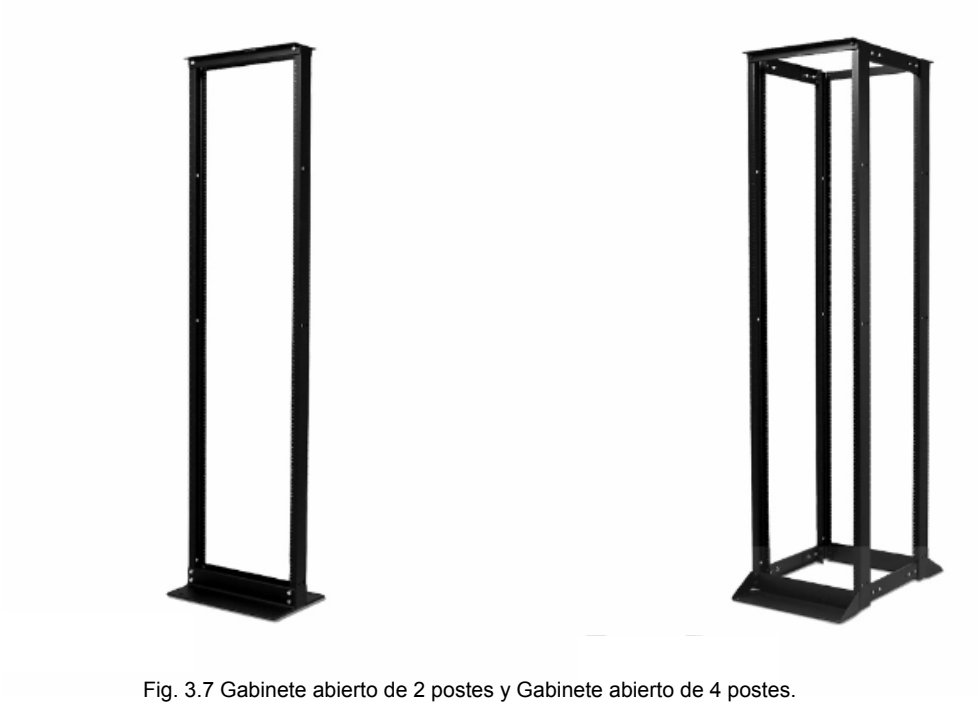


Fig. 3.7 Gabinete abierto de 2 postes y Gabinete abierto de 4 postes.

El marco de cuatro postes permite que el equipo sea apoyado del frente y de la parte posterior, haciendo una opción más versátil que el marco de dos postes.

Se utiliza típicamente para servidores, el establecimiento de una red, y los usos de la telecomunicación en ambientes de TI. La ventaja obvia del gabinete de cuatro postes es que es físicamente más fuerte que el marco de dos postes y puede apoyar un equipo más pesado. Dependiendo del fabricante, los accesorios comunes del estante pueden incluir bandejas ligeras y resistentes, organizadores verticales del cable, los soportes para la distribución de energía, y los kits que permiten la agrupación con otros estándares.

3.1.2.4 Ventajas y Desventajas de Gabinetes abiertos.

Los gabinetes abiertos tienen la ventaja de permitir de fácil acceso al equipo, y pueden ser montados sencillamente por el propietario. Son también de bajo costo y de solución económica.

Las desventajas significativas de Gabinetes abiertos son:

- No proporcionan la protección física de la seguridad.
- Se expone materialmente el equipo.
- No permiten una circulación de aire optimizada en una configuración de alto-calor-producido de equipos de procesamiento de datos o comunicaciones.

El gabinete abierto otorga a la convección natural para disipar calor del equipo. A medida la densidad de equipos aumenta en el estante, la convección natural tiene una capacidad limitada de retirar el calor que necesita ser disipado. Los recintos, acondicionados con los aspectos discutidos en el capitulo anterior, se obtienen medios mejorados para controlar y de manejar la circulación de aire.

3.1.2.5 Gabinetes Cerrados

Estos Gabinetes están dentro de los sistemas de estantes más avanzados en su desarrollo para la contención de equipos informáticos. Como lo muestra la siguiente figura, existen diversas variedades de diseños básicos de gabinetes. Sin embargo, la mayoría de estos Gabinetes incluyen las puertas delanteras y traseras, paneles laterales, y un techo.

En un gabinete cerrado se crean conductos para obligar al aire a pasar a través de los equipos montado en estantes de este tipo. Estos conductos proporcionan una mayor capacidad de refrigeración del aire en comparación de los gabinetes abiertos.

Fig. 3.8 Gabinetes Cerrados para Equipo Informático, Para pared y Gabinete para equipos de telecomunicaciones.

Dependiendo del fabricante, el gabinete puede tener opciones para manejo de: cableado, unidades de distribución de energía, dispositivos de protección de energía, dispositivos de refrigeración, sistemas de gestión ambiental, y otros accesorios.

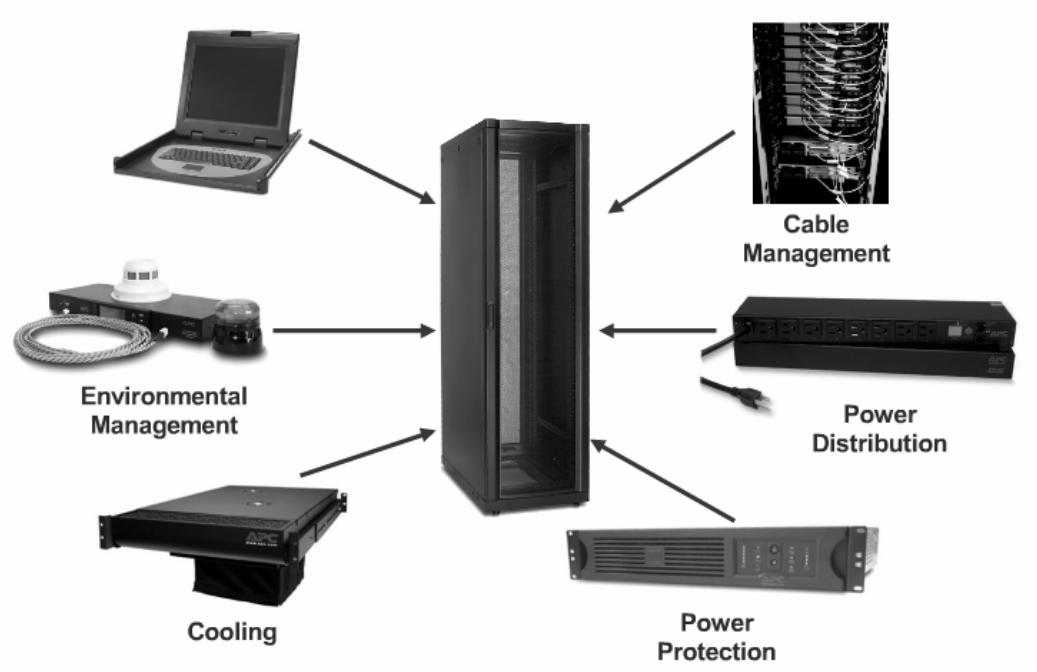


Fig. 3.9 Gabinetes Cerrados para Equipo Informático, Accesorios de Gabinete para enfriamiento.

3.1.2.6 Gabinete Abierto – Gabinete Cerrado, Comparación.

En comparación con el Gabinete Abierto, los Gabinetes Cerrados ofrecen una mejor capacidad de carga estática, refrigeración, seguridad y la compatibilidad de varios proveedores en los equipos diseñados para ser montados en gabinetes.

	Precio por unidad	Capacidad estática de carga	Refrigeración	Seguridad física para equipos	Compatibilidad con marcas de equipos.
Gabinete Abierto	Baja	Baja	Baja	Baja	Baja
Gabinete Cerrado	Alta	Alta	Alta	Alta	Alta

Tabla 3. Comparación de características de gabinetes.

Los servidores para aplicación normalmente son montados en gabinetes de 42U de altura, 600mm de amplio y 1070mm de profundidad. Los Gabinetes cerrados se han ido innovando más profundos en apoyo para la más alta densidad de potencia y el cableado que demanden los equipos. Algunas de las aplicaciones y configuración de cableado de alta densidad, combinan switches de red con el arreglo de servidores, el equipo, o la una distribución de enfriamiento lateral en lugar de la tradicional frente hacia el fondo. Esas disposiciones requieren gabinetes que son más amplios que los 600mm.

3.1.2.7 Disponibilidad

La disponibilidad de los recursos informáticos tienen como base principal el contenedor físico que le permita la optimización de todas las ventajas que estos

equipos nos puedan brindar. Los problemas más comunes que constituyen un desafío para la optimización de la disponibilidad son los siguientes:

- La insuficiencia de un adecuado flujo de aire, daña los equipos informáticos en gabinete. Este problema ha aumentado en los últimos años con el aumento exponencial de las densidades de calor. Y es importante señalar que no existe una norma para medir la eficacia de refrigeración al comparar los recintos.

- Inadecuada redundancia de energía en el Gabinete. La solución es llevar dobles vías de potencia eléctrica para equipos informáticos que demandan energía por un solo o dobles cables de poder.

- La falta de seguridad física por control humano. Debido a la cada vez mayor demanda para proporcionar suficiente aire, de energía eléctrica, y los datos de bastidores, el número de personas acceder a recintos para tareas de servicio ha aumentado, dejando a las unidades informáticas más vulnerables a error humano. Los Gabinetes necesitan estar físicamente asegurados con puertas de cierre de cerradura y paneles laterales con la misma medida, para impedir el acceso no autorizado o accidental.

- Incumplimiento de los requisitos sísmicos. La solución es que todos los Gabinetes que estén ubicadas en una zona altamente sísmica como lo es nuestro país debe estar en conformidad con las normas de construcción sísmica descritas en esta sección.

3.1.2.8 Plan de Piso

Por último, las consideraciones físicas y de diseño para Gabinete son muy importantes en el diseño de un centro de datos. Los Gabinetes deberían organizarse en los pasillos, de forma alterna: caliente y fría.

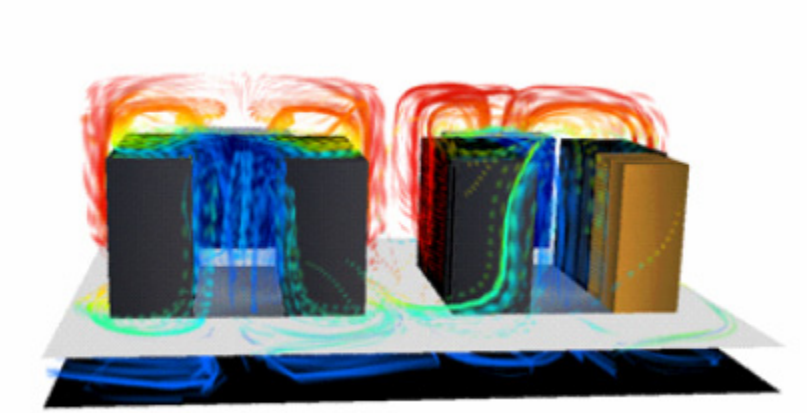


Fig. 3.10 Flujo de Aire en cuarto de servidores con múltiples Gabinetes, con diseño de piso elevado y sus cambios de temperatura.

Al elegir un Gabinete, es importante seleccionar a los aspectos que funcionan bien con los cálculos de diseño. Esta ilustración muestra un diseño óptimo de frío pasillos que son cuatro pies de ancho, caliente y pasillos que son tres pies de ancho.

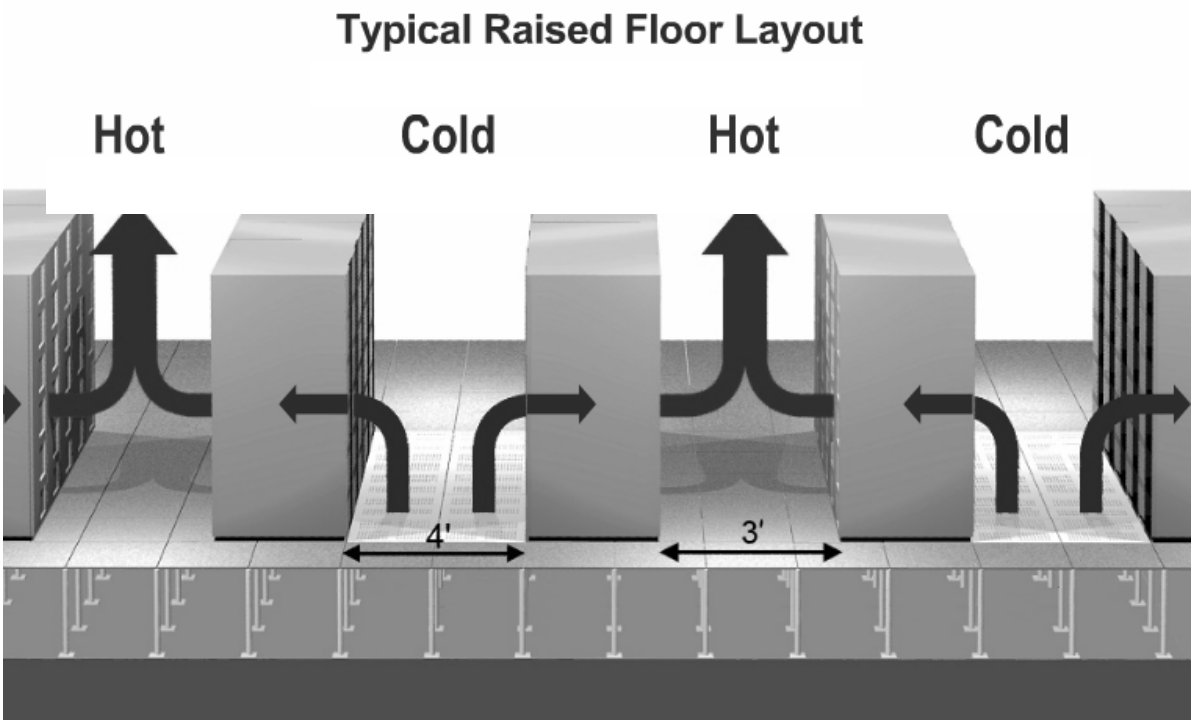


Fig. 3.11 Flujo de Aire en cuarto de servidores con múltiples Gabinetes, con diseño de piso elevado y sus cambios de temperatura.

3.2 Generalidades de Cableado para cuarto de Servidores.

Desde una perspectiva de costo, la construcción y operación de un centro de datos representa una importante pieza de cualquier presupuesto de tecnología de la información. La clave para el éxito de cualquier centro de datos es el diseño y la ejecución de los principales componentes críticos de la infraestructura. El cableado de infraestructura, en particular, es un área importante a considerar en el diseño y la gestión de cualquier centro de datos.

La infraestructura de cableado abarca todos los cables de datos que forman parte del centro de datos, así como la totalidad de los cables de energía necesarias para garantizar a todos la disponibilidad de la energía eléctrica. Es importante tener en cuenta que los canales contenedores de cable y los dispositivos para cables, son fundamentales para el apoyo de la infraestructura de TI, ya que ayuda a reducir el riesgo de tiempo de inactividad debido a un error humano y el sobrecalentamiento.

Ethernet[23] ha sido el protocolo de comunicaciones de datos estándar durante muchos años. Junto con Ethernet, algunas de las tradicionales prácticas de cableado de datos para seguir la forma cómo se despliegan de cables de datos.

- Alta velocidad de datos de cableado de más de cableado de cobre es un medio de elección.

- Cables conectados a ordenadores y placas de pared es muy común en los centros de datos.

[23] **Ethernet** es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI

3.2.1 El RJ45 es la opción de conector del cable de datos.

La funcionalidad dentro de los cables de datos y de los equipos asociados, ha experimentado grandes cambios. Sin embargo, el aumento de las velocidades de datos ha obligado a muchos cambios físicos. Cada vez que un nuevo y más rápido estándar sea ratificado por los órganos de normalización, el cable y el apoyo de los equipos electrónicos, se ha rediseñado para apoyarla. Nuevas herramientas de prueba de los instrumentos y procedimientos también dan seguimiento a cada nuevo cambio en la velocidad. Estos cambios han sido requeridos principalmente por el más nuevo y versiones más rapidas de Ethernet, que son impulsados por las necesidades de más velocidad de los clientes y mas ancho de banda. Cuando se habla de esto, es importante tener en cuenta los usos y las diferencias de los dos cables de fibra óptica y cable de cobre tradicionales.

3.2.2 Cableado de Cobre

El cableado de cobre se ha utilizado durante décadas en los edificios de oficinas, centros de datos y otras instalaciones para proporcionar la conectividad. El cobre es un medio confiable para la transmisión de información a través de distancias más cortas; Pero su rendimiento es sólo garantiza hasta 100 metros entre los dispositivos.

Fig. 3.12 Cable de Cobre libre de cubierta, barniz natural para uso industrial.

El cableado de cobre, que se utiliza para la conectividad de la red de datos, contiene cuatro pares de cables trenzados, a lo largo de la longitud del cable. El trenzado es fundamental para el correcto funcionamiento del cable. Si estos pares estuvieran desenredados, el cable se hace más susceptible a interferencias.

Cables de cobre vienen en dos configuraciones:

- Sólidos. cables de proporcionar un mejor rendimiento y son menos susceptibles a interferencias que son la mejor opción para su uso en un entorno de servidor.

- Trenzado. Los cables son más flexibles y menos costosos, y por lo general sólo se utilizan en la construcción del Patch Cord.

De cableado de cobre, Cables de Red, y los conectores se clasifican sobre la base de sus características de rendimiento y para que las aplicaciones que se utilizan normalmente.
Estas clasificaciones, llamadas categorías, se puntualizan en la TIA / EIA 568 Commercial Building Telecommunications Writing Standard.

3.2.3 Fibra Óptica

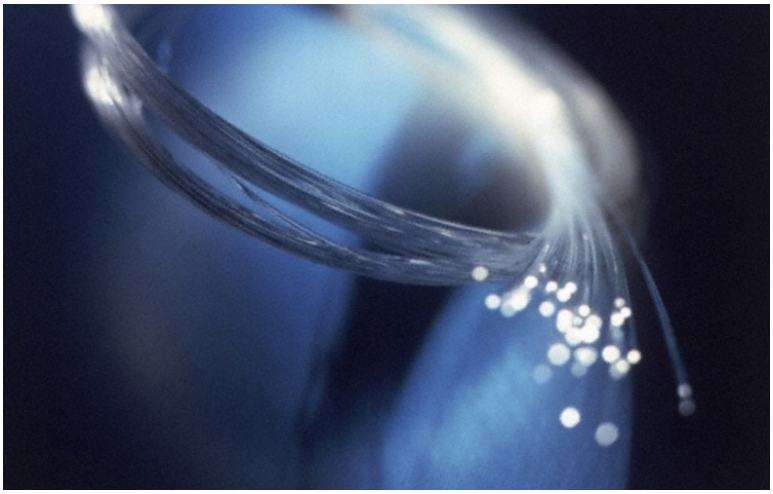


Fig. 3.13 Fibra óptica, transmisión de datos basada en as de luz a través de su refractante materia.

El cable de fibra óptica es también un muy eficaz medio para proporcionar conectividad. Este consta de cinco elementos. La parte central del cable, conocido como el núcleo, es una delgada línea de pelo de vidrio capaz de llevar la luz. Este núcleo está rodeado por una fina capa de vidrio ligeramente más pura, llamada revestimiento, que contiene y refracta la luz. El Núcleo y revestimiento de vidrio están cubiertos por una capa de plástico para protegerlos de polvo o rasgaduras. Fortaleciendo las fibras se agregan a proteger el núcleo durante la instalación. Por último, todos estos materiales son envueltos en plástico o de otro tipo de protección sustancia que sirve como cable de la cobertura general.

Una fuente de luz, parpadeando miles de millones de veces por segundo, se utiliza para transmitir datos a lo largo de un cable de fibra. Los componentes de fibra óptica tienen la labor de convertir las señales electrónicas en señales de luz y viceversa. La luz viaja por el interior del vidrio, refractando dentro de la vaina continuamente y hacia adelante hasta que llega al otro extremo del cable y es vista por el equipo receptor.

Cuando la luz pasa de un medio a otro transparente, desde el núcleo de vidrio a los materiales de revestimiento, la luz se dobla. Un cable de fibra de revestimiento se compone de un material diferente dependiendo de los fabricantes es decir en términos técnicos, tiene un índice de refracción diferente, que dobla la luz de vuelta hacia el centro. Este fenómeno, conocido como total de reflexión interna, mantiene la luz en movimiento a lo largo de un cable de fibra óptica para grandes distancias, incluso en caso de que el cable sea curvo. Sin el revestimiento, la luz se fuga.

En el cableado de fibra puede manejar conexiones de una distancia mucho mayor que el cableado de cobre, 80.5 kilómetros efectivos o más en algunas configuraciones. Dado que la luz se utiliza para transmitir la señal, los límites superiores de, hasta qué punto una señal puede viajar a lo largo de un cable de fibra, se relaciona no sólo con las propiedades del cable, sino también a la capacidad y la ubicación relativa de los transmisores.

Además de la distancia, el cableado de fibra tiene varias ventajas sobre los de cobre:

- La Fibra proporciona velocidades de conexión más rápida.

- La fibra no es propensa a interferencias eléctricas o vibración.

La fibra es más delgada y ligera de peso, por lo que más de cableado puede encajar en el mismo paquete de tamaño limitado o espacios pérdida de señal más de la distancia es menor a lo largo de fibra óptica de cable de cobre.

El cobre es en generalmente la solución de cableado menos costoso sobre distancias mas cortas, es decir la longitud de las filas servidor de centro de datos), mientras que la fibra es menos costoso para distancias más largas (es decir las conexiones entre los edificios en el campus).

3.2.4 Prácticas de instalación de cableado.

Algunas de las mejores prácticas para el cableado de datos incluyen:

3.2.4.1 Despliegues superiores.

Cables aéreos que se encuentran en grandes paquetes deben resguardarse en bandejas de cable o cubiertas. Si el fabricante de los cobertores para cable indica el radio de curvatura máximo para su deformación para curvatura del cable se debe comprobar entonces que no presione más el empaque de envolturas u otros dispositivos de ahorcamiento. Ya que puede interferir con el rendimiento del cable.

3.2.4.2 Despliegue Subterráneo.

Ser consciente en la cobertura del cable especial ya que es posible que el cable, sea sometido a humedad normal por esta alojado bajo el piso y en zona oscura, además de verificar el radio de curvatura según las especificaciones del fabricante y adherirse estrictamente a ellas. No presionar de más de empate que envuelve. Esto puede interferir con el rendimiento del cable.

3.2.4.3 Prueba de los cables

Hay varios fabricantes de los equipos de ensayo para prueba de cables, diseñados específicamente para evaluar las redes de alta velocidad. Asegúrese de que el instalador pruebe y certifique cada uno de los conectores y puntos de red internos. Un administrador de centro de datos puede solicitar un informe que muestra los resultados de la prueba.

Cuando se realiza el diseño y la instalación de la red local se debe tener cuidado especial de ruta todos los Unshielded Twisted Pair,UTP es estándar de los EE.UU. o Shielded Twisted Pair, STP es la norma europea, estos cables deben estar lejos de las posibles fuentes de interferencia, como las Líneas centrales eléctricas, motores eléctricos de iluminación o de las luces superiores generales.

3.2.1 Determinación de Capacidad a instalar.

La capacidad a instalar, en materia de conexión, resulta ser uno de los factores que nos permitirán brindar el servicio Web, con eficacia y alta calidad, siempre y cuando esta solución planteada, obedezca a una visión de crecimiento, que siempre resulta ser el comportamiento normal en este tipo de soluciones de comunicación, tanto en solicitudes al servidor, como numero de usuarios que busca utilizar los servicios.

3.2.2 Proyección de crecimiento de conexiones.

La proyección de crecimiento de las conexiones hacia un servidor Web, puede ser censado fácilmente por herramientas que se nos proporcionan hoy en día, de tipo software. Como Web Sense, ISA Server 2007, etc.

Esta proyección obedece a un análisis que debe efectuarse en diferentes capas de estudio.

Estudiantes Universitarios.

Por medio de estadísticas que se manejan en el departamento de asesoría académica y proyección estudiantil, se puede estimar la cantidad de alumnos inscritos en la institución y que por ende están habilitados a realizar consultas vía Web de al menos 3 tipos: Consulta informativa, uso de servicios Web basados en SMTP o SOAP†, y Consultas de descarga de archivos.

Comunidad Universitaria.

Usuarios potenciales también lo son, los miembros de la comunidad universitaria, tanto docentes como personal administrativo, esto con el fin de ser ellos los generadores de la gran mayoría de información que debe ser proporcionada por la institución de educación superior, con el fin de la educación de los alumnos. Además de considerar la administración de las

† Nombres de Servicios Web, estos servicios se ven con mayor detalle en el Capitulo IV Sección 6.3 de este documento. “CAPITULO VI. Seguridad Virtual, Administración de Seguridad y Servicios de aplicaciones Web”

materias vía Web, recepción de tareas, entrega de materiales y toma de pruebas evaluadas.

Publico general.

Además de controlar los accesos internos de la comunidad universitaria y los mismos estudiantes, se debe considerar la proyección de visitas diarias a un sitio Web de la institución, para determinar los correctos anchos de banda a contratar, ya que por parte de este segmento, se da la mayor consulta informativa que se registrara.

Bajo las consideraciones de estos segmentos, se puede establecer la proyección a contratar, pero antes debe tenerse las cantidades mas exactas de consultas de todos los tipos, para determinar horas pico de consulta, espacio en discos, motor de base de datos, y otros aspectos críticos de seguridad para proveer la correcta plataforma de comunicaciones necesarias.

3.2.3 Normativas que rigen el cableado para datos.

Las diferentes normativas internacionales de cableado estructurado, han sido creadas y diseñadas para facilitar los diseños de solución de transporte de datos, tanto en infraestructuras civiles, como en coberturas internacionales en enlaces de datos. Todo esto bajo un concepto de optimización de la solución y costo controlado dentro de la mejor adaptación de diseño para las necesidades que asumamos.

A continuación un detalle de las normativas actualmente vigentes que regulan el espacio de cableado estructurado.

ANSI/EIA/TIA-568-A DOCUMENTO PRINCIPAL QUE REGULA TODO LO CONCERNIENTE A SISTEMAS DE CABLEADO ESTRUCTURADO PARA EDIFICIOS COMERCIALES.

Esta norma reemplaza a la EIA/TIA 568 publicada en julio de 1991.
El propósito de la norma EIA/TIA 568-A se describe en el documento de la siguiente forma:

Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multi producto y multi fabricante. También proporciona directivas para el diseño de productos de telecomunicaciones para empresas comerciales.

El propósito de esta norma es permitir la planeación e instalación de cableado de edificios comerciales con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad. La instalación de sistemas de cableado durante la construcción o renovación de edificios es significativamente menos costosa y desorganizadora que cuando el edificio está ocupado.

La norma EIA/TIA 568-A especifica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables
- El rendimiento de los componentes
- Las tomas y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 km
- Un espacio de oficinas de hasta 1,000,000 m2
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- Voz
- Datos
- Texto
- Video
- Imágenes

ESTÁNDAR ANSI/TIA/EIA-569 PARA LOS DUCTOS, PASOS Y ESPACIOS NECESARIOS PARA LA INSTALACIÓN DE SISTEMAS ESTANDARIZADOS DE TELECOMUNICACIONES

Este estándar reconoce tres conceptos fundamentales relacionados con telecomunicaciones y edificios:

- Los edificios son dinámicos. Durante la existencia de un edificio, las remodelaciones son más la regla que la excepción.
- Este estándar reconoce, de manera positiva, que el cambio ocurre.
- Los sistemas de telecomunicaciones y de medios son dinámicos. Durante la existencia de un edificio, los equipos de telecomunicaciones cambian dramáticamente. Este estándar reconoce este hecho siendo tan independiente como sea posible de proveedores de equipo.
- Telecomunicaciones es más que datos y voz. Telecomunicaciones también incorpora otros sistemas tales como control ambiental, seguridad, audio, televisión, alarmas y sonido. De hecho, telecomunicaciones incorpora todos los sistemas de bajo voltaje que transportan información en los edificios.

Este estándar reconoce un precepto de fundamental importancia: De manera que un edificio quede exitosamente diseñado, construido y equipado para telecomunicaciones, es imperativo que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

Esta norma se refiere al diseño especifico sobre la dirección y construcción, los detalles del diseño para el camino y espacios para el cableado de telecomunicaciones y equipos dentro de edificios comerciales.

ANSI/EIA/TIA-606 REGULA Y SUGIERE LOS METODOS PARA LA ADMINISTRACION DE LOS SISTEMAS DE TELECOMUNICACIONES.

El propósito de este estándar es proporcionar un esquema de administración uniforme que sea independiente de las aplicaciones que se le den al sistema de cableado, las cuales pueden cambiar varias veces durante la existencia de un edificio. Este estándar establece guías para dueños, usuarios finales, consultores, contratistas, diseñadores, instaladores y administradores de la infraestructura de telecomunicaciones y sistemas relacionados.

Para proveer un esquema de información sobre la administración del camino para el cableado de telecomunicación, espacios y medios independientes. Marcando con un código de color y grabando en estos los datos para la administración de los cables de telecomunicaciones para su debida identificación. La siguiente tabla muestra el código de color en los cables.

- NARANJA Terminación central de oficina
- VERDE Conexión de red / circuito auxiliar
- PURPURA Conexión mayor / equipo de dato
- BLANCO Terminación de cable MC a IC
- GRIS Terminación de cable IC a MC
- AZUL Terminación de cable horizontal
- CAFÉ Terminación del cable del campus
- AMARILLO Mantenimiento auxiliar, alarmas y seguridad
- ROJO Sistema de teléfono

TIA/EIA TSB-67 ESPECIFICACIÓN DEL DESEMPEÑO DE TRANSMISIÓN EN EL CAMPO DE PRUEBA DEL SISTEMA DE CABLEADO UTP

Este boletín especifica las características eléctricas de los equipos de prueba, métodos de prueba y mínimas características de transmisión del UTP en categorías 3, 4 y 5.

TIA/EIA TSB-72 GUIA PARA EL CABLEADO DE LA FIBRA OPTICA

Este documento especifica el camino y conexión del hardware requerido para el sistema de cableado de fibra óptica y equipos localizados dentro del cuarto de telecomunicaciones o dentro del cuarto equipos en el área de trabajo.

3.3 Generalidades de Enlaces de comunicación de datos para servidores Web

Los enlaces de comunicación, es la parte mas importante a cumplir, en el objetivo a colocar a disposición la información de una institución de educación superior y que esta pueda accederse desde cualquier lugar, ya que por medio de ellos conseguiremos efectuar consultas de muchos tipos, a continuación los aspectos a considerar al seleccionar la provisión de conexión para un servidor.

3.3.1 Tipos de Conexiones de datos para enlaces internacionales.

Los servicios de enlace internacionales o IPL (Internacional Private Line) como se conocen, se proveen por medio de las Redes MPLS[24] de Datos. Esta es una red robusta que permita la integración de protocolos de comunicación sobre una sola plataforma, haciendo esto transparente la transmisión de datos, voz o video sobre una red.

[24] **MPLS** Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

3.3.1.1 Medio de transmisión y conexión física

Las redes o infraestructuras de Fibra Óptica serán utilizadas para brindar las interconexiones locales en cada país. Es decir, esto nos permite tener la capacidad de ampliación de los enlaces de forma casi inmediata al ser solicitada por ustedes.

3.3.1.2 Plataforma de la Red de Datos

La interconexión de las redes privadas de cada país se realiza a través de la red MPLS de Datos. Dentro de la red multi servicio MPLS se crea una red privada exclusivamente para los solicitantes del enlace. Un proveedor será el encargado de asociar los accesos de la oficina principal y las unidades remotas a esta red privada MPLS. Luego de haber hecho esta asociación, de ninguna manera, un acceso de la red privada del solicitante podría intercambiar algún tipo de información con otra red privada de la red MPLS. Esto se logra a través del etiquetamiento particular que la red hace a los diferentes accesos. Esta etiqueta es colocada o eliminada de los paquetes IP que entran o salen de la red MPLS.

Con este método de etiquetamiento en ningún punto de la red, el contenido de información IP que el cliente envía es analizada, ya que dentro de la red, el enrutamiento de tráfico se hace con base a etiquetas y no a la dirección IP, por lo tanto la información que se envía viaja segura sobre la red.

3.3.2 Recomendación de Anchos de Banda y proveedores de servicios de enlaces de datos.

Actualmente en el país, existen múltiples proveedores de este servicio, pero entre los cuales podemos destacar dos:

Proveedor	Ancho de Banda		Recomendación
	Mínimo	Máximo	
NAVEGA.COM Tel.(503)2507-0733 Cel.(503)7930-7774 Centro Financiero Gigante Nivel 9 Torre "A" Alameda Roosevelt y 63av. Sur San Salvador El Salvador	**256 kbps**	**T1**[†]	★
AMNET DATOS Teléfono 2252.8024 Teléfono: (503) 2236-8000 e-mail: infosv@amnetcorp.com	**256 kbps**	**T1**	

Se recomienda introducir un ancho de banda no menor a un **E1**, que lleva datos en una tasa de 2048 millones de bits por segundo (Mbps) y puede llevar 32 canales de 64 Kbps * cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos en SS7 o Sistema de Señalización Número 7 (tambien denominado CCS). En R2 (o CAS) el canal 16 se usa para señalización por lo que están disponibles 30 canales para voz o datos. E1 lleva en una tasa de datos algo más alta que el T-1 (que lleva 1544 millones de bits por segundo) porque, a diferencia del T-1, no hace el bit-robbing y los ocho bits por canal se utilizan para cifrar la señal. E1 y el T-1 se pueden interconectar para uso internacional.

3.3.3 Seguridad en Comunicación de datos para servidores Web.

La seguridad en cada una de las comunicaciones establecidas para nuestra información, debe ser un aspecto crítico al momento de poner a disposición información de cualquier índole, pero que lleve la etiqueta de oficial por una institución de educación superior, ya que representa, en muchas ocasiones las intenciones educativas y el rumbo en materia académica que intenta transmitir la

[†] El sistema del T-Portador, introducido por Bell System en los Estados Unidos en los años 60, fue el primer sistema acertado que soportó la transmisión de voz digitalizada. La tasa de transmisión original (1,544 Mbps) en la línea T-1 es comúnmente usada hoy en día en conexiones de Proveedores de Servicios de Internet

institución. Por ello basándonos en las siguientes recomendaciones, procuramos establecer el marco de seguridad para la transmisión de la información por via de las telecomunicaciones.

3.3.3.1 Seguridad en Comunicación de datos para servidores Web, Generalidades.

Propiciar un sitio virtual para los clientes de una institución educativa superior, que contenga una vasta y renovada información sobre la entidad educativa, que sea practico y de gran aporte de información educativa, todo esto disponible las 24 horas del día y desde cualquier punto del planeta. Todo esto se vuelve una ventaja competitiva de alto rendimiento y eficiente al momento de brindar una opción más de recuso educativo de gran espectro.
Teniendo en cuenta que la naturaleza de la información que se trasmite en una red local de datos que tiene acceso dedicado a Internet es considerada de tipo sensible, ya que se concede acceso a información de estados educativos de alumnos y datos que los catedráticos crean para fines educativos, información administrativa de toma de decisión y datos que autentican a usuarios, estos datos deben ser manejados con niveles de seguridad altos para evitar una falla en la seguridad y una posible fuga o un uso no adecuado de estos registros.

Además de ofrecer a las figuras importantes de esta institución, así como a los alumnos, una opción segura, confiable y eficiente de acceso a la red privada de datos, desde la Internet, se vuelve una herramienta más, que facilitara el trabajo de todos los que tengan a disposición esta ventaja.

Es por ello que se incluye esta sección dentro del análisis informático de Infraestructura de TI y arquitectura de Red a proponer como anexo a la solución informática propuesta, donde se considera aislar la red local del resto de la Internet,

por medio de ISA[25] Server, proveer de un servidor seguro para el alojamiento del sitio Web de la institución y finalmente aprovechar el potencial de la nueva infraestructura de red con la inclusión de un enlace de Internet dedicado.

3.3.3.2 Objetivos de seguridad de servidor Web integrado a red local.

El objetivo principal al momento de diseñar un perímetro de seguridad para red es habilitar un servidor Web apto para alojar el sitio virtual de la institución educativa, y proveerle de todos los servicios de comunicación necesarios para su correcto desempeño al ser consultado, sin antes tomar todas las medidas de seguridad contempladas en los detalles específicos del aislamiento de la red, al tener un enlace internacional a Internet, por medio de una DMZ[26] para el control de acceso de usuarios no pertenecientes al dominio local y extrayendo del enlace a Internet, la herramienta de conexión de una VPN[27] para accesos a usuarios con altos privilegios.

Para un mayor detalle del nivel de seguridad que se recomienda podemos ver aspectos de manera puntual.

- Proveer del medio principal de comunicación para el servidor Web que alojara el sitio Web de la institución.

- Diferenciar el tipo de solicitudes de consulta de datos desde las redes externas ó Internet, por medio del filtrado de tipo de consulta para determinar el direccionamiento adecuado hacia el servidor que provee la prestación sin tener que acceder a la red local para realizar una consulta de información.

---

[25] ***Internet Security and Acceleration*** es un firewall de stateful packet inspection, es decir, analiza el encabezado de los paquetes IP y de application layer, analizan la trama de datos en busca de tráfico sospechoso. Adicionalmente, ISA Server es un firewall de red, VPN y web cache como contenedor de sitios web.

[26] **DMZ** ***(del inglés DeMilitarized Zone)*** o Zona Desmilitarizada. En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

[27] **VPN** Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

- Recomendar la configuración de una VPN para permitir acceso remoto a usuarios pertenecientes al dominio y que puedan gozar de los privilegios que la red local les brinda.

- Cifrado de la información que transita en el enlace de datos de la red regional de la institución educativa y la Internet, por medio de servidores configurados con ISA para control de datos.

3.3.3.3 Situación deseada de seguridad en diseño de red.

Implementar un enlace dedicado a Internet, para completar el requerimiento de la creación de sitio Web para un servidor adecuado para su alojamiento y ofrecer un acceso controlado a usuarios internos por medio de VPN para ingresar a la red de local de la institución de educación superior y monitorear una cantidad desconocida de usuarios provenientes de Internet en busca de información y recursos que la institución pueda brindar, siempre con las precauciones de restricción necesarias para el registro de acceso a usuarios pertenecientes al dominio de la red local.

Separación de la Red local del centro de estudios superiores y servidores públicos que esta tenga a disposición para uso general, por medio de la creación de una DMZ que brinde administración de direccionamiento para solicitudes entrantes.

3.3.3.4 Beneficios del cambio seguridad en diseño de red.

- Nivel de seguridad mejorado a tener segmentada la red y permitir acceso a usuario según perfil y privilegios desde la Internet por medio de VPN.

- Nueva puerta de acceso a la información para estudiantes de la universidad que requieran información sobre intereses académico, por medio de conexión

a Internet dedicado y la implementación del servidor de sitio virtual, para ofrecer el adecuado hardware con el fin de alojar el sitio Web.

- Cifrado de información crítica que se trasmite por la red regional y clientes por conexión a VPN, que se traduce en beneficio de confianza tanto para clientes internos de red, como externos al ofrecer una de las más altas protecciones a la información que se maneja.

3.3.3.5 Solución propuesta y descripción de la solución.

Contratación a mediano plazo de servicio de Internet dedicado para las instalaciones del centro educativo, con miras a que se convierta en acceso de nuestro sitio Web y sea herramienta de acceso de los clientes que forma parte de la institución.

Los aspectos básicos con los que debe contar el servicio de conexión para el servidor Web son.

- Conexión a Internet dedicado a una velocidad a 1024 Kbps28 considerando el posible incremento de solicitudes a recibir en los servidores.

- Inclusión de Direcciones IP publicas para direccionar el nombre del sitio Web y proporcionarles una de estas direcciones como vía de acceso a una VPN desde Internet a usuarios del dominio del centro educativo.

- Colocación de servidores ISA, de manera frontal para completar configuración de perímetro de seguridad, establecer conexiones de datos y pruebas de transferencia.

[28] Un **kilobits por segundo** es una unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de transferencia de información a través de una red. Su abreviatura y forma más corriente es kbps.

3.3.3.6 Seguridad en diseño de red, Uso de la solución.

- El Internet dedicado y el sitio Web publicado, será utilizado para brindar la puerta de enlace como acceso al servidor Web de la institución de estudios superiores, que alojara el sitio Web antes descrito, utilizando las direcciones IP publicas como direccionadores al momento de los usuarios digiten la dirección de este sitio Web.

- El portal de conexión a Internet, nos ofrece una solución de acceso a la red privada local de la infraestructura de Tecnología de la información de la universidad, esta ventaja permite una red mas versátil para los usuarios internos del dominio controlador, en algún momento que se encuentren fuera de los puntos de red local habilitados, pero que cuenten con una vía a Internet, aprovechando las ventajas de la VPN que se sugiere configurar.

CAPITULO IV. Acceso Físico, Seguridad material de la infraestructura y Prevención de contingencias básicas.

4.1 Áreas Seguras infraestructura civil de tratamiento de la información.

4.1.1 Perímetro de Seguridad Física. Infraestructura Material del cuarto de Servidores

Este espacio dentro de la institución debe ser claramente definido, siendo los principales agentes a tomar en cuenta, la fuerza física material de lugar, el área que agrupe todos los recursos de procesamiento de información debe tener solidez en la infraestructura civil, las paredes deben ser de material solidó y difícil de derribar por fuerza humana en conjunto, estas paredes es recomendable que no carezcan de las características de los demás muros que se encuentren en la infraestructura de edificio donde se encuentre en CE.

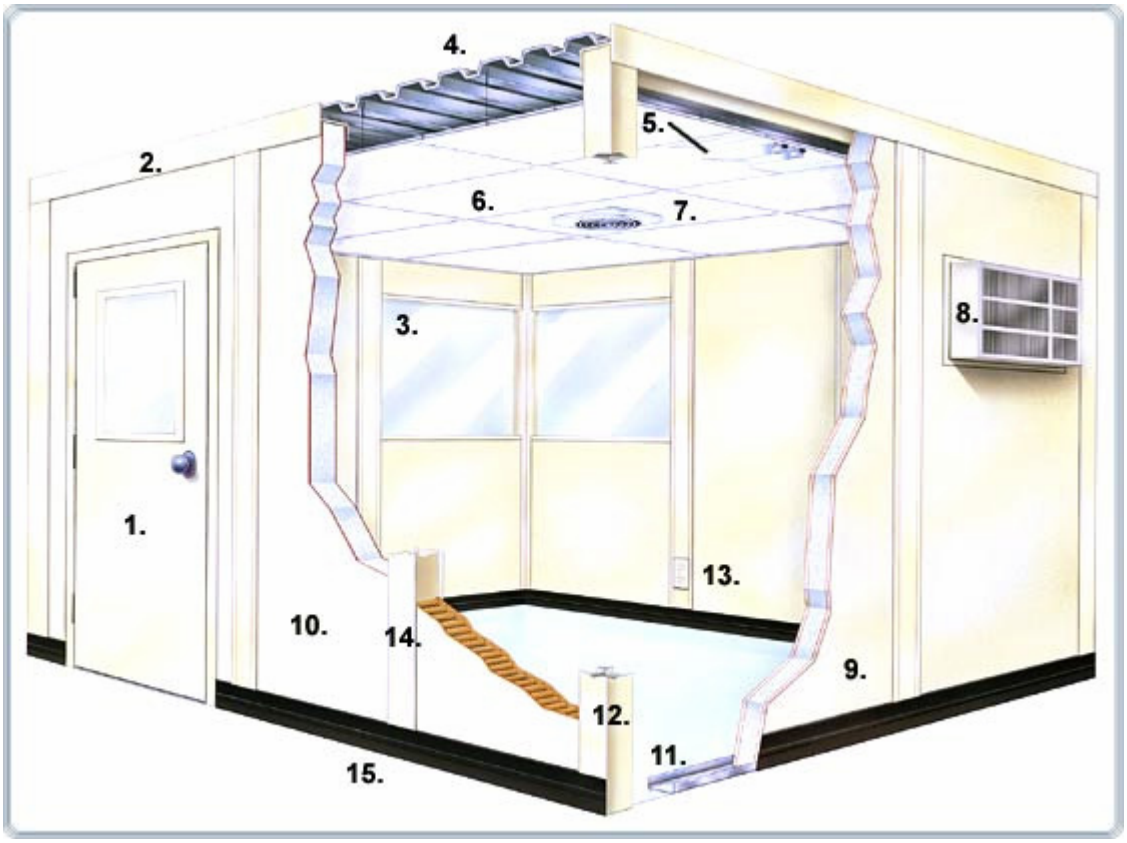


Fig. 4.1 Detalle General de Cuarto de servidores promedio.

1. Puertas
Unidades estándar están disponibles en puertas de acero de ancho de vía o ensambles dobles de puerta. El dibujo indica uno con (vidrio de seguridad claro templado de 1/4 ") Las opciones estándar deben incluir herrajes en las puertas, manijas de aluminio y cerraduras.

2. Cornisas
La construcción de aluminio pintado de cornisa suministra una apariencia agradable.

3. Ventanas Fijas
Las ventanas estándar son de 4 ' o 2 ' en el ancho y 3 ' de altura con vidrios templados de seguridad de 1/4"

4. Cubiertas de Polvo de Acero Corrugado
Acero de 22'' reforzado con líneas verticales dobles y pintado estándar para todas las unidades.

5. Cascarones de Lámpara de 4' x 2'
Luces de 4 lámparas con lente acrílico (focos no incluidos)

6. Techo Exterior Acústico
Enrejado de metal con cielos falsos acústicos fabricados con tablas minerales sin combustibles.

7. Extractores de Aire
Poderosos extractores de aire pueden ser incluidos en cualquier oficina.

8. Unidad de Control de Clima
Las unidades con paredes precortadas de fabrica para el montaje de unidades de refrigeración o climas.

9. Panales de Sonido y Fuego
Los paneles de sonido y fuego son de 3" de grosor con aislante en el centro de poliestireno con 1/2 " de vinilo de yeso en la superficie de cada lado.

10. Paneles Térmicos
Los paneles de tablero de estándar son de 3" de grosor y tienen un vinilo de 1/8 " de grosor adherido con poliestireno al centro.

11. Rieles de Piso de Acero
Los Canales de Acero reforzados sostienen con seguridad los paneles de paredes.

12. Postes de Esquina
Deben ser parte del sistema de enmarcado para montaje de paredes
13. Cajas Conector Eléctricos Dobles
Parte del paquete eléctrico estándar que debe incluir:
- Salidas dúplex
- Interruptor de pared
- Caja de fusibles
- Cajas de teléfono y conductos.

14. Espacios para Cableado.
Forma parte de todos los sistemas estructurales, y permite la instalación de servicios eléctricos verticalmente además acepta cajas eléctricas comunes.

15. Base Café de Vinilo
La protección de base de pared, para evitar cualquier tipo de filtración descontrolada.

Los accesos para personal deben ser controlados por medio de identificación de código y de ser posible también por medio de escaneo relacionado a dimensiones biométricas o identificación de impresiones digitales, siendo la primera una opción muy adecuada para presupuestos de menor dimensión con destino de control de accesos y la segunda, una elección optima para la seguridad de la información dentro del entorno físico; a su vez si existe el caso en que se irrumpe dentro de la habitación de manera no autorizada, el CE debe estar convenientemente protegido con mecanismos de control, alarmas, cierres automáticos de las puertas; esta protección externa debe ser considerada también para las ventanas.

Para salvaguardar la condición física de los recursos de procesamiento de información manejadas por la organización deben ser físicamente separados de las que son manejadas por terceros dentro de un centro de cómputo común de acceso, controlado por un estándar menor de seguridad.

Al no poder disponer de un recinto adecuado que permita todas las libertades necesarias para el adecuado diseño de un Cuarto de Equipos que procesan información, es preciso acondicionar una habitación idónea acorde a las necesidades de espacio que demandan los equipos, para ello es necesario montar barreras físicas desde el piso real hasta el techo real.

Barreras adicionales y perímetros para controlar el acceso físico pueden ser necesarios entre áreas con requisitos de seguridad diferentes dentro del perímetro de seguridad. El uso de múltiples barreras nos brinda protección adicional, donde la falla de una sola barrera no significa que la seguridad este inmediatamente comprometida.

4.1.2 Control Físico de entradas.

El objetivo principal que se persigue con establecer un control físico de entradas a personal acreditado a todas las áreas dentro del perímetro de seguridad física para el Cuarto contenedor de equipos que procesan datos, es proteger de cualquier tipo de amenaza potencial que se pueda generar de terceras persona que podrían significar

un riesgo alto al no saber las intenciones que persiguen al intentar ingresar al sector controlado por el tipo y cantidad de información que se maneja. Las áreas de seguridad deben estar protegidas por controles de entrada adecuados que aseguren el permiso de acceso únicamente al personal autorizado.

Fig. 4.2 La huella digital tiene 16 puntos de inflexión únicos para cada ser humano, eso lo hace una marca que nos individualiza y nos identifica personalmente para medidas de seguridad.

4.1.3 Seguridad en Oficinas.

Esta relacionado profundamente el Cuarto de equipos y su seguridad, como el cuidado de todos los puntos de distribución de la información, tanto para personas de perfil menor de acceso a los datos, como las estaciones de trabajos de los administradores remotos de los servidores y los DBA's[29] de la institución de educación superior.

Comúnmente las oficinas del personal autorizado, tanto físicamente como lógicamente a acceder a la información, se encuentran alrededor del Cuarto de Equipos, para proteger íntegramente la información por parte de los usuarios de perfil normal, es necesario tomar en cuanta los siguientes aspectos:

- Se debe aplicar dentro de la infraestructura del edificio, la discreción del la localidad física de los datos y dar una mínima indicación del propósito del

[29] DBA, Siglas en ingles que obedecen a Administrador de la Base de Datos. Persona Responsable del diseño físico, administración, y de la selección, evaluación e implementación de los Sistemas de Administración de las Bases de Datos.

edificio. Fuera de estos mantener la misma reserva de dar indicios que resulta ser un lugar donde se procesa la información.

- Cada una de las estaciones de trabajo de los usuarios que accedan a la información, parcial o restringidamente, deben poseer contraseña alfanumérica y esta debe activarse al corto tiempo de no actividad, para evitar el acceso publico sin autorización previa.

- Toda la información de tipo Directorio Telefónico y Guías internas de la institución de educación superior, tienen que guardar moderación en indicar las locaciones de los recursos de información sensible, no deben estos documentos estar a disposición del publico.

4.1.4 Protección contra amenazas externas y ambientales.

Se debe designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humana.

Se debe dar consideración a cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.

Las siguientes pautas deben ser consideradas para evitar daño por parte del fuego, inundación, temblores, explosiones, malestar civil y otras formas de desastre natural o humana:

- Los materiales peligrosos e insumos que sean de tipo combustibles se deberían almacenar en algún lugar distante de las áreas seguras. No se

deberían almacenar dentro de un área segura suministros a granel hasta que se necesiten.

- El equipo y los medios de respaldo deberían estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal.

- Equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente.

4.1.5 Trabajo en áreas seguras.

Se debe diseñar y aplicar pautas para trabajar en áreas de seguridad de la información.
Se deben considerar los siguientes modelos:

- El personal ajeno al área de seguridad de la información sólo deberá conocer la existencia de esta; si y solo si para completar las actividades de estas personas se necesitara para su trabajo.

- Se debería evitar en todo caso, el trabajo no supervisado en áreas de seguridad de la información, tanto por motivos de seguridad materia, así como para evitar oportunidades de actividades maliciosas.

- Las áreas seguras deberían estar cerradas y controlarse periódicamente cuando estén vacías.

- No se debería permitir la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial.

Los arreglos para trabajar en áreas de seguridad para la información deben incluir controles para los empleados, contratistas y usuarios de terceros que trabajen en dicha área, así como otras actividades de terceros que se lleven acabo ahí.

4.1.6 Ubicación de los equipos.

Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.

4.2 Política de control de accesos.

Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. Los controles de acceso son lógicos y físicos.[30]

Estos deben ser considerados juntos. Se debería dar a los usuarios y proveedores de servicios una especificación clara de los requisitos de negocio cubiertos por los controles de accesos.

Esta política debería contemplar lo siguiente:

- Requisitos de seguridad de cada tipo de acceso ya sea lógico o físico. visto individualmente.

- Identificación de toda la información relativa a las aplicaciones y los riesgos que la información esta enfrentando.

[30] Ver sección 4.1 “Áreas Seguras”

- Políticas para la distribución de la información y las autorizaciones es decir, el principio de suministro sólo de la información que se necesita conocer y los niveles de seguridad para la clasificación de dicha información.

- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes. Como se ejemplifica en la figura siguiente.

Fig. 4.3 Diagrama de estabilidad en coherencia entre políticas control acceso físico y lógico, y clasificación de la información.

- Legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios. Esto para documentar lo aplicable al usuario y notificarle de sus responsabilidades sobre la información que maneja.

- Perfiles de acceso de usuarios estandarizados según las categorías comunes de estudio o trabajo dentro del centro de estudios superiores.

- Administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión.

- Segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos. Todo documentado para prevenir debilidades del modelo de seguridad en caso de una falla en la seguridad.

- Requerimientos para la autorización formal de los pedidos de acceso, ya sea por otorgamiento de rol de empleo, o nuevos privilegios otorgados a usuario por nivel de responsabilidad.

- Requerimientos para la revisión periódica de los controles de acceso. Esto con el fin de determinar errores humanos al momento de otorgar nuevos accesos o bien accesos temporales por extensión de horario de trabajo o extensión de este.

- Retiro de los derechos de acceso. Al momento de dar de baja a un usuario por abandono de rol desempeñado o cambio de actividades no relacionadas con la información.

4.2.1 Acceso Público, Áreas de entrada.

Dentro de una organización de educación superior, existe información que puede ser entregada a los alumnos, de manera publica sin restricciones y otra que debe ser manejada únicamente por el personal de administración académica o similares encargados de custodia de datos. Todo esto con la clara intención de mantener íntegros los datos son opción de corrupción.

El papel de la institución es de tipo dual con cierto grado de permisión, ya que debe garantizar el principio de publicidad y libertad de acceso a los datos finales de la institución, de los alumnos y proyectos de toda índole realizados por y para los alumnos; Además debe certificar la seguridad de la información de carácter sensible tanto de los alumnos, como de la institución al no permitir su alteración de manera descontrolada, ni el acceso de la misma por personas no autorizadas.

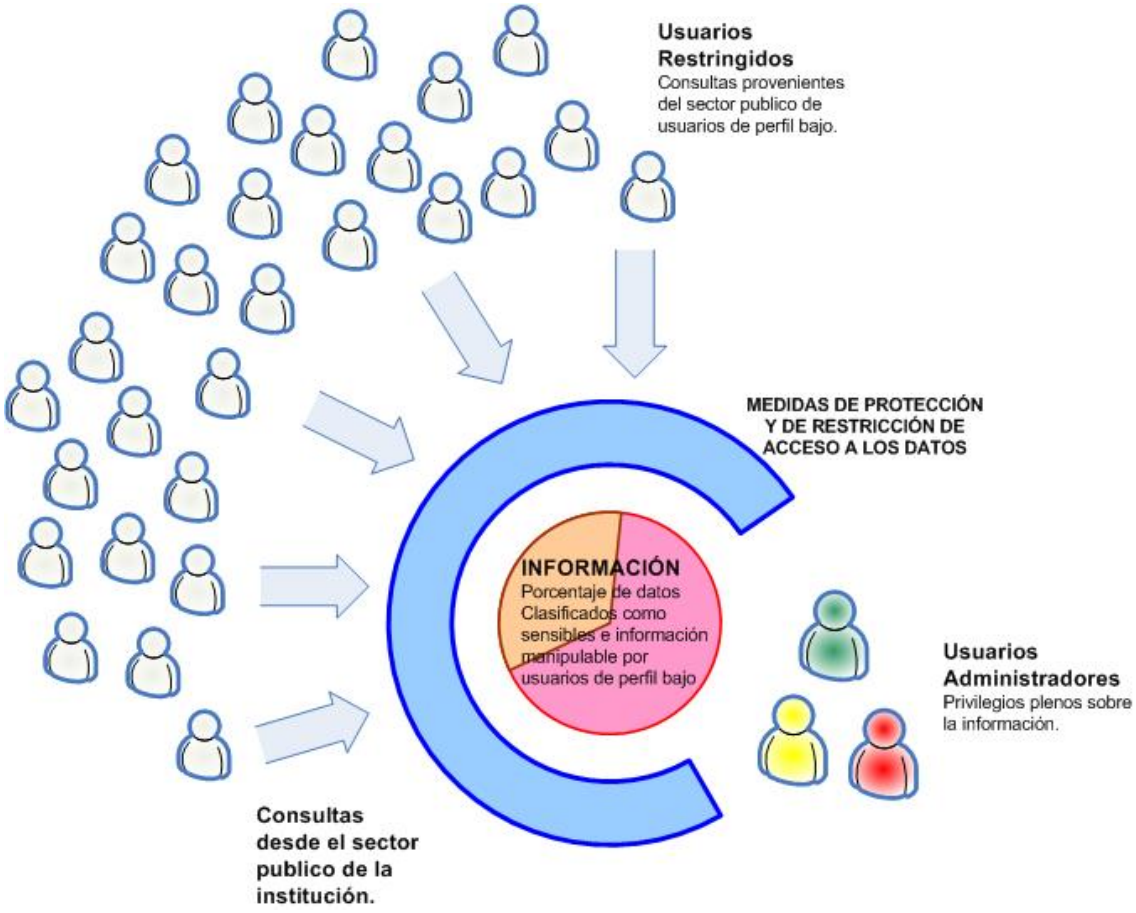


Fig. 4.4 Diagrama de ubicación de proveniencia de consultas y distinción de usuarios por perfil de acceso publico a la información.

Para ello se recomienda implementar las siguientes políticas de acceso a los datos:

- Debe existir una clara distinción entre reglas a cumplir siempre y reglas opcionales o condicionales, de control de la información por parte del perfil que se le otorgue al usuario.

- El establecimiento de las reglas basándose en el indicio "**está prohibido todo lo que no esté permitido explícitamente**", premisa que es contraria a la regla "está permitido todo lo que no esté prohibido explícitamente", considerada más débil o más permisiva.

- Los cambios en las autorizaciones al usuario deben existir y ser realizados automáticamente por el sistema de información y a su vez debe coexistir con los que sean realizados por un usuario administrador.

- Debe ser efectiva la distinción por parte de todos los usuarios, entre reglas que requieren o no la aprobación del administrador o de otra autoridad antes de su promulgación.

4.2.2 Gestión de Acceso de usuarios.

El objetivo principal de este apartado, es cerciorarnos con seguridad sobre el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información de una institución de educación superior.

Para dar cumplimiento a esto se debe establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios en dependencia al rol que desempeñe un usuario dentro de la infraestructura de TI.

Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los

usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debería prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema informático.

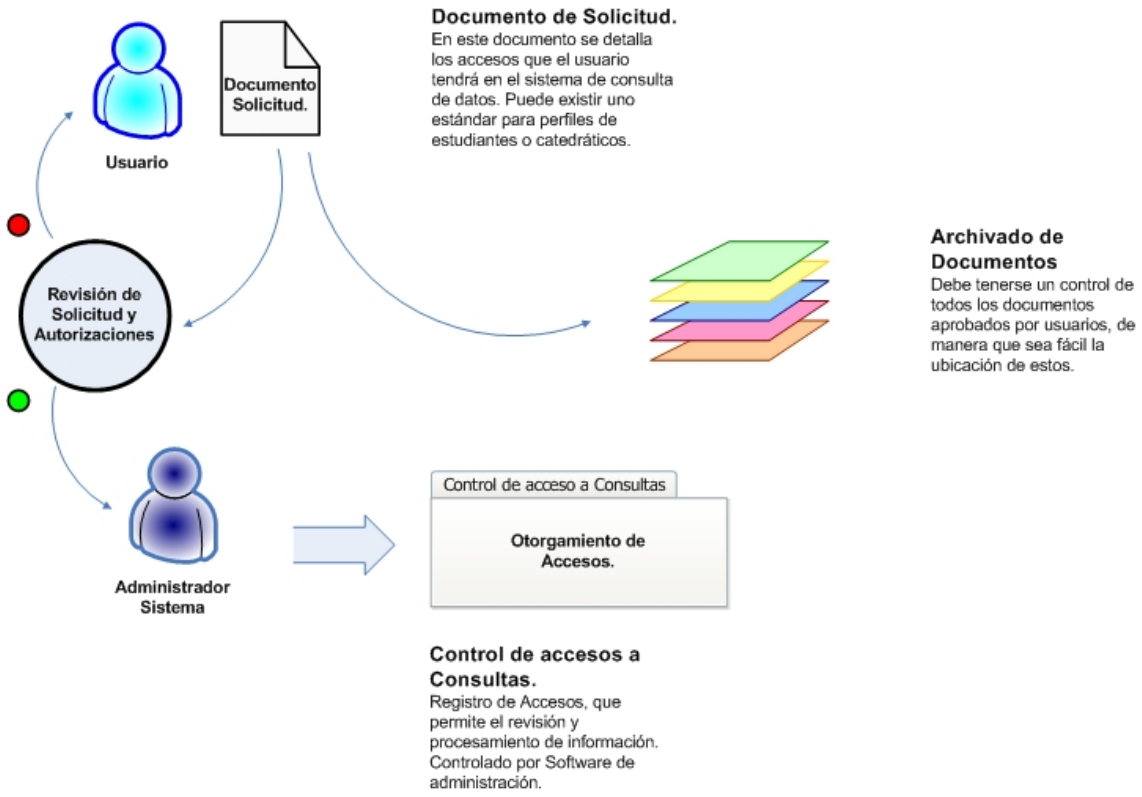


Fig. 4.5 Diagrama de Flujo de Control para documentación, otorgamiento de privilegios y archivado de documentos, de Altas y Cambios de accesos para usuarios

4.2.3 Registro de usuarios.

Cada una de las infraestructuras organizativas, debe poseer un procedimiento coherente para brindar y garantizar el acceso a cada uno de los usuarios, de acuerdo al perfil que ellos posean. Este procedimiento se debe formalizar de acuerdo a un registro de altas y bajas de usuarios para avalar el acceso a los sistemas y servicios de información multiusuario.

Se debe controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro que debe incluir:

- La utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debe permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados; Estos casos se puede dar para privilegios por departamentos internos, por mencionar un caso.

- La comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información. También puede ser conveniente que la dirección de TI apruebe por separado los derechos de acceso.

- Verificación de la adecuación del nivel de acceso asignado al propósito del usuario dentro de los servicios de TI que se proporcionan y su consistencia con la política de seguridad de la organización.

- La entrega a los usuarios de una relación escrita de sus derechos de acceso.

- La petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso.

- La garantía de que no se provea acceso al servicio hasta que se hayan completado los procedimientos de autorización establecidos.

- El mantenimiento de un registro formalizado de todos los autorizados para usar el servicio.

- La eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de rol dentro de la institución.

- La revisión periódica y eliminación de identificadores y cuentas de usuario redundantes.

- La garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

4.2.4 Gestión de privilegios.

Se debe controlar la asignación de privilegios por un proceso formal de autorización en los sistemas multiusuario. Se obliga a considerar los pasos siguientes:

- Identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación; así como las categorías de usuarios que necesitan usar dentro de ellos.

- Asignar privilegios a los usuarios, según los principios de "necesidad de su uso", "caso por caso" y en línea con la política de control de acceso previamente establecida[31].

- Mantener un proceso de autorización y un registro de todos los privilegios asignados a todos los usuarios. No se otorgarán privilegios hasta que el proceso de autorización haya concluido, es decir, debe de otorgarse todos los accesos solicitados, únicamente que la solicitud y autorización de los mismos hayan pasado por todos los controles de seguridad y revisión, este documentado como se indique.

[31] Referirse a la sección 4.2 "Política de control de acceso"

- Promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios, no autorizados u otorgados de manera temporal, sin respetar los lineamientos de seguridad.

Un uso inapropiado de los privilegios de la administración del sistema, cualquier característica o facilidad de un sistema de información que habilite al usuario sobrescribir los controles del sistema o de la aplicación, pueden ser un gran factor contribuidor de fallas o aberturas en los sistemas.

4.2.5 Gestión de contraseñas de usuarios.

El proceso de gestión de contraseñas para todo tipo de usuarios, debe incluir los siguientes requisitos:

- Requerir que los usuarios firmen un compromiso para mantener en secreto sus contraseñas personales y las compartidas por un grupo sólo entre los miembros de ese grupo, este compromiso que podría incluirse en los términos y condiciones del contrato de empleo.

- Proporcionar inicialmente una contraseña temporal segura que forzosamente deben cambiar inmediatamente después. Para que sea únicamente el usuario quien posea su llave privada y responsabilidad de este, todas las transacciones, consulta y demás que se realicen bajo su usuario.

- Establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de reemplazo o temporal.

- Establecer un conducto seguro para hacer llegar las contraseñas temporales a los usuarios. Se debería evitar su envío por terceros o por mensajes no cifrados de correo electrónico.

- Las contraseñas temporales deben ser únicas para cada individuo y no deben ser obvias.

- Los usuarios deberían remitir acuse de recibo de sus contraseñas.

- Las contraseñas nunca deben ser almacenadas en sistemas de cómputo sin ser protegidos;

- Las contraseñas por defecto que vienen asignadas por el fabricante del producto, deben ser alteradas después de la instalación de los sistemas o software.

Las contraseñas son un medio común de verificar la identidad del usuario antes de conceder el acceso a un sistema de información o servicio, sea dado de acuerdo a la autorización del usuario. Se deben considerar, si son apropiadas, otras tecnologías para identificación y autentificación de usuario como las biométricas, así como la verificación de huellas, la verificación de la firma o el uso de dispositivos hardware como las tarjetas inteligentes, para caso de acceder a un lugar físico[32].

[32] Referirse a la sección 4.2.1 "Acceso Público, Áreas de entrada".

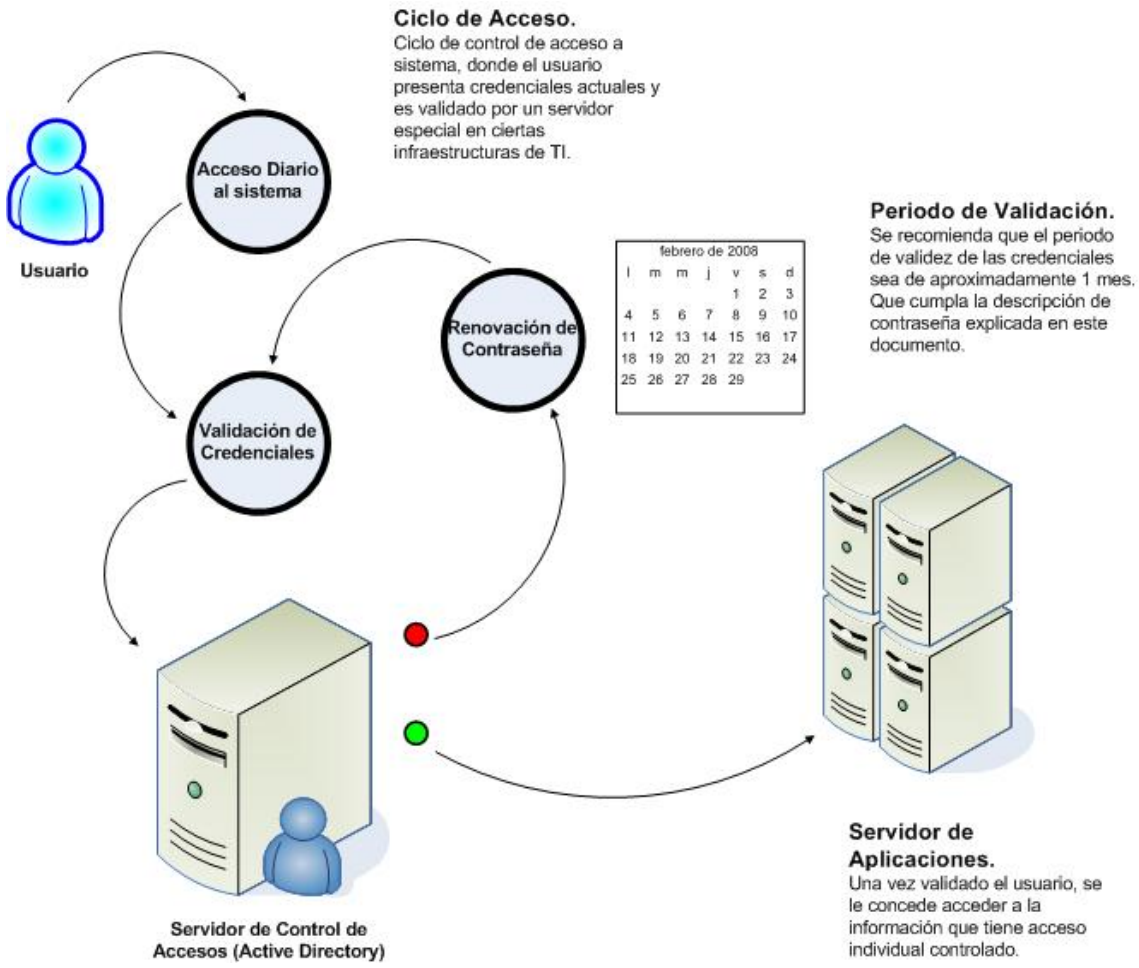


Fig. 4.6 Diagrama de Flujo de Control para autenticación de usuario, al momento de acceder al sistema administrador de la información que necesitamos.

4.2.6 Revisión de accesos de usuarios.

La revisión de los derechos de acceso de usuario debería considerar las siguientes pautas:

- Revisar los derechos de acceso de todos los usuarios a intervalos de tiempo regulares, se recomienda un periodo entre tres y seis meses. Para renovar, después de cualquier cambio como promoción, degradación o término del rol que desempeñe el usuario.

- Los derechos de acceso de los usuarios deben ser revisados y reasignados cuando se traslade desde un perfil de usuario a otro dentro de la misma organización.

- Revisar más frecuentemente, se recomienda mensualmente, las autorizaciones de derechos de acceso con privilegios especiales.

- Comprobar las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados. Esto descansa en parte en los roles de auditores internos del sistema de TI.

- Los cambios en las cuentas privilegiadas deben ser inspeccionadas por una revisión periódica. Para los casos de administradores generales del sistema.

Es necesario revisar regularmente los derechos de los accesos de los usuarios para mantener un control efectivo del acceso a los datos y los sistemas de información.

4.2.7 Responsabilidades de usuarios.

Cada uno de los usuarios que gocen de privilegios de accesos físicos y virtuales a los sitios donde se procesa la información, deben tener plena conciencia de la seguridad que se brinda en el sitio y de las normas que deben acatar y colaborar en el cumplimiento de ellas. Para ello deben tomarse en cuenta los siguientes lineamientos.

- Evitar el acceso de usuarios no autorizados, aun cuando estos hayan tomado el compromiso de no hurto de la información y la no identificación de los sitios donde se da el procesamiento de información.

- Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

- Un escritorio limpio, así como una política de pantalla clara debe ser implementado con el fin de reducir el riesgo de acceso no autorizado o de daño a los papeles, medios e instalaciones del procesamiento de información.

4.2.8 Uso de contraseñas.

Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

Todos los usuarios deberían ser informados acerca de:

- Mantener la confidencialidad de las contraseñas.

- Evitar guardar registros en papel, archivos de software o dispositivos contenedores de datos, donde las contraseñas puedan almacenarse, salvo si existe una forma segura de hacerlo y el método de almacenamiento ha sido aprobado.

- cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema, esto puede ser detectado por el usuario mismo o administradores del sistema.

- Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres, que sean:

    - Fáciles de recordar.

    - No estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario, por ejemplo, nombres, fechas de nacimiento, números de teléfono, o similares.
    - No sean vulnerables a ataques de diccionario.
    - Estén carentes de caracteres consecutivos repetidos o que sean todos números o todas letras.

- Cambiar las contraseñas a intervalos de tiempo regulares o en proporción al número de accesos. Las contraseñas de las cuentas con privilegios especiales deberían cambiarse con más frecuencia que las normales, evitando utilizar contraseñas antiguas o cíclicas.

- Cambiar las contraseñas temporales asignadas para inicio, la primera vez que se ingrese al sistema.

- No incluir contraseñas en ningún procedimiento automático de conexión, que, las deje almacenadas permanentemente.

- No compartir contraseñas de usuario individuales.

- No utilizar la misma contraseña para propósitos personales o de negocio.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se les pide que mantengan contraseñas múltiples, deberían ser aconsejados sobre la posibilidad de usar una sola contraseña de calidad, para todos los servicios, que brinde un nivel razonable de protección para la contraseña almacenada.

4.3 Prevención contingencias Básicas.

Se deberá establecer un proceso de gestión de continuidad del servicio de disponibilidad de la información para reducir, a niveles aceptables, la interrupción causada por fallas de seguridad o bien por desastres naturales, accidentes, problemas de equipos o acciones deliberadas. Mediante una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.

Se debe analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio. Se debe desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la institución.

La gestión de la continuidad del servicio de información debe incluir, en adición al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales.

4.3.1 Guía de Determinación de Contingencias Básicas.

La determinación de plan de continencia para continuidad de los servicios de TI, debe realizarse de manera paralela a la implementación de la solución informática para un servidor Web, es decir se debe designar recursos humanos para su documentación y establecimiento de puntos críticos de acción que pueden afectar o provocar la interrupción de los servicios de TI.

4.3.1.1 Elementos clave para la gestión de continuidad de servicio de información.

El proceso de definición debe reunir los siguientes elementos clave de la gestión de continuidad del servicio:

- Comprender los riesgos que la institución corre desde el punto de vista de su vulnerabilidad e impacto, incluyendo la identificación y priorización de los procesos críticos del servicio de información.

- Identificar todos los activos implicados en los procesos críticos de procesamiento de la información necesarios para brindar los servicios de TI.

- Comprender el impacto que tendrían las interrupciones de disponibilidad de la información. Es importante encontrar soluciones que manejen las pequeñas incidencias así como los grandes accidentes que puedan amenazar la disponibilidad de los servicios de TI. Además de establecer los objetivos de suplir la demanda de la información, en lo referente a los medios informáticos.

- Considerar la adquisición de los seguros de riesgos adecuados que formarán parte del proceso general de continuidad de los servicios de TI así como parte de la gestión operacional de riesgo.

- Identificar y considerar la implementación de controles adicionales de prevención; para cada uno de las amenazas identificadas en los literales I y II.

- Identificar los recursos financieros, organizacionales, técnicos y ambientales necesarios para realizar la cobertura de los requisitos identificados como necesarios, para dar cumplimiento a la seguridad de la información.
- Garantizar la seguridad del personal y la protección de las instalaciones de procesamiento de datos y de la propiedad de la institución.

Los eventos que pueden causar interrupciones a los procesos de servicio de la información; deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

El estudio para la continuidad de servicios de TI, debe comenzar como lo mencionábamos, por la identificación de los eventos que pueden causar interrupciones en los procesos de servicio de la información, por mencionar un patrón, una falla del equipo, una inundación o un incendio.

Se debería continuar con una evaluación del riesgo para determinar la probabilidad e impacto de dichas interrupciones, en términos tanto de escala de daños como de periodo de recuperación.

La evaluación del riesgo de continuidad de negocio debe ser llevada a cabo con una total implicancia por parte de los propietarios de los recursos y procesos de la información.

Debería considerar todos los procesos de servicio de la información, no solo a los dispositivos informáticos, pero debe incluir los resultados específicos para la seguridad de información. Es importante vincular los diferentes aspectos de riesgos para obtener una figura completa de los requerimientos de continuidad de los servicios de la información de la organización. La evaluación debe identificar, cuantificar y priorizar los riesgos contra criterios y objetivos relevantes para la organización incluyendo recursos críticos, impactos de las interrupciones, tiempos permisibles de interrupción y prioridades de recuperación.

Se debería desarrollar un plan estratégico para determinar un enfoque global de la continuidad de los servicios de TI, a partir de los resultados de la evaluación del riesgo. Una vez creada la estrategia, deberá respaldarla y crear un plan para implementar dicha estrategia.

4.3.2 Plan de Continuidad de los servicios de TI.

El proceso de planificación de la continuidad del negocio debería considerar los siguientes aspectos:

- La identificación de los procedimientos de emergencia y los acuerdos de todas las responsabilidades.
- La identificación de las pérdidas aceptables de información y servicios.
- La implementación de procedimientos que permiten la recuperación y restauración de las operaciones de los servicios de TI y la disponibilidad de información en escalas de tiempo requerido. Se necesita particular atención para la evaluación de las dependencias de los servicios de información externas e internas.
- Los procedimientos operacionales de seguimiento para completar la restauración y recuperación.
- La documentación de los procedimientos y procesos acordados.
- La formación apropiada del personal en los procedimientos y procesos de emergencia acordados, incluyendo la gestión de crisis.
- La prueba y actualización de los planes.

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo, en la recuperación de servicios específicos a los clientes en un plazo aceptable. Se deberían considerar los servicios y recursos necesarios para conseguirlo, incluyendo el personal, los recursos no informáticos y los contratos de respaldo de los dispositivos informáticos. Estos contratos pueden incluir arreglos con terceros en la forma de acuerdos recíprocos o servicios de subscripciones comerciales.

CAPITULO V. Instrucciones De Instalación de Rack, Servidor Web y Direct Attached Storage.

5.1 Instalación Rack.

5.1.1 Instrucciones de Seguridad.

El estante de 42 unidades cumple las especificaciones de American National Standards Institute (Instituto Nacional Americano de Estándares, ANSI), el estándar de Electronic Industries Association (Asociación de industrias electrónicas, EIA) ANSI/EIA-310-D-92, el estándar de Consumer Electronics
Association (Asociación de electrónica de consumo, CEA) CEA-310-E, Internacional Electrotechnical Commission (Comisión electrotécnica internacional, IEC) 297 y la Norma de la industria alemana (DIN) 41494.

Antes de instalar sistemas en el estante, instale estabilizadores frontales y laterales en estantes independientes o el estabilizador frontal en estantes unidos entre ellos. Un fallo al instalar estabilizadores adecuadamente antes de instalar sistemas en un estante puede hacer que este se caiga, lo que podría causar daños físicos a personas en determinadas circunstancias. Por lo tanto, instale siempre el estabilizador antes de instalar los componentes en el estante.
Después de instalar un sistema o componente en un estante, no saque nunca del estante más de un componente a la vez por sus ensamblajes de deslizamiento. El peso de más de un componente extendido podría hacer que el estante se cayera y causara graves daños físicos a personas.
Los gabinetes de estante pueden ser extremadamente pesados, pero se mueven fácilmente sobre las ruedecillas. Los gabinetes no tienen frenos.

Prestar extremo cuidado al mover el armario. Recoja las patas niveladoras al volver a colocar el armario. Evite inclinaciones largas o pronunciadas para evitar pérdidas de

control del armario. Extienda las patas niveladoras de apoyo para evitar que el armario se desplace.

5.1.2 Herramientas materiales recomendados para la instalación de un Rack.

Es posible que necesite las siguientes herramientas y materiales para instalar el estante:

Destornillador Phillips del n. º 2
Destornillador de cabeza plana
Llave inglesa de 12 mm.
Alicates de punta fina
Llave Allen de 4 mm. (Si desea que la puerta se abra en sentido inverso)
Llave Allen de 5 mm. (Incluida en el kit)
Llaves para las puertas del estante y los paneles laterales

5.1.3 Puerta Frontal.

1) Pulse el botón del pestillo de la puerta para soltar el mango de la puerta, y luego abra la puerta frontal por completo.

2) Mientras sujeta la puerta, coloque el pasador de la bisagra hacia arriba para que libere la cubierta del pasador de la bisagra.
   El gancho de retención del pasador de la bisagra previene que la bisagra se salga de su sitio.

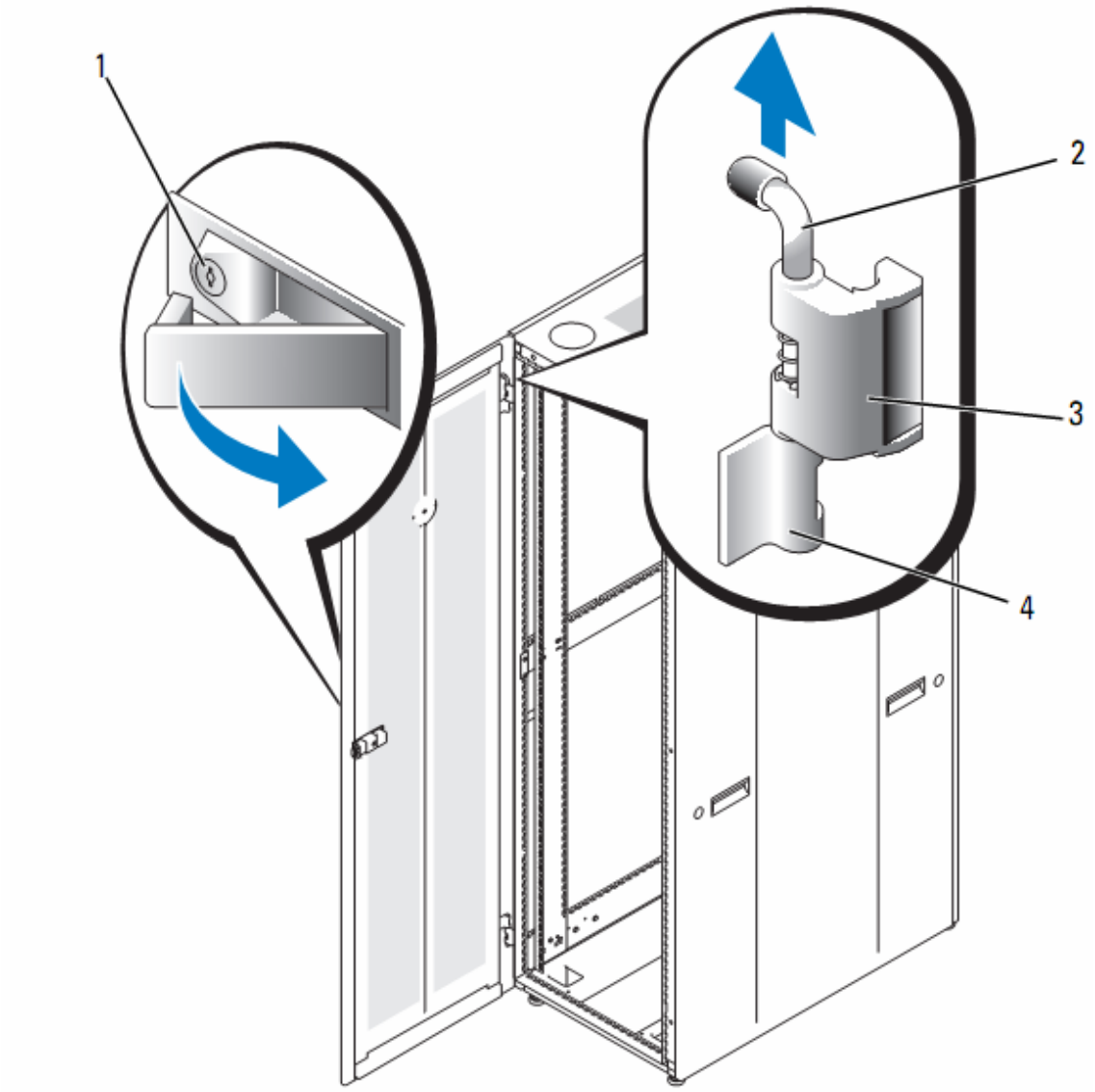


Fig. 5.1 Montado de puerta frontal del gabinete.

3) Mientras mantiene el pasador de la bisagra fuera de la cubierta del pasador de la puerta, saque ligeramente la puerta del estante para liberar el cuerpo de la bisagra.
4) Libere el pasador de la bisagra.

5) Levante la puerta hacia arriba para que se libere la parte inferior del pilar de la bisagra.

   PRECAUCIÓN: debido a su tamaño y peso, le recomendamos que coloque la puerta extraída en horizontal.

6) Coloque el panel en un sitio seguro con la cara exterior hacia arriba.

   Dejar la puerta en horizontal con la superficie exterior hacia arriba ayudará a prevenir daños en la capa que recubre la puerta.

5.1.4 Puertas Posteriores.

1) Abra las puertas posteriores.
2) Pulse el botón del pestillo de la puerta para liberar la manivela de la puerta derecha.
3) Abra la puerta derecha.
4) Presione el pestillo de la puerta izquierda para liberarla
5) Abra la puerta izquierda.

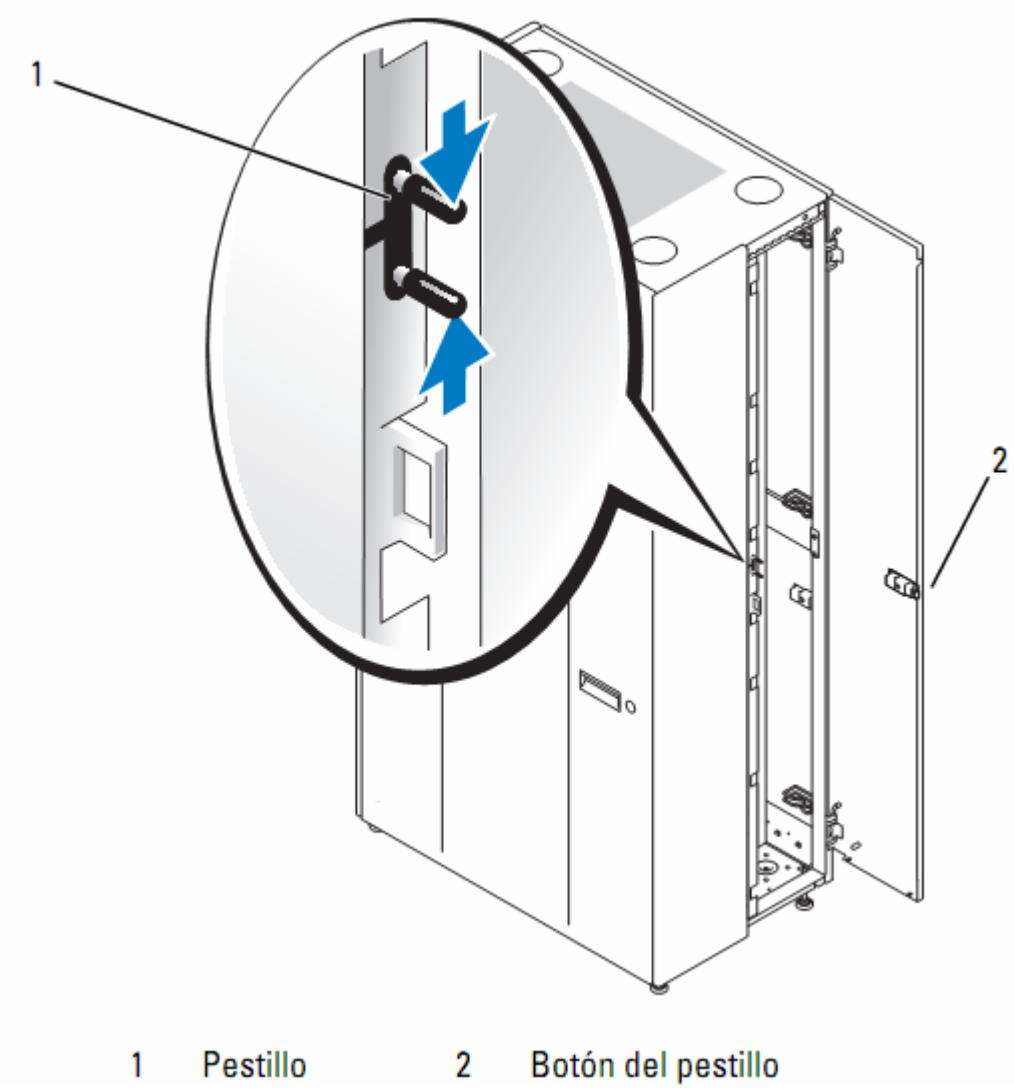


Fig. 5.2 Montado de puertas posteriores del gabinete.

5.1.4.1 Extraer la puerta derecha.

1) Mientras sujeta la puerta, coloque el pasador de la bisagra hacia arriba para que libere la cubierta del pasador de la bisagra.
2) Oirá un clic al sacar el pasador de la cubierta de la bisagra de la puerta.
3) Las bisagras están diseñadas para prevenir que se salgan del pasador de la bisagra.

4) Repita el paso A para la bisagra trasera.
5) Saque la puerta del estante.

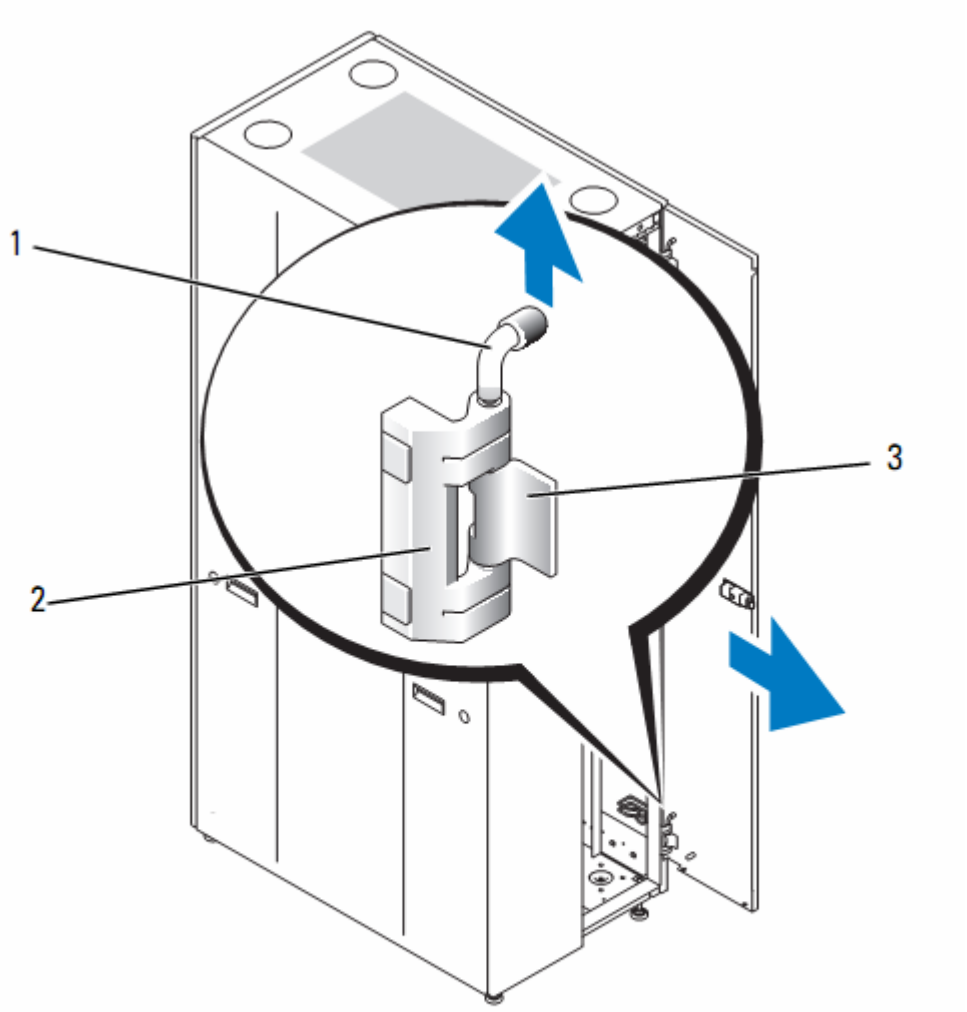


Fig. 5.3 Montado de bisagras posteriores del gabinete.

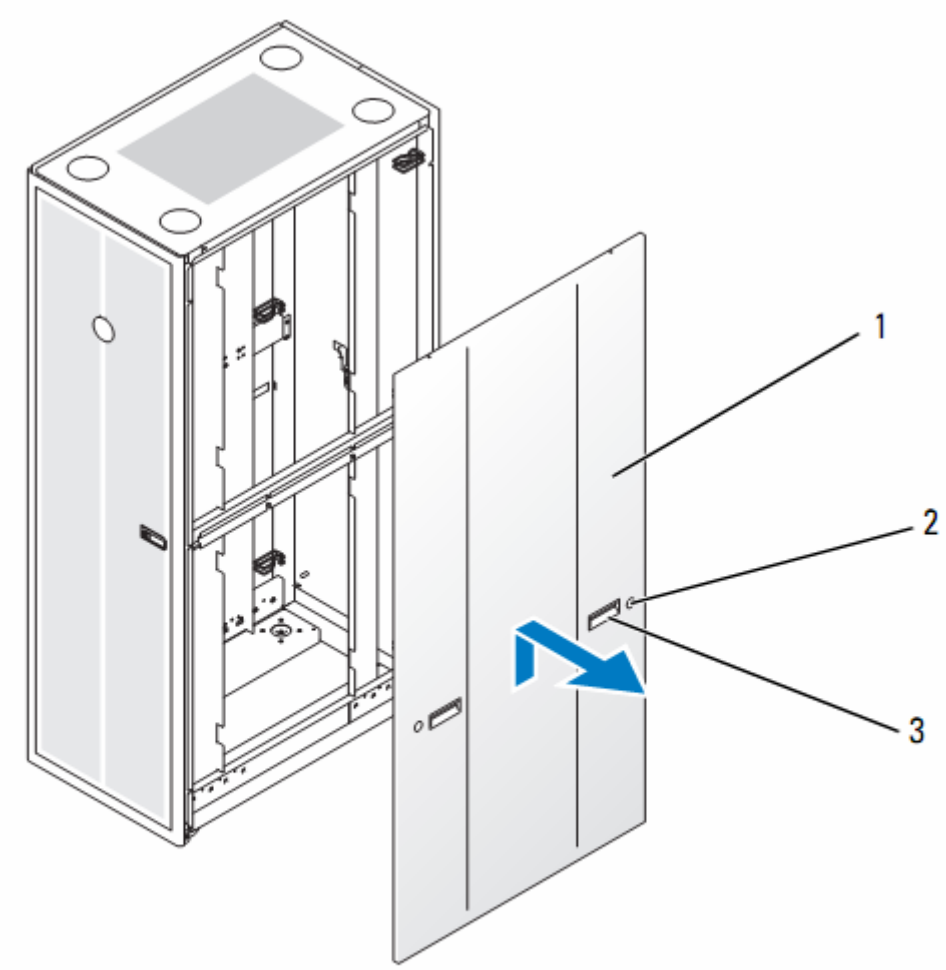
PRECAUCIÓN: debido al tamaño y peso de la puerta, se recomienda colocar la puerta retirada con la superficie exterior hacia arriba.

6) Coloque la puerta en un sitio seguro con la superficie exterior hacia arriba. Esto prevendrá daños en la capa que la recubre.

7) Repita desde el paso 1 hasta el 6 para la puerta izquierda.
8) Para extraer las puertas posteriores, realice de forma inversa los pasos para extraerlas.

5.1.4.2 Extraer los paneles laterales

1) Desbloquee los pestillos que se encuentran cerca de los extremos izquierdos y derechos del panel (ver Ilustración).



1 Panel lateral (2) 2 Pestillos (2)
3 Manijas (2)

Fig. 5.4 Montado de puertas laterales del gabinete.

2) Permita un ligero balanceo hacia el exterior del panel lateral desde la parte inferior.
3) Sujete firmemente el panel usando las manijas.
4) Levante el panel hasta liberar la parte superior del estante (ver imagen anterior).
5) Aleje el panel del estante.

PRECAUCIÓN: debido al tamaño y el peso de los paneles laterales de gabinete del estante, nunca intente retirarlos o instalarlos usted mismo.

6) Coloque el panel en un sitio seguro con la superficie exterior hacia arriba. Esto prevendrá daños en la capa que recubre la puerta.
7) Repita paso1 el procedimiento paso6 en el otro lado del panel.

Para reemplazar los paneles laterales, realice de forma inversa los pasos para extraerlos.

5.1.5 Asegurar las patas niveladoras individuales del estante.

El estante incluye cuatro patas niveladoras montadas en las esquinas. Las patas niveladoras están diseñadas para alinear el estante en una posición recta cuando éste se sitúa en superficies ligeramente desniveladas. Antes de instalar los sistemas en el estante, implante y ajuste las patas niveladoras. Cuando nivele el estante, siga estas instrucciones.

Recomendaciones:
Al ajustar las patas niveladoras, asegúrese de que las ruedecillas de cada esquina no se levantan más de 9.5 mm. Sobre el suelo. Si excede los 9.5 mm. de distancia de separación entre el suelo y las ruedecillas cuando ajuste las patas niveladoras,

extraiga lentamente las patas niveladoras y cambie el estante a otra ubicación que requiera ajustes mínimos.

Ajuste las patas niveladoras para que se apoyen firmemente en el suelo. Un contacto adecuado con el suelo asegura que cada pata niveladora soporta el peso del estante y evita que se balancee en cualquier dirección. Si las patas niveladoras no tienen un contacto firme con el suelo, el estante puede desestabilizarse y caerse.
No intente mover el estante con las patas niveladoras desplegadas. Recoja siempre las patas niveladoras antes de mover el estante. Si están desplegadas cuando mueve el estante, este puede caerse.

Antes de instalar los sistemas, nivele el estante e instale las patas estabilizadoras. Un estante totalmente cargado puede caerse si se apoya en una superficie irregular y las patas niveladoras y estabilizadoras no soportan su peso.

1) Baje las patas niveladoras con un destornillador hasta que se apoyen en el suelo.
2) Si necesita bajar aun más la pata, ajuste la tuerca hexagonal con un destornillador de 12 mm.
3) Repita los pasos 1 y 2 para el resto de las patas niveladoras.
4) Asegúrese de que el estante está nivelado.

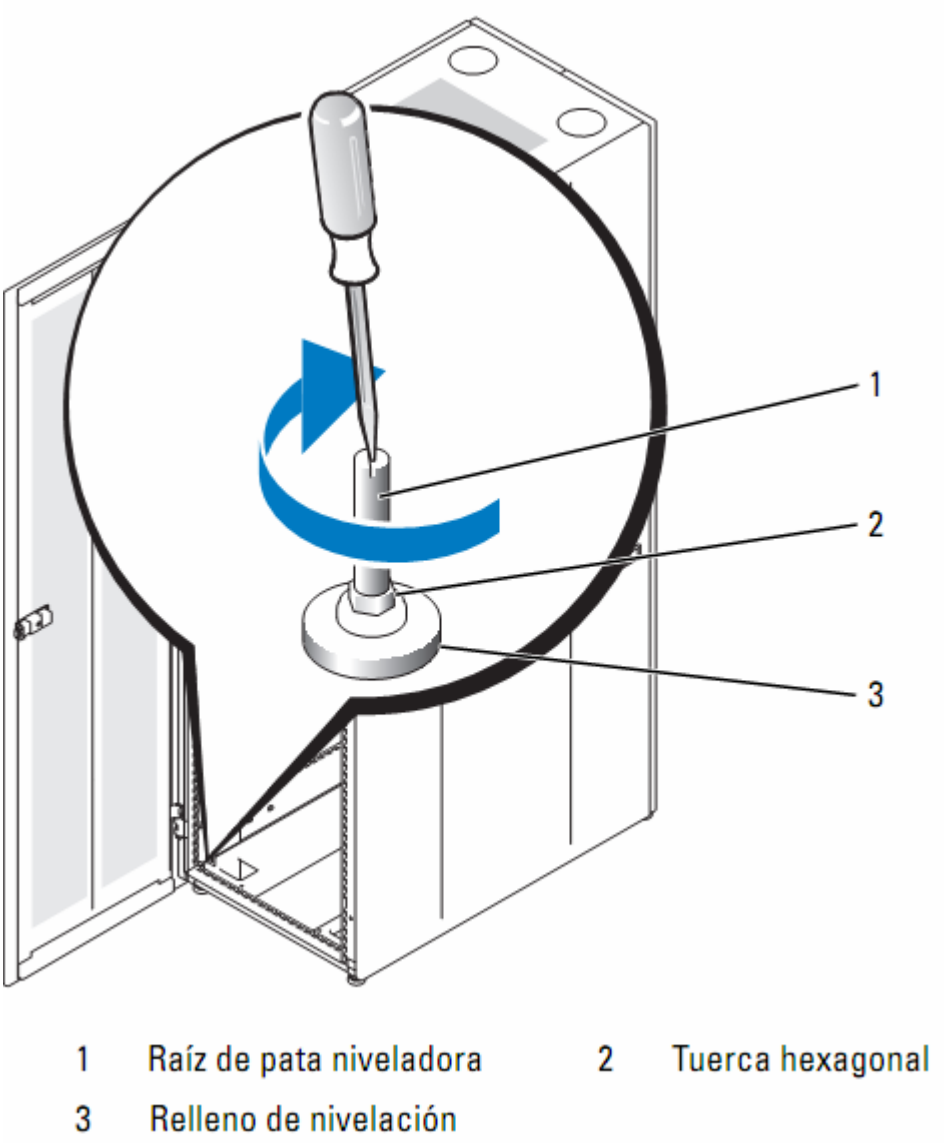


Fig. 5.5 Estabilización del gabinete mediante tuerca estabilizadora inferior.

5.1.6 Instalación de las patas estabilizadoras del estante.

5.1.6.1 Estabilizador frontal.

Recomendaciones.

Si instala sistemas en un estante sin tener instaladas las patas estabilizadoras frontal y lateral, el estante puede caerse, lo que podría causar daños físicos a personas en

determinadas circunstancias. Por lo tanto, instale siempre la pata estabilizadora antes de instalar componentes en el estante.

Instale la pata estabilizadora en el estante del modo siguiente:

- Instale las patas estabilizadoras frontal y lateral en un estante independiente.
- Instale las patas estabilizadoras frontales en todos los estantes de una serie e instale una pata estabilizadora derecha o izquierda en los estantes del final de cada serie.

Para instalar una pata estabilizadora frontal, siga los siguientes pasos:

1) Abra la puerta frontal.
2) Introduzca las manos en el estante y tire firmemente del estabilizador para separarlo del cuadro.
3) Posicione la pata estabilizadora frontal contra la base del cuadro del estante y alinee los orificios con los correspondientes del cuadro.
4) Utilice la llave Allen de 5 mm. y los tornillos correspondientes para asegurar la pata estabilizadora frontal al estante, tal y como de indica en la ilustración.

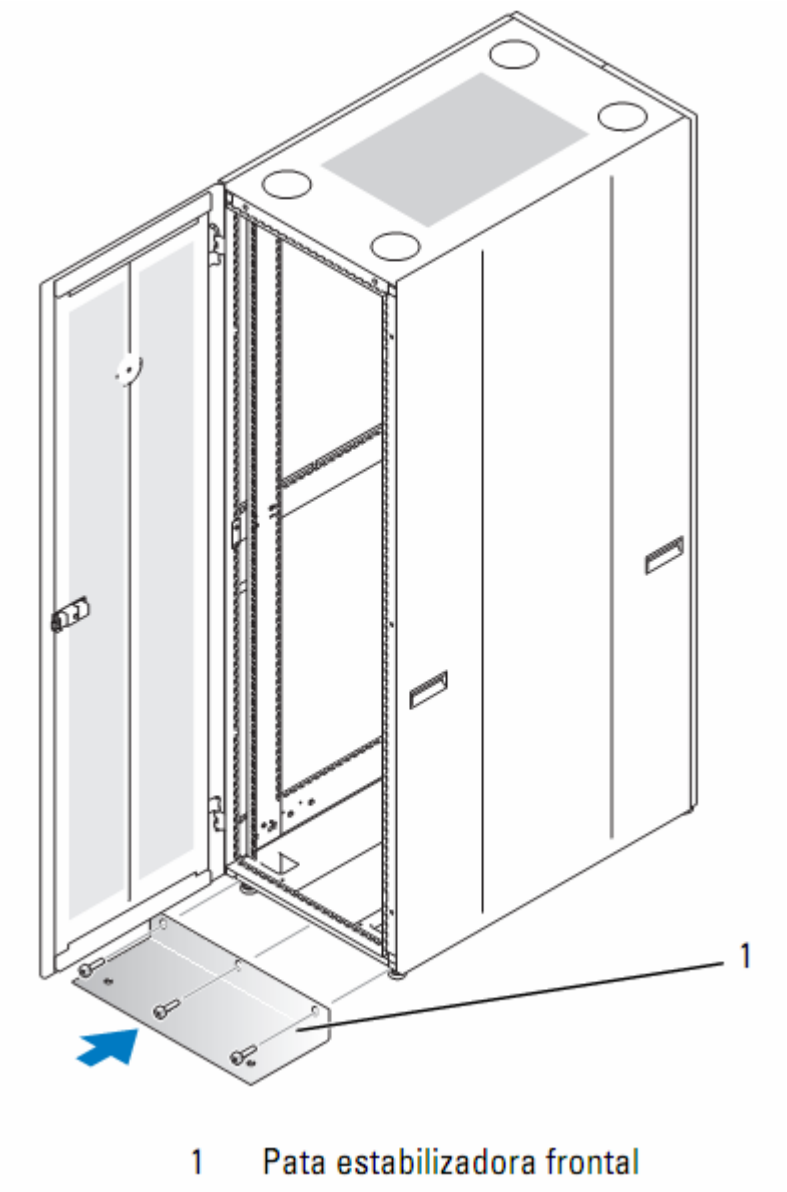


Fig. 5.6 Estabilización del gabinete mediante refuerzo frontal.

5.3.4.1 Estabilizador Lateral.

Para instalar una pata estabilizadora lateral, siga los siguientes pasos:

1) Extraiga el panel lateral.

2) En un lado del riel inferior del cuadro del estante, ubique los tres orificios en cadena (ver Ilustración1-10).
3) Coloque la pata estabilizadora frontal contra la base del cuadro del estante y alinee los orificios con los correspondientes del cuadro.

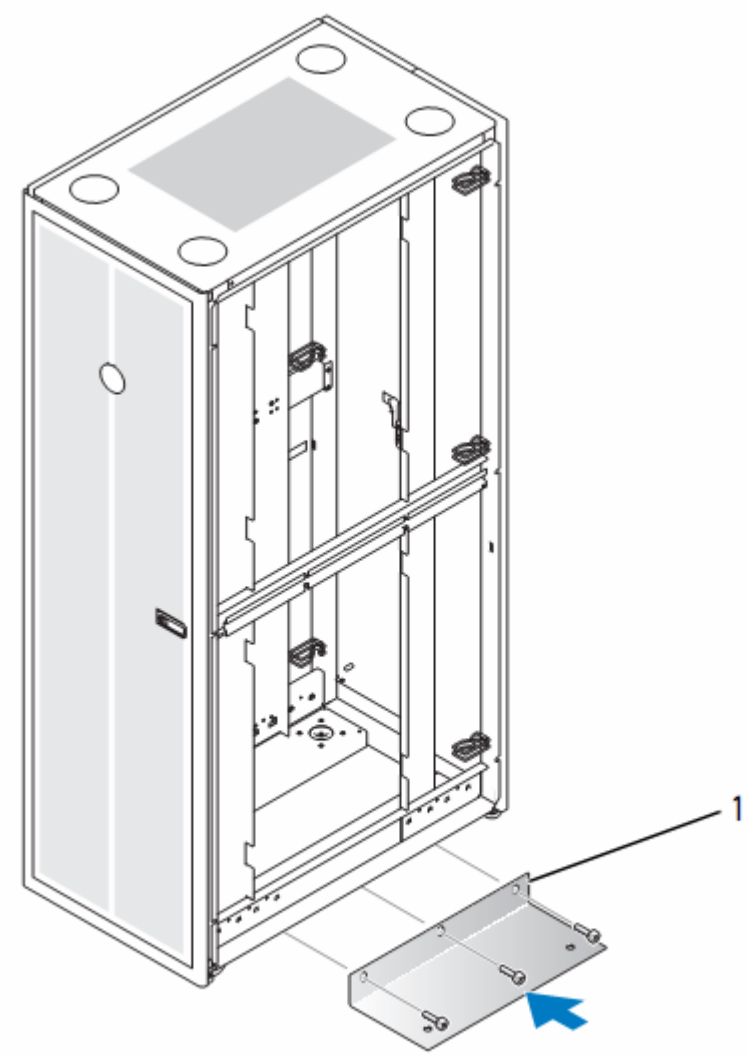


Fig. 5.7 Estabilización del gabinete mediante refuerzo lateral.

4) Utilice los tornillos y la llave Allen de 5 mm. para asegurar la pata estabilizadora al cuadro del estante.

NOTA: a no ser que necesite acoplar dos o más estantes, ya puede instalar sistemas en el estante. Consulte las etiquetas blancas numeradas en la parte frontal y trasera de los rieles de montaje para informarse sobre cómo instalar componentes en el estante.

5.2 Instalación Servidor.

5.2.1 Instrucciones Generales de Instalación.

En este apartado se proporcionan instrucciones para técnicos de servicio especializados que instalen uno o más sistemas en un armario tipo gabinete. Se cuenta con un kit de rack RapidRails que lo fabrica DELL, se puede montar en todos los armarios del fabricante sin herramientas, y el kit de rack VersaRails se puede montar en la mayoría de los armarios rack estándar del sector. Los procedimientos para instalar los kits de rack RapidRails y VersaRails son similares. Para cada sistema que se montará en el armario se precisa un kit de rack.
A continuación, brindaremos procedimientos para los kits de rack de cuatro postes siguientes:

- Kit de rack de rieles deslizantes
- Kit de rack de rieles estáticos (versiones RapidRails y VersaRails)

AVISO: el kit de rack VersaRails lo deben montar únicamente técnicos de servicio cualificados en un rack que cumpla las especificaciones siguientes:

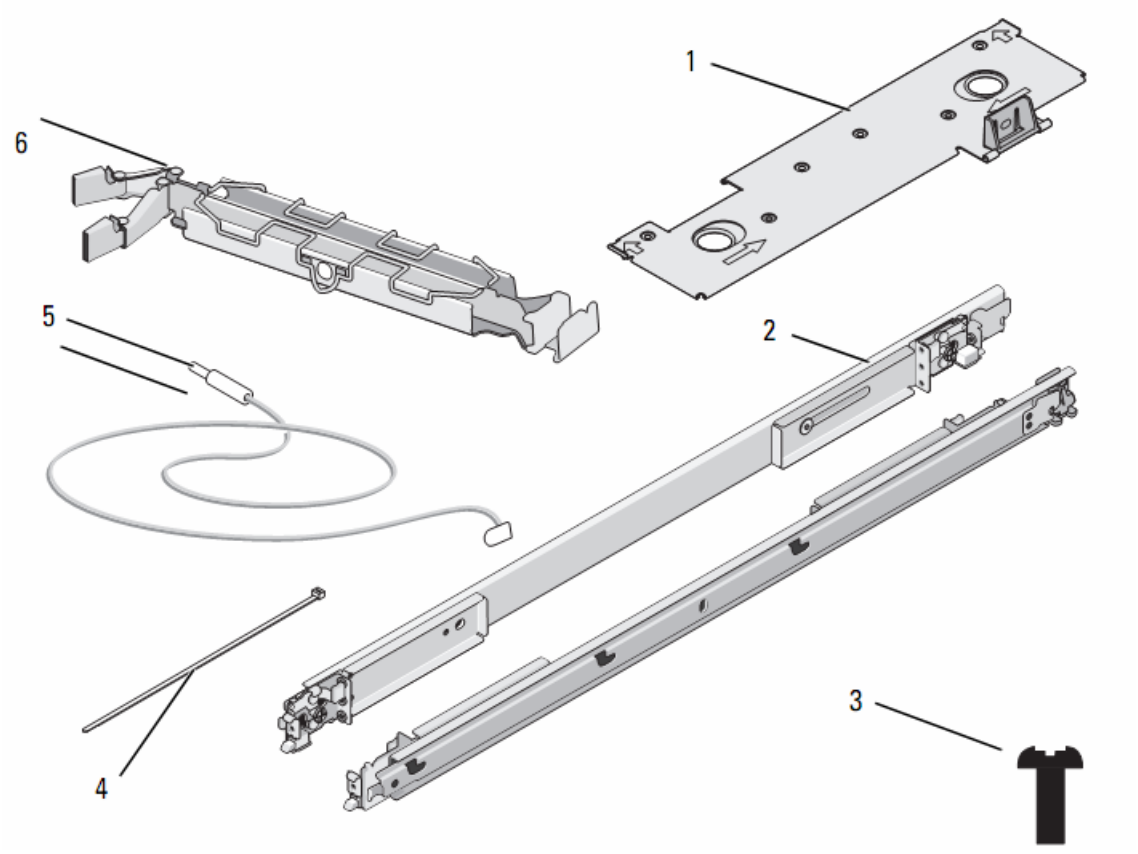
- ANSI/EIA-310-D-92, IEC 297 y DIN 41494[33].

[33] ANSI/EIC: American National Standard Institute/Electronic Industry Association, IEC: International Electronic Comisión, DIN: Deutsches Institut für Normung

5.2.2 Configuración de rieles deslizantes.

5.2.2.1 Contenido del kit para rack de rieles deslizantes.

- Un par de ensamblajes deslizantes (convertibles a la configuración RapidRails o VersaRails)
- Un brazo para tendido de cables
- Una bandeja
- Un cable de indicador de estado (si procede)
- Abrazaderas para fijar los cables al brazo para tendido de cables
- Ocho tornillos Phillips con arandela 10-32 x 0,5 pulgadas (utilizados únicamente en la configuración VersaRails)



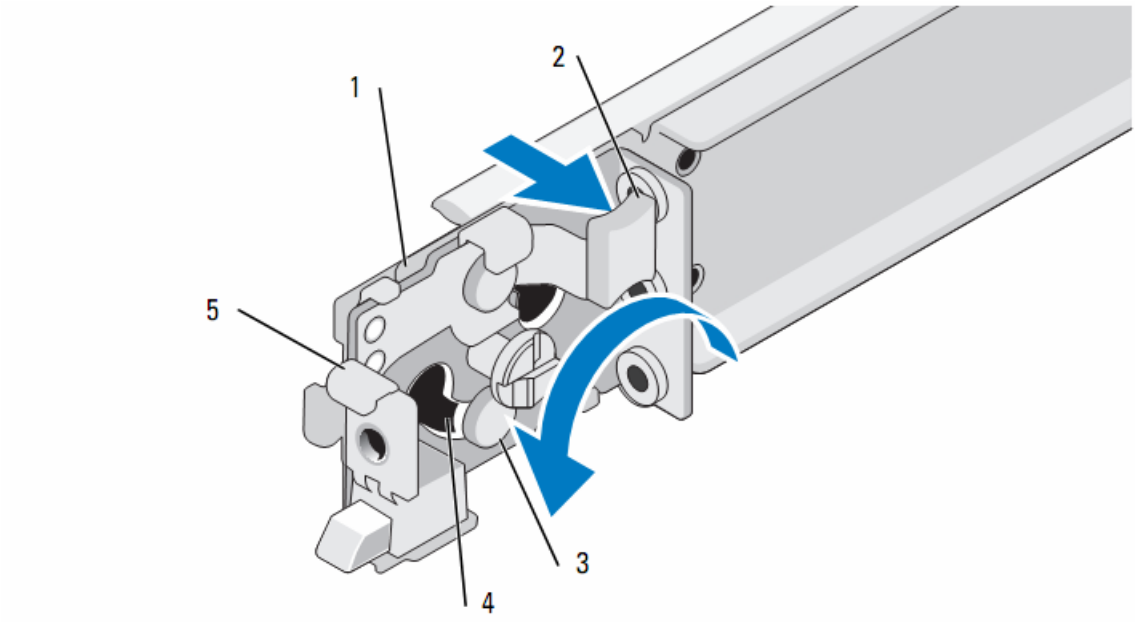
1	Bandeja	2	Ensamblajes deslizantes (2)	3	8 tornillos Phillips con arandela 10-32 x 0,5 pulgadas (únicamente en la configuración VersaRails)
4	Abrazaderas	5	Cable de indicador de estado (si procede)	6	Brazo para tendido de cables

Fig. 5.7 Contenido de kit de servidores para montado en rack.

El ensamblaje de rieles deslizantes presenta un soporte de montaje giratorio en cada extremo del riel. La posición del soporte determina si el ensamblaje de rieles se utiliza como RapidRail o como VersaRail. El lado RapidRail del soporte tiene un gancho y un pestillo que lo fijan al riel vertical. El lado VersaRail del soporte tiene tres orificios y se fija al riel vertical mediante tornillos.

Para girar el soporte de montaje y cambiar los rieles de montaje de RapidRails a VersaRails

1) Levante la palanca de liberación del soporte de montaje giratorio.
2) Gire el soporte y levántelo para sacarlo de los dos topes.
3) Continúe girando el soporte 180 grados hasta que pueda volver a colocar las muescas sobre los topes.
4) Gire el soporte en la dirección contraria sobre los topes hasta que el soporte encaje en su sitio.

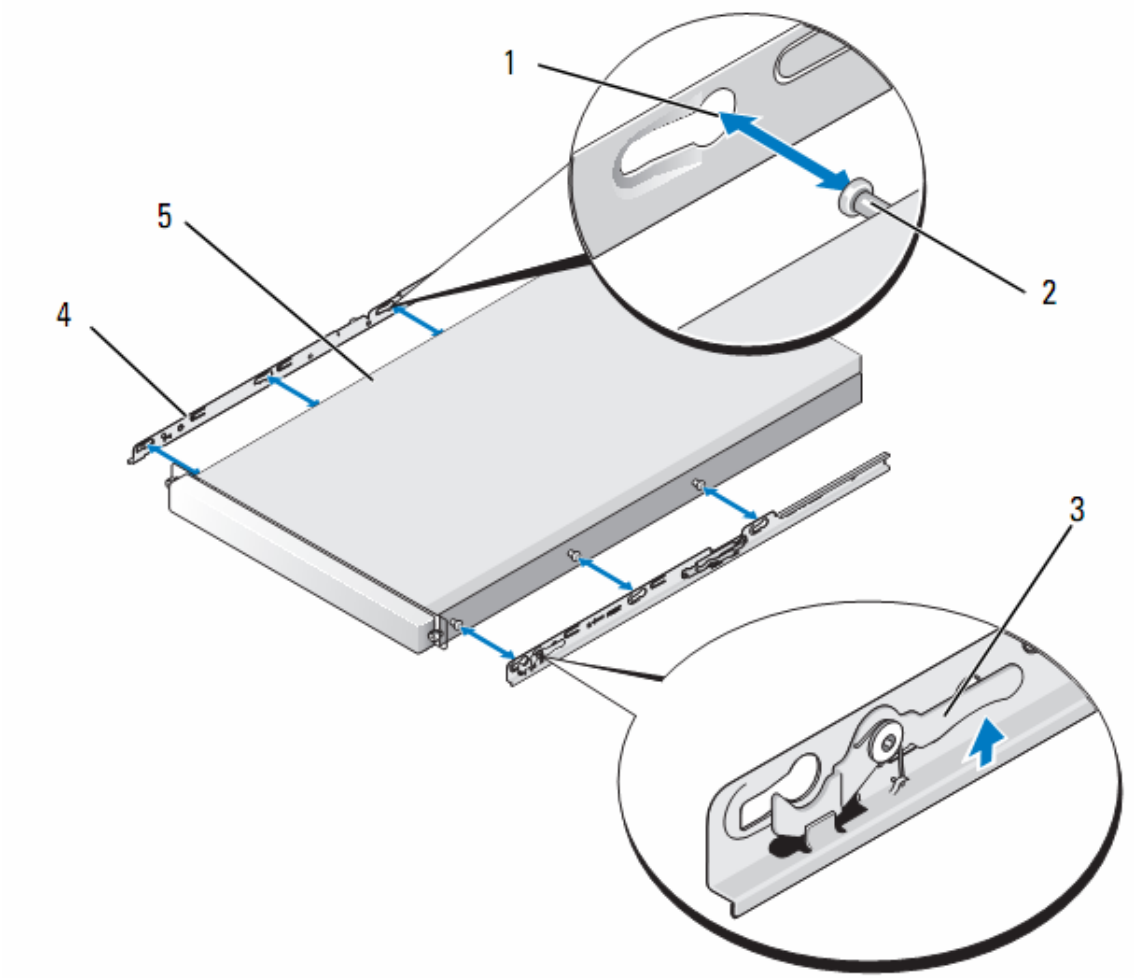


1	Soporte giratorio	2	Palanca de liberación	3	Topes (2)
4	Muescas (2)	5	Superficie de montaje del soporte (configuración RapidRails)		

Fig. 5.8 Cambio de la posición del soporte de montaje giratorio

5.2.3 Instalación de rieles estáticos en Gabinete.

1) Para instalar un módulo de rieles, localice las tres ranuras en forma de cerradura del módulo de rieles y los tornillos de pivote correspondientes en el lateral del sistema.
2) Coloque el módulo de rieles al lado del sistema de modo que los tornillos de pivote se ajusten a la parte redonda de las ranuras y, a continuación, inserte el módulo hacia la parte posterior del sistema.
3) Repita los pasos 1 y 2 para instalar el otro módulo de rieles.
4) Para extraer un módulo de rieles del chasis, tire del pestillo de liberación, deslice el riel hacia adelante y extraiga el módulo de rieles del chasis.



1	Ranuras en forma de cerradura (6)	2	Tornillos de pivote (6)	3	Pestillo de liberación
4	Módulos de rieles (2)	5	Sistema		

Fig. 5.9 Instalación y extracción de los módulos de rieles estáticos del chasis.

1) En la parte frontal del armario rack, coloque uno de los rieles de montaje de forma que la superficie de montaje del soporte quede situada entre las marcas o la cinta que ha colocado (o las posiciones numeradas) en los rieles verticales. El gancho de montaje superior de la superficie de montaje de soporte frontal debe entrar en el orificio superior entre las marcas realizadas en los rieles verticales.

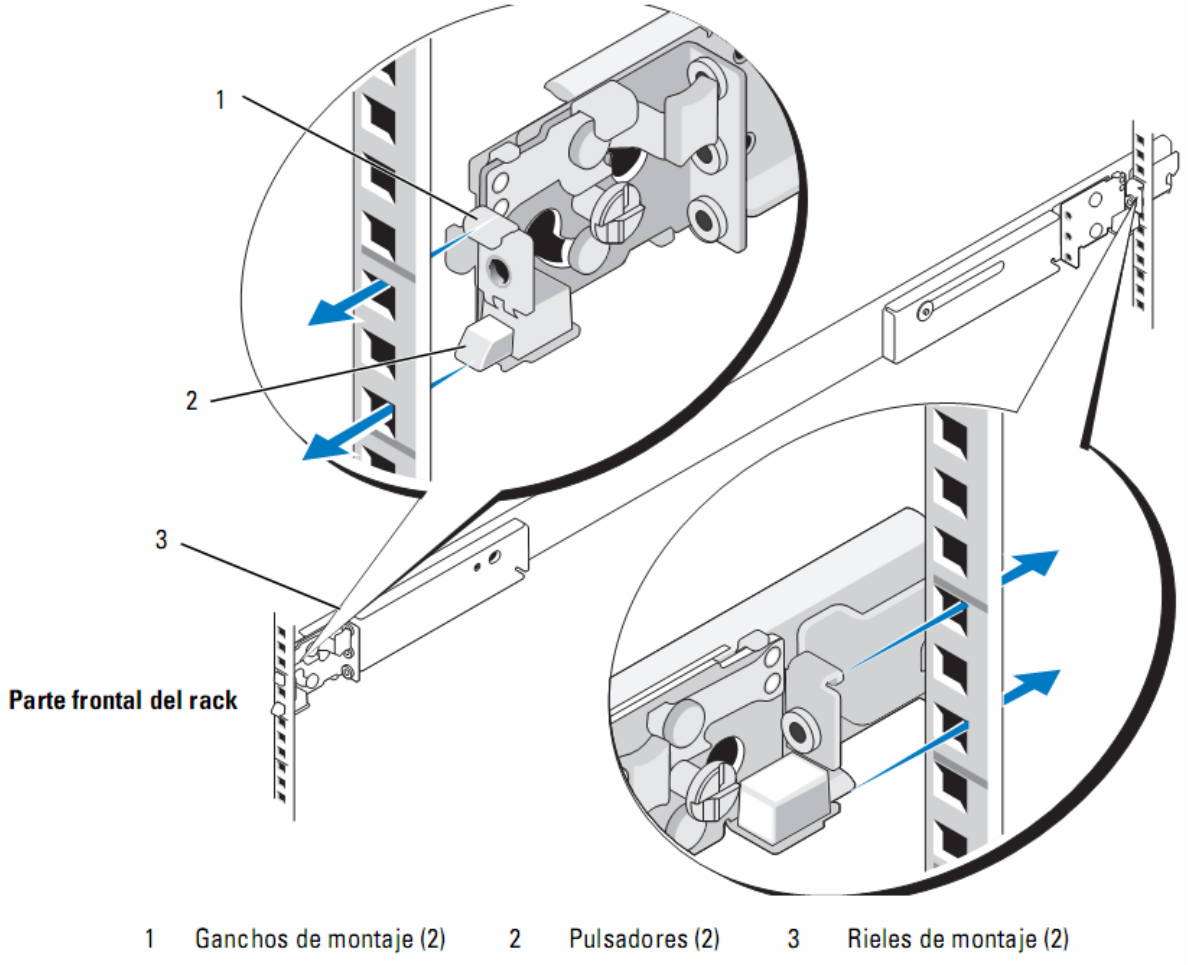


Fig. 5.10 Instalación de los rieles de montaje RapidRails.

2) Empuje el riel de montaje hasta que el gancho de montaje entre en el orificio cuadrado correspondiente. A continuación, presione hacia abajo la superficie de montaje del soporte hasta que el gancho de montaje quede encajado y el botón de presión salga por el orificio cuadrado inferior

3) En la parte posterior del armario, tire hacia atrás de la superficie de montaje hasta que el gancho de montaje encaje en el orificio cuadrado superior y, a continuación, empuje hacia abajo la superficie hasta que el gancho de montaje quede encajado y el botón de presión salga por el orificio cuadrado inferior.

4) Repita del paso1 al paso3 para el riel de montaje del otro lado del rack.

5) Asegúrese de que los rieles de montaje estén montados en la misma posición vertical en ambos lados del rack.

5.2.4 Instalación de servidor en el gabinete.

1) Tire de los dos rieles deslizantes internos hacia fuera del rack hasta que queden totalmente extendidos.

2) Levante el sistema hasta colocarlo por encima de los rieles deslizantes extendidos.
   Los tres tornillos de pivote de cada lado del sistema encajan en las ranuras “J” correspondientes de los ensamblajes deslizantes internos.

3) Baje la parte posterior del sistema alineando los tornillos de pivote posteriores situados en los lados del sistema con las ranuras “J” posteriores de los ensamblajes deslizantes.

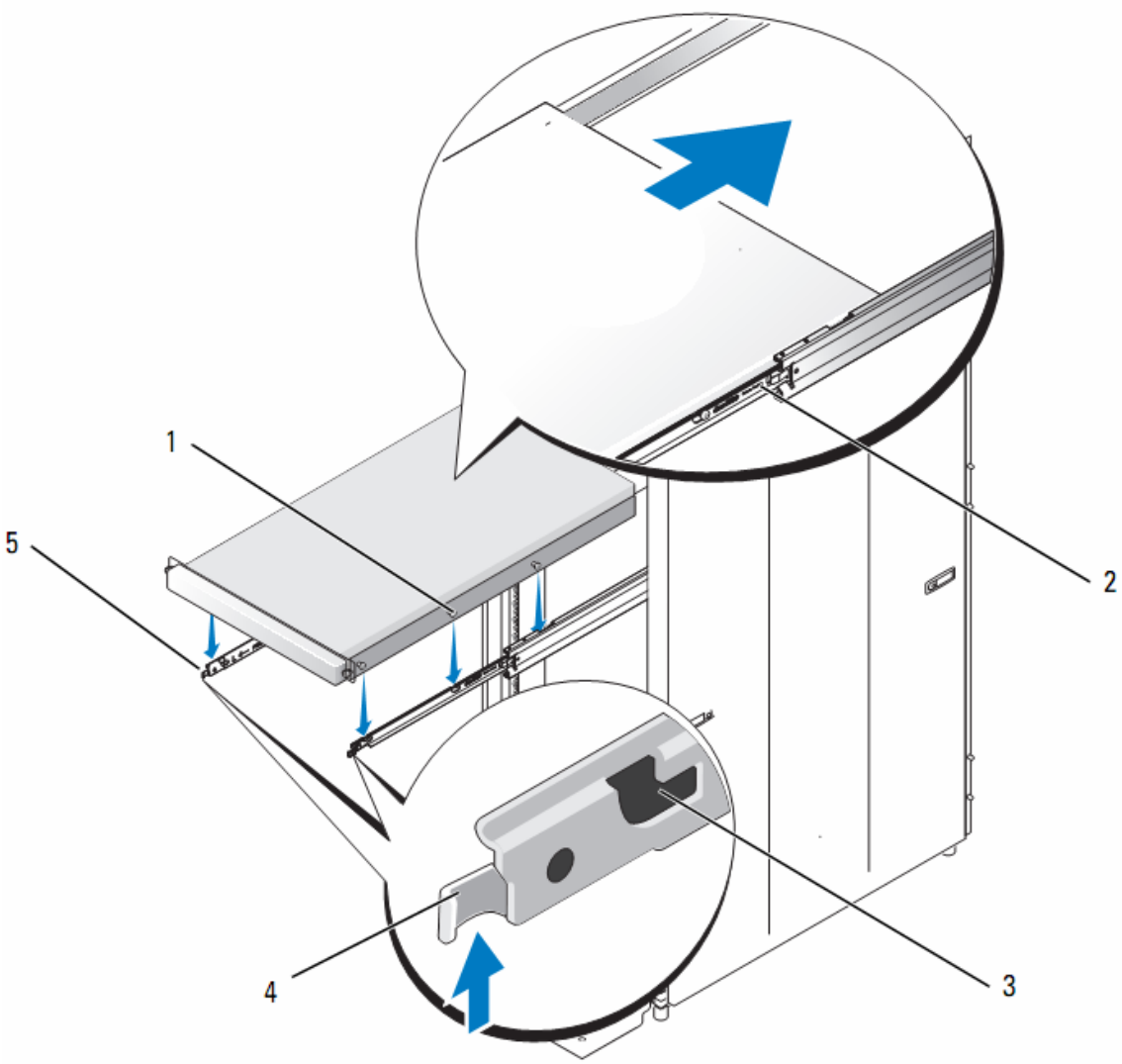
4) Coloque los tornillos de pivote posteriores en sus respectivas ranuras “J”.

5) Baje la parte frontal del sistema y encaje los tornillos de pivote centrales y frontales en sus respectivas ranuras “J” de los ensamblajes deslizantes.
   El pestillo de liberación del sistema de la parte frontal del riel deslizante interno encajará en su sitio cuando el tornillo de pivote encaje en la ranura frontal. Utilice este pestillo de liberación del sistema cuando desee extraer el sistema de los ensamblajes deslizantes.

6) Presione el pestillo de liberación deslizante de la parte exterior de cada riel deslizante interno y, a continuación, inserte el sistema en el rack.

7) Instale el brazo para tendido de cables. Consulte “Instalación de la bandeja y el brazo para tendido de cables.

8) Apriete los tornillos mariposa del panel frontal del rack para fijar los ensamblajes deslizantes al rack.



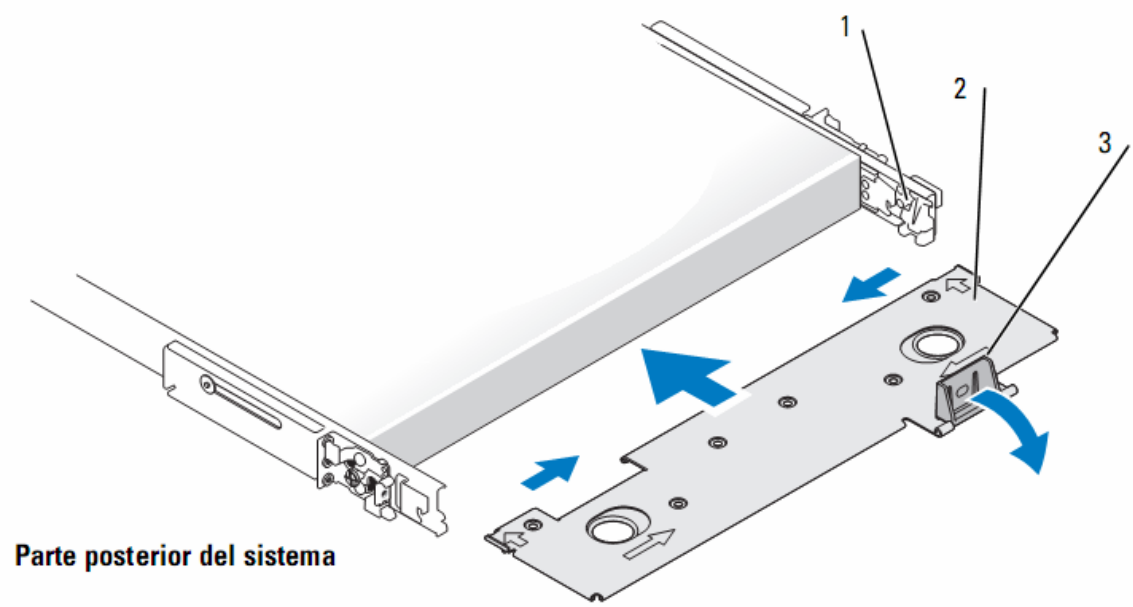
1	Tornillos de pivote (6)	2	Pestillo de liberación deslizante	3	Ranuras J (6)
4	Pestillo de liberación frontal	5	Rieles deslizantes internos (2)		

Fig. 5.11 Instalación de servidor en rieles ya montados en rack.

5.2.4.1 Instalación de Bandeja y Brazo para tendido de cables.

1) En la parte posterior del sistema, ajuste los extremos de la bandeja entre los extremos de los rieles de montaje y deslícela hacia adelante hasta que quede encajada en su sitio.

2) Para preparar la instalación del brazo para tendido de cables, libere el retén del centro del seguro de retención del brazo para tendido de cables y gire el seguro hacia abajo.



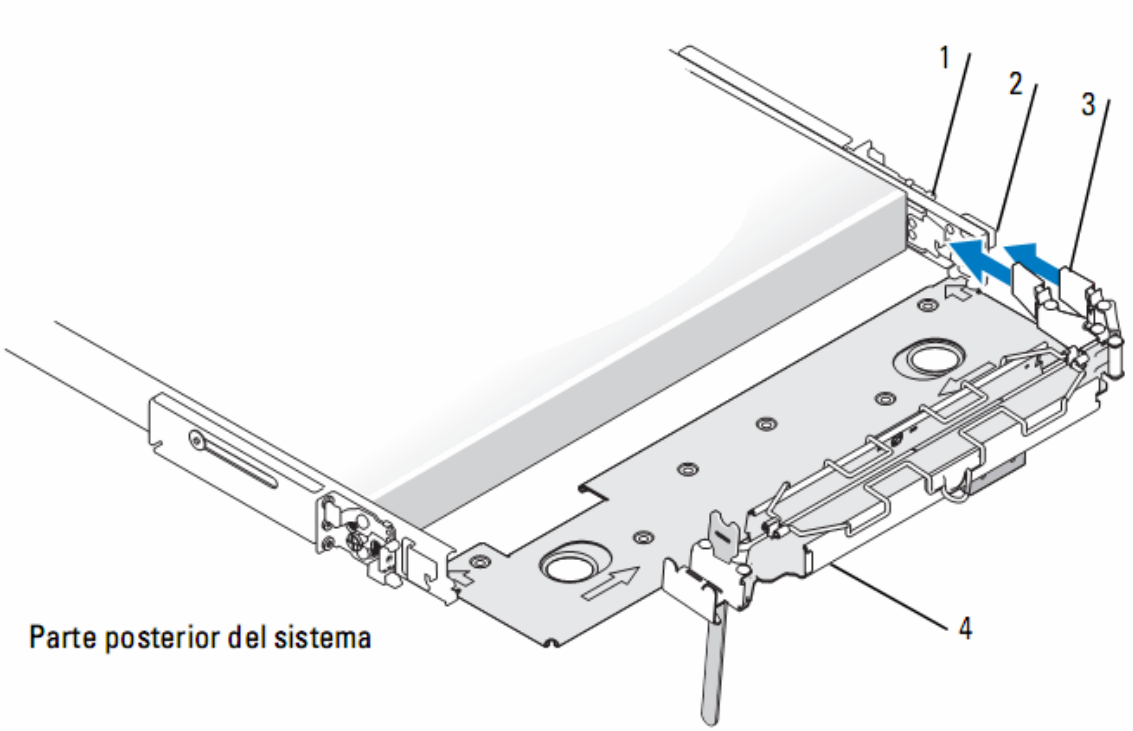
1 Rieles de montaje (2) 2 Bandeja 3 Seguro de retención del brazo para tendido de cables

Fig. 5.12 Instalación de bandeja de cableado.

3) Si es necesario, libere el retén del centro del seguro de retención del brazo para tendido de cables en la bandeja y gire el seguro hacia abajo.

4) En la parte posterior del sistema, encaje el pestillo del extremo frontal del brazo para tendido de cables en el soporte más interno del ensamblaje deslizante hasta que el pestillo encaje en su sitio.

5) Encaje el pestillo del extremo sin fijar del brazo para tendido de cables en el soporte más externo del ensamblaje deslizante hasta que el pestillo encaje en su sitio.



1	Rieles de montaje (2)	2	Soportes (2)	3	Pestillos (2)
4	Brazo para tendido de cables				

Fig. 5.13 Instalación de Brazo de cableado.

5.3 Instalación DAS.

5.3.1 Instrucciones Generales de Instalación.

En este apartado se proporcionan instrucciones para técnicos de servicio especializados que instalen uno o más sistemas en un armario tipo gabinete. Se cuenta con un kit de rack RapidRails que lo fabrica DELL, se puede montar en todos los armarios del fabricante sin herramientas, y el kit de rack VersaRails se puede montar en la mayoría de los armarios rack estándar del sector. Los procedimientos para instalar los kits de rack RapidRails y VersaRails son similares. Para cada sistema que se montará en el armario se precisa un kit de rack.

A continuación, brindaremos procedimientos para los kits de rack de cuatro postes siguientes:

- Kit de rack de rieles deslizantes
- Kit de rack de rieles estáticos (versiones RapidRails y VersaRails)

AVISO: el kit de rack VersaRails lo deben montar únicamente técnicos de servicio cualificados en un rack que cumpla las especificaciones siguientes:

- ANSI/EIA-310-D-92, IEC 297 y DIN 41494[34].

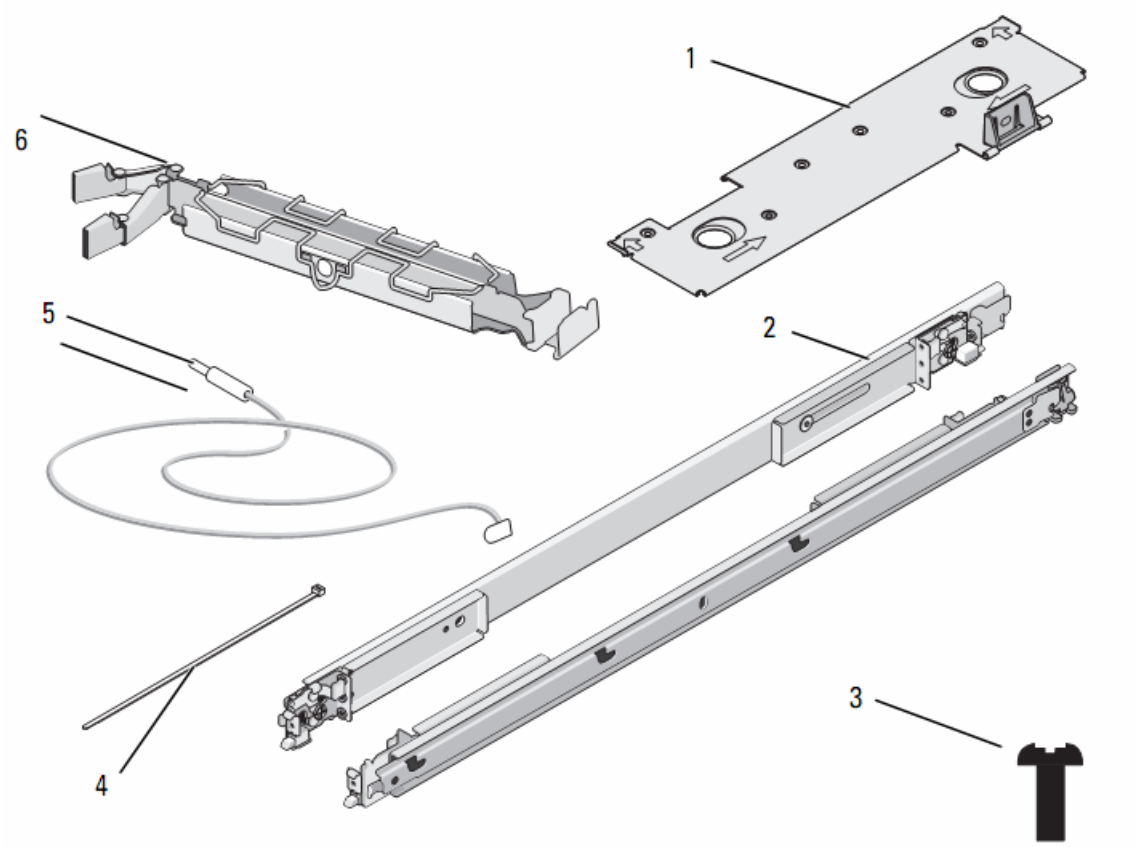
5.3.2 Configuración de rieles deslizantes.

5.3.2.1 Contenido del kit para rack de rieles deslizantes.

- Un par de ensamblajes deslizantes (convertibles a la configuración RapidRails o VersaRails)
- Un brazo para tendido de cables
- Una bandeja
- Un cable de indicador de estado (si procede)
- Abrazaderas para fijar los cables al brazo para tendido de cables

[34] ANSI/EIC: American National Standard Institute/Electronic Industry Association, IEC: International Electronic Comisión, DIN: Deutsches Institut für Normung

- Ocho tornillos Phillips con arandela 10-32 x 0,5 pulgadas (utilizados únicamente en la configuración VersaRails)



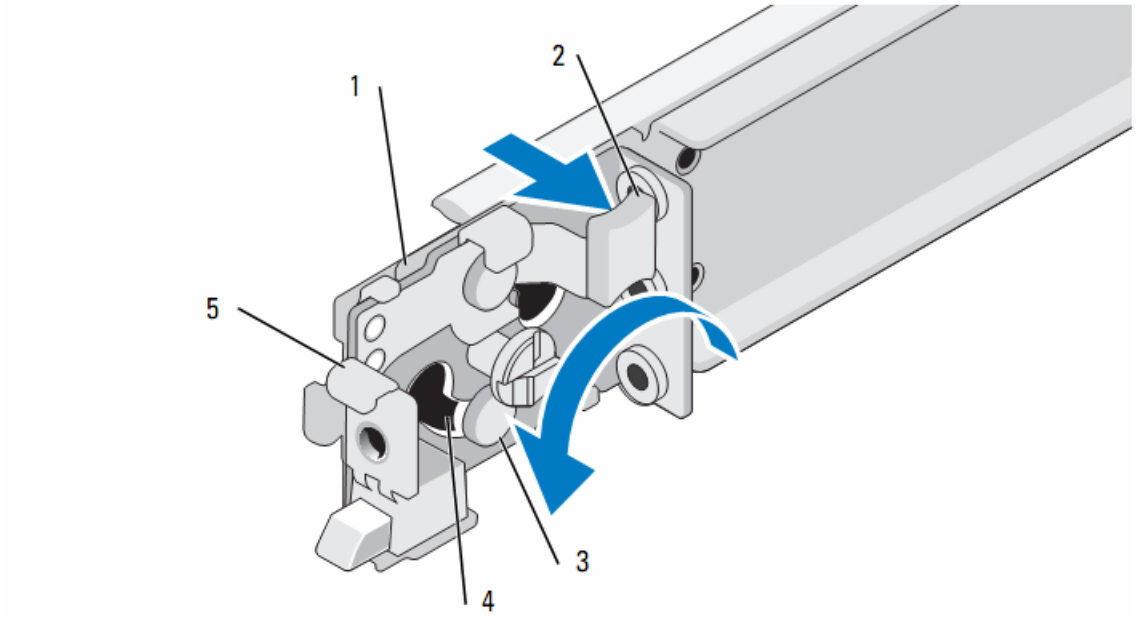
1	Bandeja	2	Ensamblajes deslizantes (2)	3	8 tornillos Phillips con arandela 10-32 x 0,5 pulgadas (únicamente en la configuración VersaRails)
4	Abrazaderas	5	Cable de indicador de estado (si procede)	6	Brazo para tendido de cables

Fig. 5.14 Contenido de kit de servidores para montado en rack.

El ensamblaje de rieles deslizantes presenta un soporte de montaje giratorio en cada extremo del riel. La posición del soporte determina si el ensamblaje de rieles se utiliza como RapidRail o como VersaRail. El lado RapidRail del soporte tiene un gancho y un pestillo que lo fijan al riel vertical. El lado VersaRail del soporte tiene tres orificios y se fija al riel vertical mediante tornillos.

Para girar el soporte de montaje y cambiar los rieles de montaje de RapidRails a VersaRails

5) Levante la palanca de liberación del soporte de montaje giratorio.
6) Gire el soporte y levántelo para sacarlo de los dos topes.
7) Continúe girando el soporte 180 grados hasta que pueda volver a colocar las muescas sobre los topes.
8) Gire el soporte en la dirección contraria sobre los topes hasta que el soporte encaje en su sitio.



1	Soporte giratorio	2	Palanca de liberación	3	Topes (2)
4	Muescas (2)	5	Superficie de montaje del soporte (configuración RapidRails)		

Fig. 5.15 Cambio de la posición del soporte de montaje giratorio

5.3.3 Instalación de rieles estáticos en Gabinete.

1) Para instalar un módulo de rieles, localice las tres ranuras en forma de cerradura del módulo de rieles y los tornillos de pivote correspondientes en el lateral del sistema.

2) Coloque el módulo de rieles al lado del sistema de modo que los tornillos de pivote se ajusten a la parte redonda de las ranuras y, a continuación, inserte el módulo hacia la parte posterior del sistema.
3) Repita los pasos 1 y 2 para instalar el otro módulo de rieles.
4) Para extraer un módulo de rieles del chasis, tire del pestillo de liberación, deslice el riel hacia adelante y extraiga el módulo de rieles del chasis.

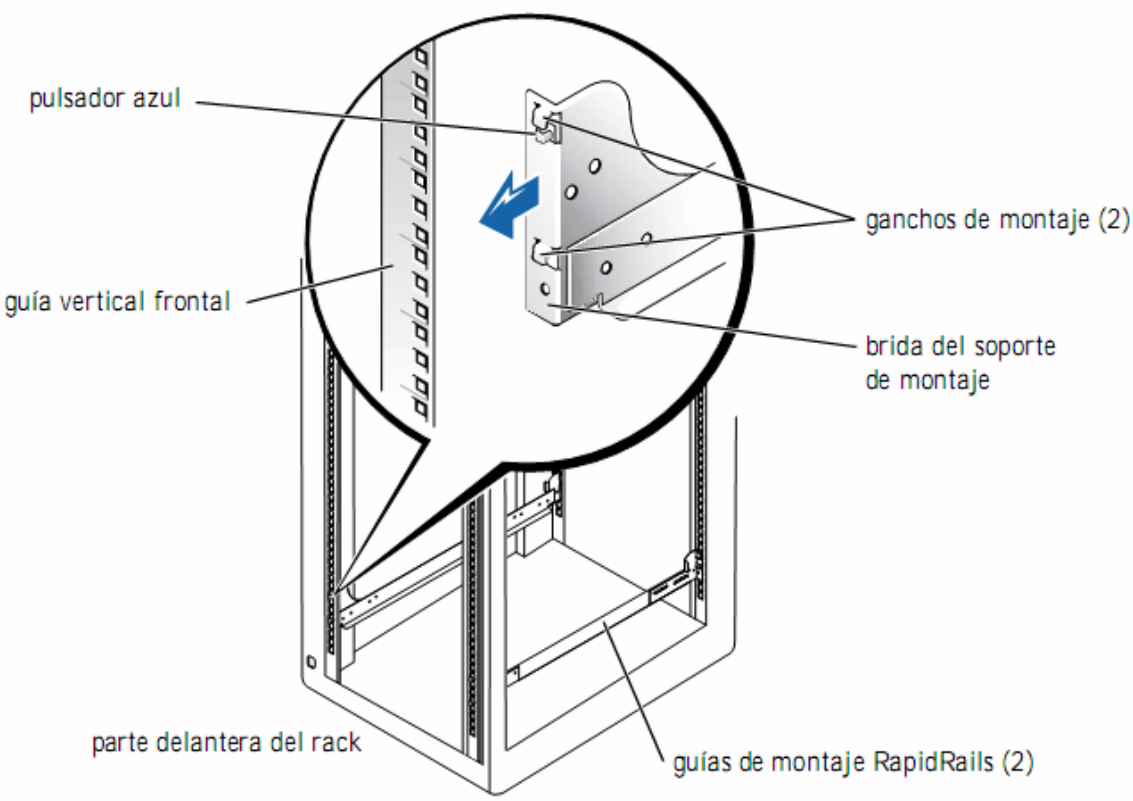


Fig. 5.16 Instalación y extracción de los módulos de rieles estáticos del chasis.

6) En la parte frontal del armario rack, coloque uno de los rieles de montaje de forma que la superficie de montaje del soporte quede situada entre las marcas o la cinta que ha colocado (o las posiciones numeradas) en los rieles verticales. El gancho de montaje superior de la superficie de montaje de soporte frontal debe entrar en el orificio superior entre las marcas realizadas en los rieles verticales.

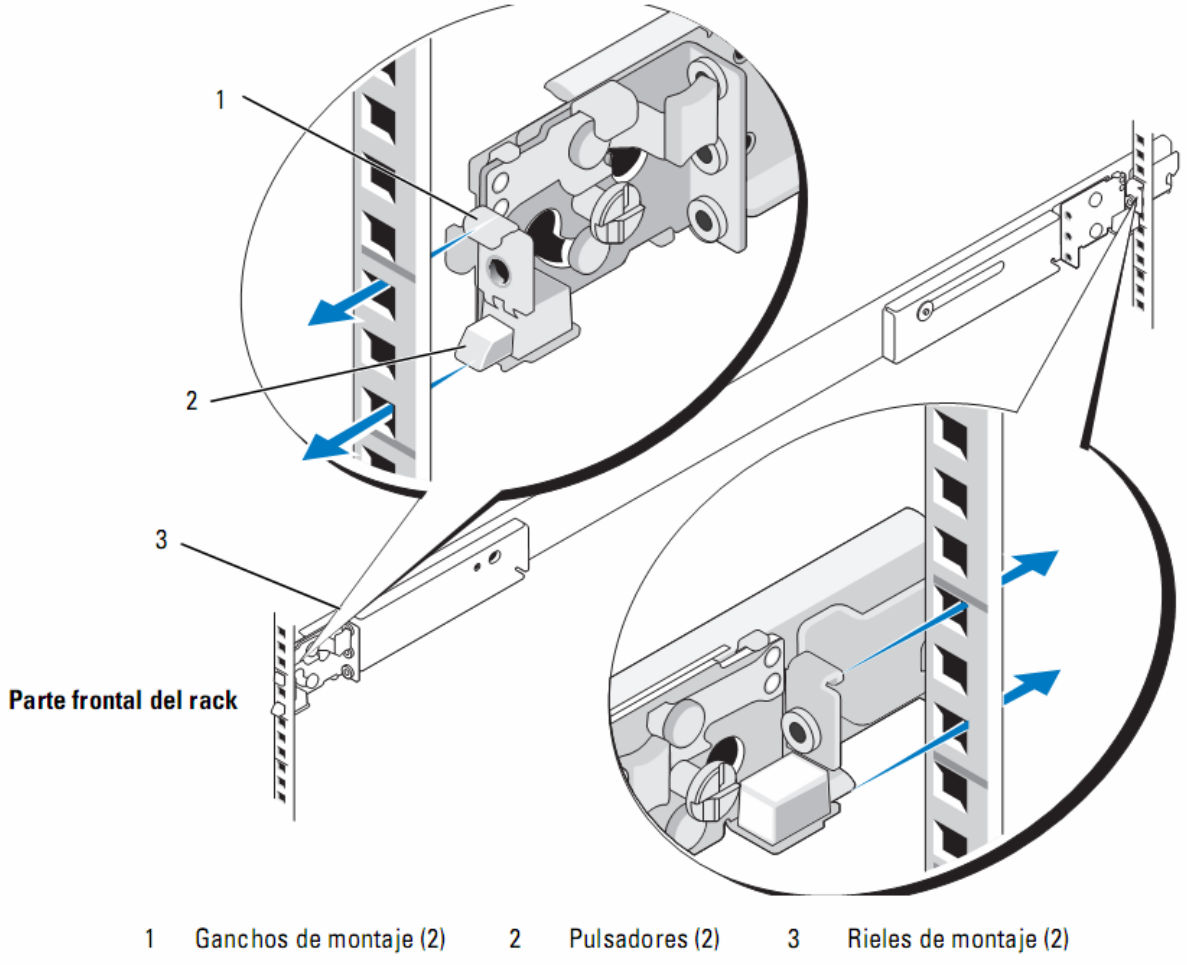


Fig. 5.17 Instalación de los rieles de montaje RapidRails.

7) Empuje el riel de montaje hasta que el gancho de montaje entre en el orificio cuadrado correspondiente. A continuación, presione hacia abajo la superficie de montaje del soporte hasta que el gancho de montaje quede encajado y el botón de presión salga por el orificio cuadrado inferior

8) En la parte posterior del armario, tire hacia atrás de la superficie de montaje hasta que el gancho de montaje encaje en el orificio cuadrado superior y, a continuación, empuje hacia abajo la superficie hasta que el gancho de montaje quede encajado y el botón de presión salga por el orificio cuadrado inferior.

9) Repita del paso1 al paso3 para el riel de montaje del otro lado del rack.

10) Asegúrese de que los rieles de montaje estén montados en la misma posición vertical en ambos lados del rack.

5.3.4 Instalación Direct Attached Storage.

PRECAUCIÓN: si va a montar más de un sistema, monte el sistema más pesado en la posición más baja que haya disponible en el rack y nunca extraiga más de un componente del rack a la vez.

1) Levante el sistema hasta colocarlo frente a las guías de montaje instaladas en el armario rack.

PRECAUCIÓN: debido al tamaño y el peso del sistema, no intente nunca montar el sistema en las guías sin ayuda.

2) Inserte el sistema en el rack que el panel frontal esté colocado contra las guías verticales.

3) Apriete los tornillos de mano integrados en cada lado del panel frontal del sistema.

4) Consultando las imágenes siguientes, se completa esta tarea de ubicar en el Rack, el dispositivo de alta capacidad de almacenaje.

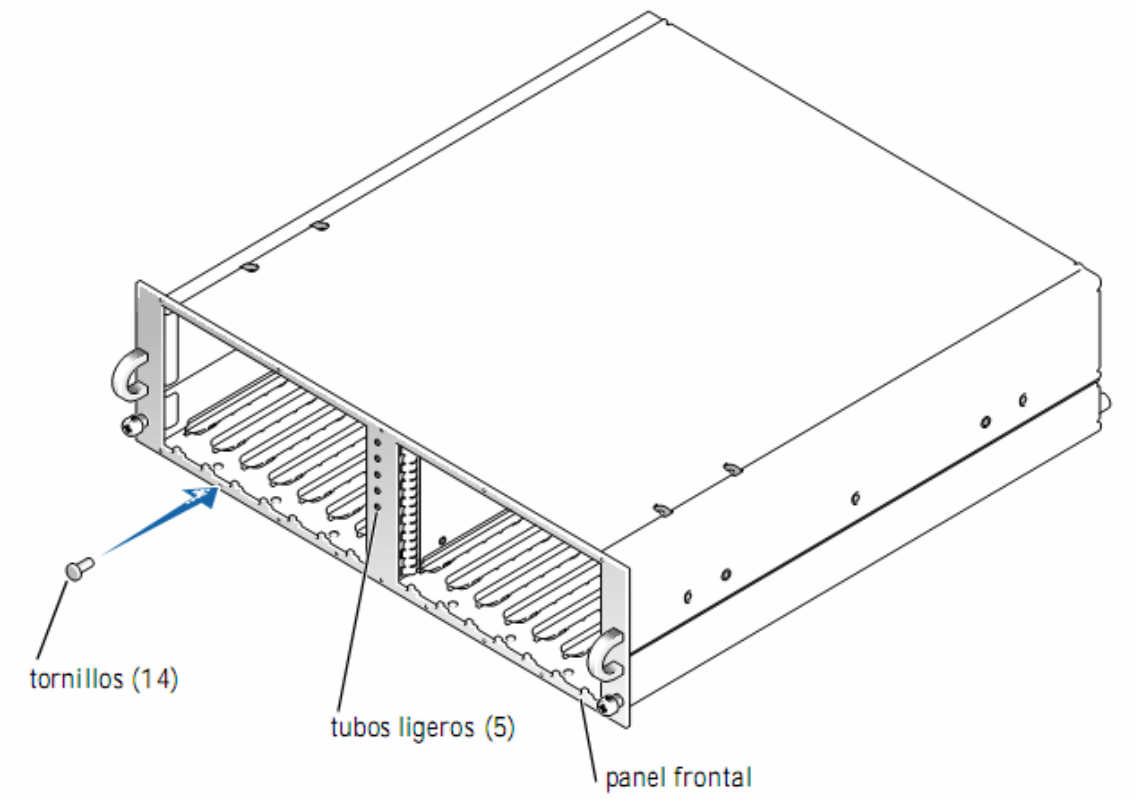


Fig. 5.18 DAS

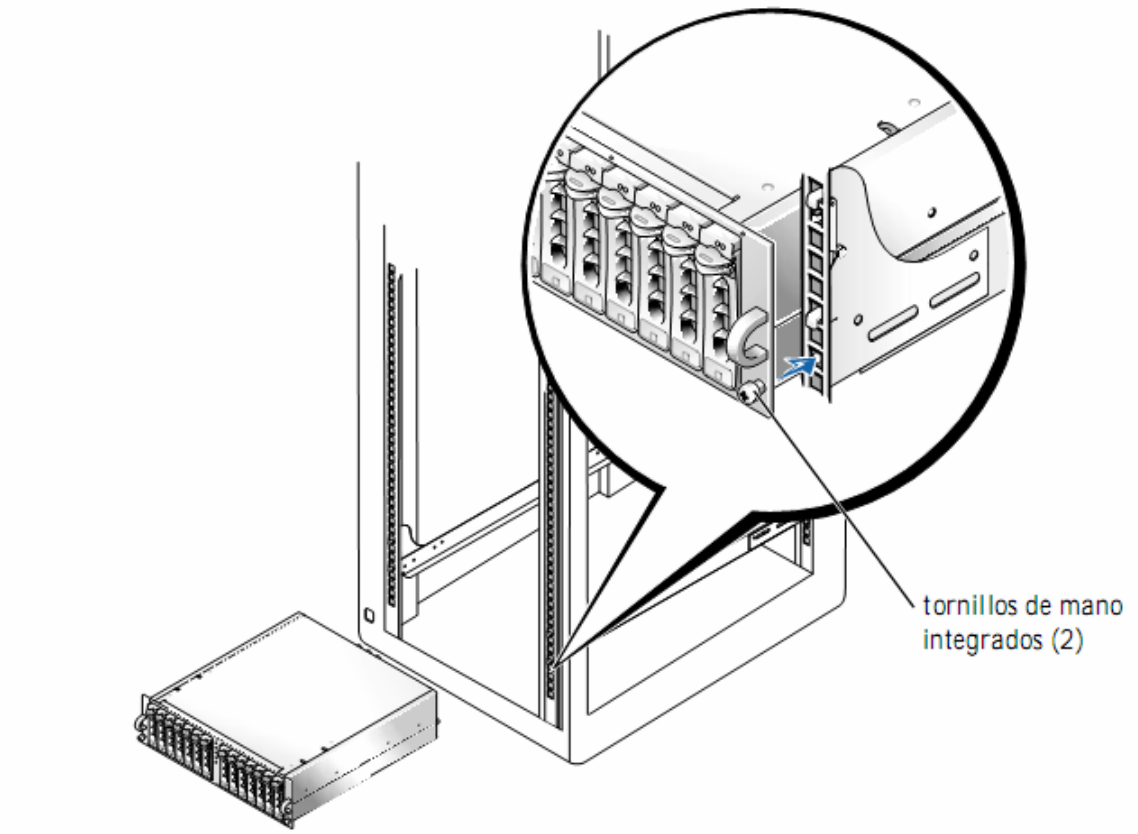


Fig. 5.19 Montaje de DAS en la parte baja del rack debido a su peso.

5.4 Diseño de ubicación CE.

Generalidades.

La distribución dentro del recinto que albergara el hardware, es de alta importancia, ya que debe de aprovecharse al máximo la distribución de espacios para las partes más importantes que estarán contenidas en ese lugar, como lo son el gabinete de servidores, gabinete de comunicaciones, instalación eléctrica y distribución de sistema de conservación de temperatura ambiental, a continuación se detalla un diagrama en vista de planta, que sirve de referencia y recomendación de distribución de estos elementos indispensables para el correcto procesamiento de la información. Además, de sugerir de manera grafica, los lugares para la ubicación de dispositivos de seguridad de acceso, y elementos de mitigación en caso de incendios.

5.4.2 Diseño de Planta General del CE.

El diseño de planta, para la distribución de los elementos de procesamiento de la información, la ubicación de los dispositivos de comunicaciones y parte eléctrica, nos brinda la mejor opción de visualización de colocación de cada una de estas secciones indispensables de infraestructura de TI, con la inclusión de una proyección de crecimiento en hardware en las áreas ya descritas.

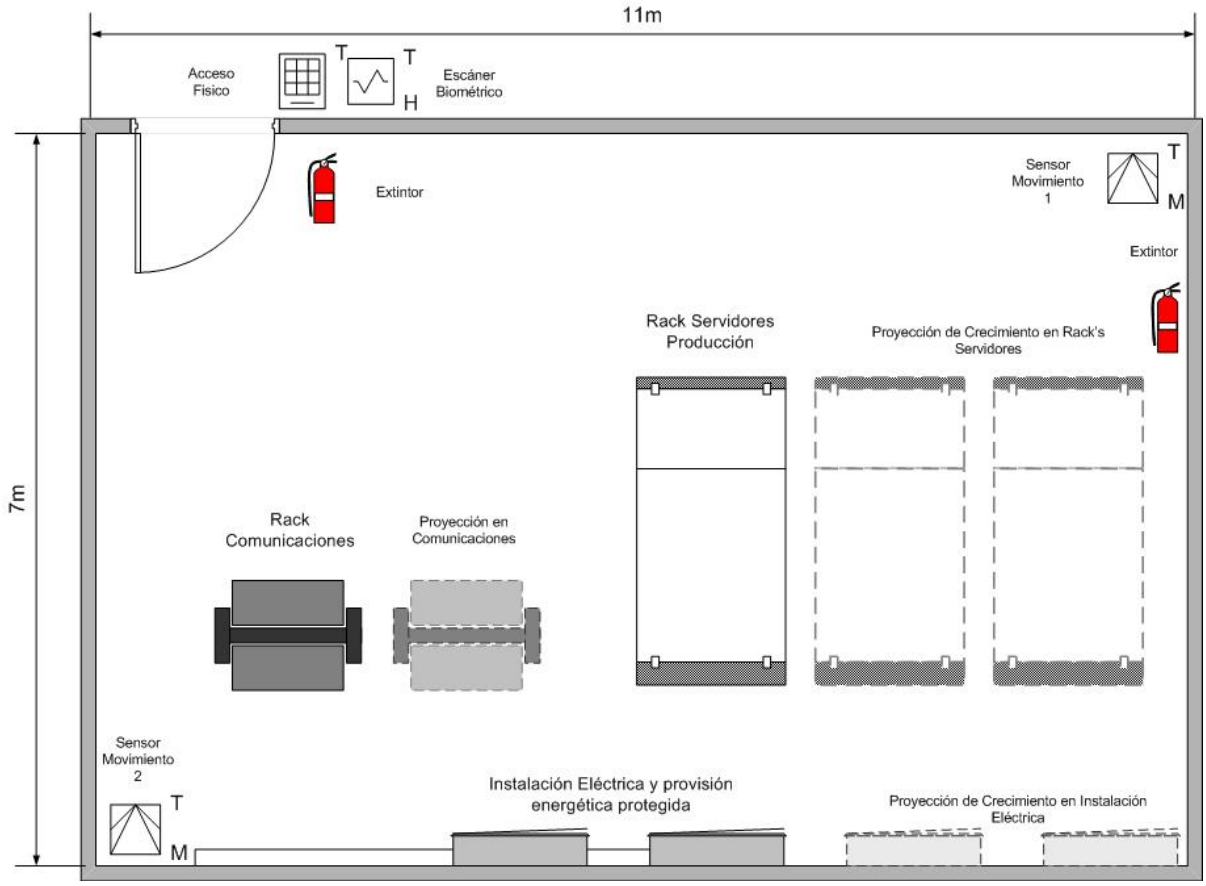


Fig. 5.20 Diseño de Planta para distribución de equipos en CE.

5.4.2 Diseño de Planta sistema de conservación de temperatura ambiental.

En el orden de establecer una cobertura adecuada y correcta del mantenimiento de temperatura ambiental necesaria dentro del CE, se recomienda una distribución de aire frío, por medio de distribución de tubería elevada dentro del falso cielo del recinto de equipos. Esto con el objetivo de intercambiar el aire del cuarto de equipos a razón de una vez cada hora, para extraer el calor del recinto e intercambiarlo por aire nuevo, y así mantener el ciclo continuamente.

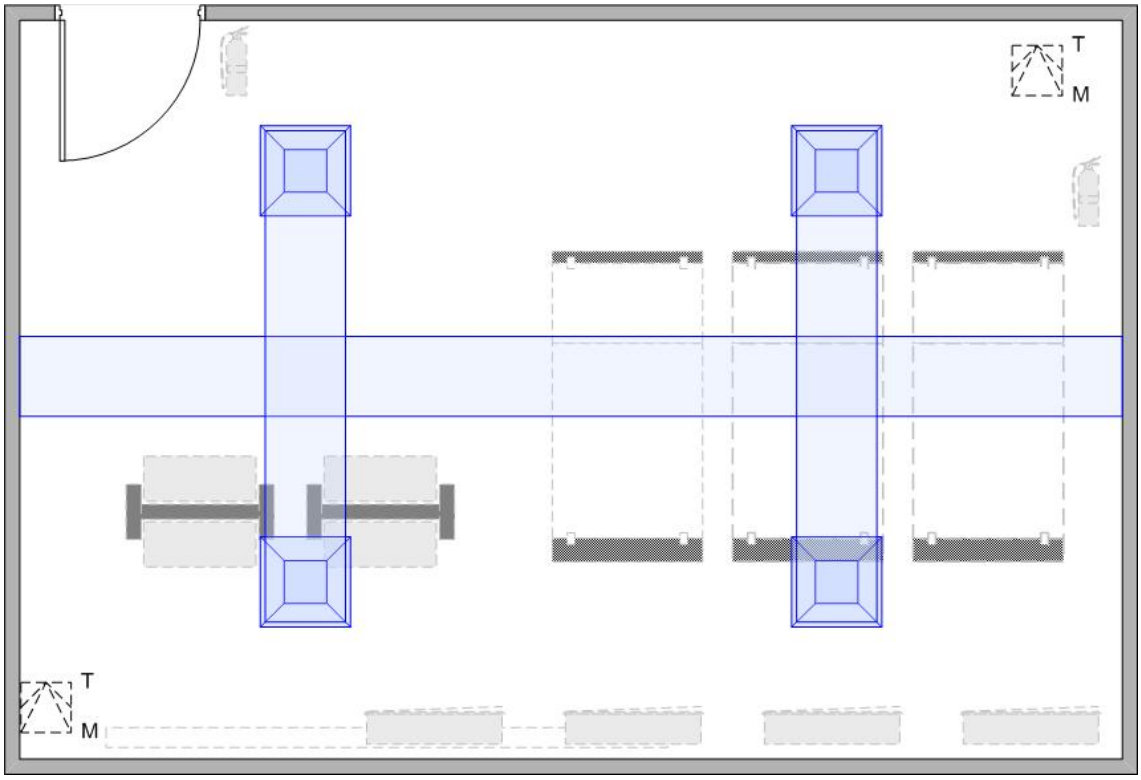


Fig. 5.21 Diseño de Planta para distribución de aire acondicionado dentro del CE

5.4.2.1 Recomendación de Sistema de Conservación de temperatura ambiental.

El equipo de aire acondicionado, debe poseer la característica de entregar aire seco, es decir libre de humedad. Esto se logra por medio de la selección adecuada del equipo de enfriamiento, que no entregue aire acondicionado convencional el cual contiene niveles de oxigeno, necesarios para los seres humanos, pero no así para los equipos de procesamiento de la información, ya que procura, con el pasar del tiempo, la oxidación de estos, ya que están hechos en su mayoría de materiales metálicos y por tanto expuestos a la oxidación y deterioro ambiental.

CAPITULO VI. Seguridad Virtual, Administración de usuarios y Servicios de aplicaciones Web.

6.1 Seguridad Virtual.

Generalidades.

La necesidad de seguridad ha existido desde la introducción del primer equipo. El paradigma ha cambiado en los últimos años, sin embargo, la terminal de los sistemas de servidor central, el modelo cliente - servidor de sistemas, a la ampliamente distribución del Internet.

Aunque la seguridad es uno de los aspectos más importantes, no siempre ha sido un aspecto crítico para una institución de éxito. Con un sistema Servidor Central Principal, que estuvo importantemente para la protección de sus sistemas se puede dar el uso indebido de recursos, tanto los usuarios autorizados a estos recursos o usuarios no autorizados a acceder y utilizar los recursos de respaldo. Resultaba perjudicial el mal uso de estos recursos ya que estos eran costosos en los primeros días en que se implementaba este modelo.

A medida que la tecnología desarrollaba y el costo de los recursos de los sistemas se redujo, este factor de seguridad se convirtió en menos importante. Acceso remoto a

sistemas de una institución fuera de la red era casi inexistente. Por otra parte, sólo la comunidad informática de la institución, poseían los conocimientos necesarios para acceder de manera remota a los sistemas basados en arquitectura de Servidor Principal.

6.1.1 Seguridad en un enlace publico a Internet.

Una institución que sólo tiene una oficina y alberga todos sus servidores en casa, se considera un servicio centralizado de TI. Incluso en este escenario simple, usted tiene varias opciones en cuanto a donde puede colocar sus servidores,

Una opción es colocar todos los servidores en una red principal detrás de un muro de fuego, de la institución. Esta es la configuración más sencilla para diseñar y desplegar en la red, pero no la más segura. Por ejemplo, ¿qué sucede si usted se olvida de instalar el parche de seguridad más reciente en el servidor Web? El cual puede ser el caso que estudiamos en esta GRT. En esta configuración, es el servidor Web que se ve mas comprometido, es sólo una cuestión de tiempo antes de que el atacante gana el control de cada sistema de su red, inclusive el servidor que almacena la información mas sensible de la institución, información critica de alumnos y código fuente de aplicaciones.

6.1.2 DMZ

Una Zona Desmilitarizada (DMZ por sus siglas en ingles). Es la parte de una red privada que es visible a través de la red con contrafuegos o firewall. Este término fue determinado a finales de 1990 como el termino referente a la frontera de un ámbito de TI que tiene como infraestructura una institución o empresa.[†]

[†] El concepto de DMZ es tratado también en la sección **3.3.2.2 Objetivos de seguridad de servidor Web integrado a red local.** de este documento. Con la visión en una institución de educación superior.

Para mitigar el riesgo que describimos en la introducción del apartado 6.1.1 se recomienda colocar sus servidores de acceso público (servidores Web, servidor de correo, servidores FTP, etc.) en lo que se denomina una zona desmilitarizada (DMZ). Una zona desmilitarizada es una red separada físicamente de su red corporativa interna. Al mover los recursos sensibles en una subred fuera de la zona desmilitarizada, una institución de educación superior, puede proteger mejor los recursos internos, los recursos que no necesitan ser visitados desde Internet. Los atacantes se centrarán en los servidores que enfrenta la Internet; Es decir, los que dentro de la zona desmilitarizada. Pero incluso un ataque con éxito allí no debe comprometer el resto de sistemas en su red corporativa.

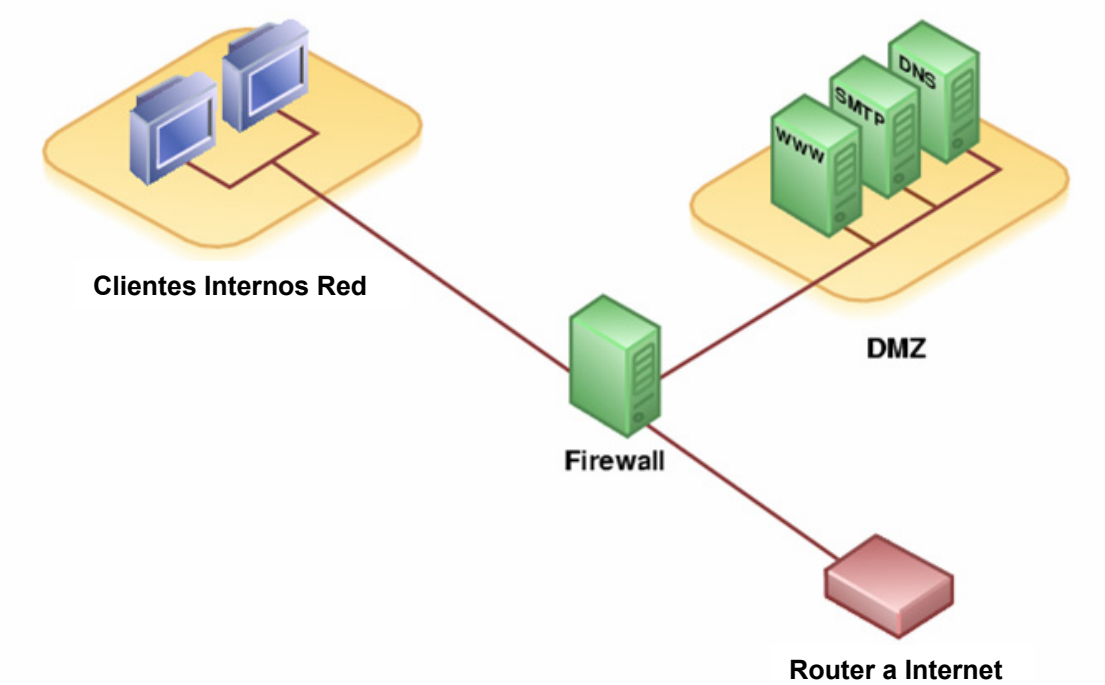


Fig.6.1 Diseño General de una DMZ con Servidores públicos diseccionados a través de un Firewall.

6.1.3 Firewall's

El primer paso en la ejecución física de su infraestructura de seguridad es determinar qué tipo de perímetro de seguridad que funciona mejor en su entorno. Perímetro de

seguridad, por lo general un cortafuegos, es la primera línea de defensa en activo y la protección de los recursos.
Cuando un visitante malicioso, un espía industrial o un Hacker, por ejemplo, lanza un ataque en su red, la primera zona que buscamos que ataque es hacia nuestro perímetro de seguridad.
Los cortafuegos son un componente clave en su infraestructura de seguridad. Configurado adecuadamente, pueden proteger de un gran porcentaje de ataques.

En general, un firewall es un dispositivo o conjunto de dispositivos que restringen el acceso de confianza entre las redes. La mayoría de las veces, los firewalls proteger una red de confianza institucional de la Internet que no es confiable. También se pueden usar firewalls para proteger a una subred corporativa sensible de un público que encontramos dentro de nuestra red.

Los cortafuegos son la base de su infraestructura física. Sin ellos, no tiene nada que ofrecer para una capa de seguridad en su red.

6.1.3.1 La Arquitectura de selección de subred.

La arquitectura de selección de subred añade otra capa de seguridad a la arquitectura de Firewall tradicional la cual busca aislar el perímetro de admisión.

Un perímetro de selección de subred, una red adicional situada entre la Internet y su red interna para proporcionar un mayor nivel de seguridad. Esta red también se conoce como una zona desmilitarizada DMZ.

La incorporación de dos routers de firewall y un servidor Proxy añade tres capas de seguridad que un atacante debe llegar a penetrar en su red. El servidor Proxy se sienta en su propia red, que comparte sólo la proyección con los routers. En esta red,

el router interior de selección, controla el tráfico local y el router exterior monitorea y controla las entradas y salidas del tráfico de Internet.

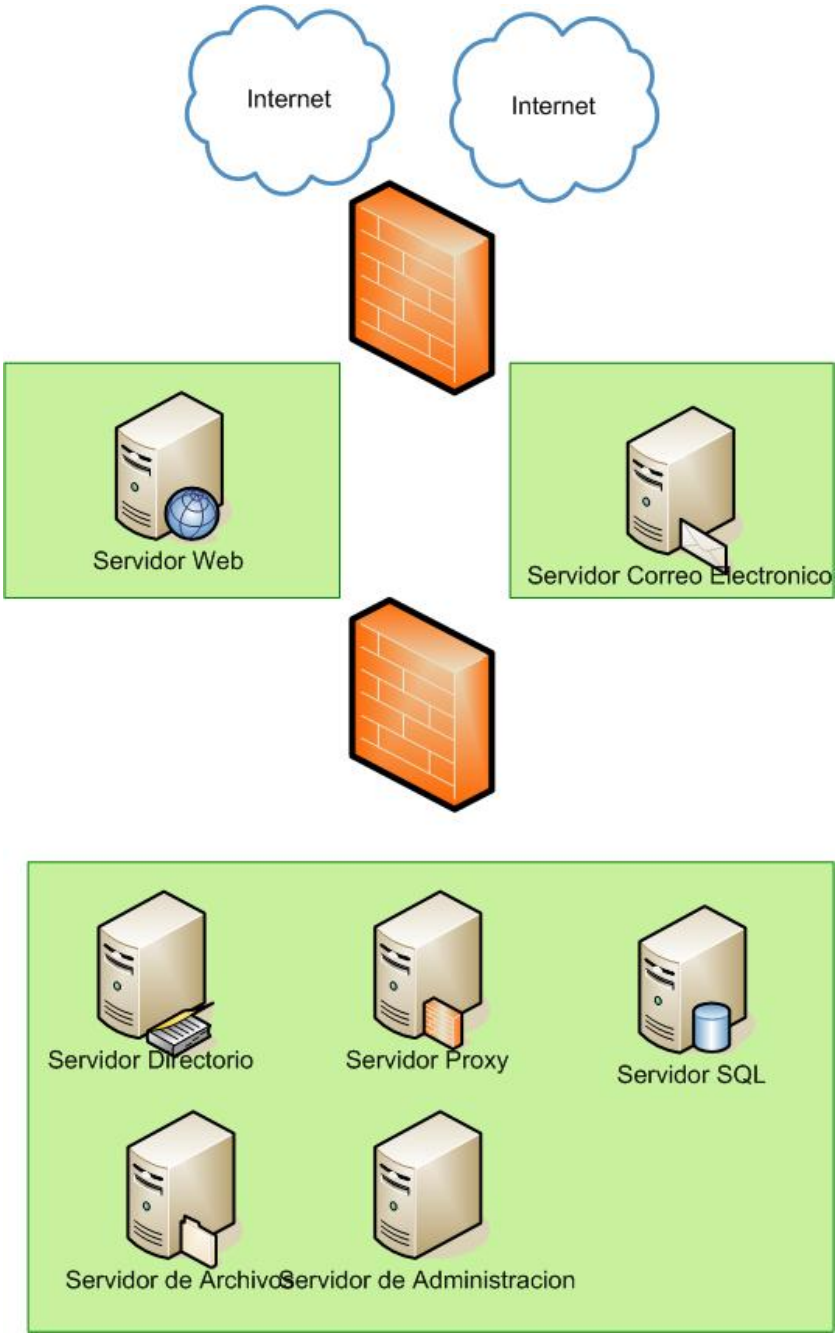


Fig.6.2 Diseño General de una Infraestructura de Selección de Subred con doble Firewall y un Proxy Server

6.2 Administración de Seguridad de Red.

La administración de la red, es la parte coherente a definir, luego de construir una robusta y escalable solución de comunicación para las distintas terminales y servidores que la componen. La materia de seguridad de red, estará siempre mejor soportada por procedimientos concretos de confirmación, segmentación y delegación de responsabilidades, Monitoreo de los recursos y servicios de TI. Todo esto administrado por personal calificado con alto sentido de la seguridad, visionarios de amenazas y que sean capaces de montar un modelo de prevención y no de corrección.

6.2.1 Definiciones de Roles.

Tomando en cuenta la asignación de responsabilidades que debe existir en el área de TI, para cumplir con las mejores practicas de administración de la información, y las recomendaciones que Microsoft nos hace a través del Microsoft Operation Frameworks[†], planteamos el modelo de roles mas importantes en relación a la seguridad de la información, tanto en infraestructura como en seguridad lógica de TI, a continuación describimos la consistencia de los roles mencionados, sus actividades y los objetivos que se busca se cumplan.

6.2.1.1 Rol Operaciones.

El rol de operaciones debe ser el responsable de las siguientes funciones de servicio para los recursos de TI:

- Función de administración del sistema.
- Función de administración de los directorios de servicios.
- Función de administración de redes.
- Función de monitoreo y control del servicio.
- Función de gestión del almacenamiento.

[†] ***Microsoft Operations Frameworks***, es una guía para hacer de las actividades del entorno de TI, confiables, y efectivas en costo.

Fig.6.3 Rol de Operaciones, Administrador general de recursos de TI, se diagraman los sectores de todo el entorno de TI de una Institución.

6.2.1.1.1 Función de administración del sistema.

El rol de operaciones debe ser el responsable de la administración diaria de los sistemas de computación y redes en general. También es responsable de los recursos de computación como los servidores de información Web, servidores de impresión, servidores de base de datos y servidores de aplicaciones.

Objetivos de la función:

- Regular todas las funciones del rol de operaciones.
- Implementar físicamente todos los cambios aprobados.
- Cumplir con los acuerdos del nivel de operación.
- Asegurar que los estándares de operación se aplican correctamente.

Resultados esperados:

- Gestión y control de las cuentas de la red.
- Gestión y control de los recursos de la red.

6.2.1.1.2 Función de administración de los directorios de servicios.

El rol de operaciones debe ser el responsable de proporcionar una vista consistente del directorio, una infraestructura de directorios segura y un monitoreo completo con el fin de identificar y resolver incidentes.

Objetivos de la función:

- Proveer el acceso a la información de la institución.
- Mantener consistencia entre distintos tipos de directorios.
- Reducir el costo de mantener los datos de la institución.
- Reducir el tiempo de propagación de los cambios a los datos de la institución.
- Hacer que los datos de la institución sean fáciles de acceder y usar.

Resultados esperados:

- Un solo repositorio de datos.
- Habilidad de los usuarios y las aplicaciones de encontrar recursos en la red. Los recursos de la red pueden ser usuarios, aplicaciones, servidores, impresores y otros.

6.2.1.1.3 Función de administración de redes.

También debe ser el responsable de proveer una infraestructura de red confiable, consistente, escalable y segura.

Objetivos de la función:

- Asegurar la conectividad.
- Asegurar el rendimiento.
- Proporcionar capacidad y volumen fiables.

- Diagnosticar y corregir problemas.

Resultados esperados:

- Una red consistente y fiable.
- Prestación de los servicios adecuados a los usuarios.
- Minimización de cambios en la red.
- Manejo eficiente de incidentes y problemas.
- Menor riesgo de fallas.

6.2.1.1.4 Función de monitoreo y control del servicio.

El rol de operaciones debe ser el responsable de definir alertas para monitorear el cumplimiento de los objetivos de servicio y promover las medidas correctivas cuando se presentan las alertas.

Objetivos de la función:

- Asegurar que se cumplen los niveles de servicio prometidos.
- Permitir que operaciones vea la salud de los servicios en tiempo real.
- Proporcionar a operaciones con monitoreo preventivo y correctivo.

Resultados esperados:

- Enfoque en la disponibilidad de los servicios más que en la disponibilidad de los componentes.
- Disminución del número de violaciones de los acuerdos de servicio[†].
- Mayor conocimiento de los componentes claves.
- Mayor disponibilidad de servicios.
- Mayor satisfacción del usuario con los servicios recibidos.

[†] Un **servicio de TI** es un conjunto de actividades que buscan responder a una o más necesidades de un cliente por medio de un cambio de condición en los bienes informáticos potenciando el valor de estos y reduciendo el riesgo inherente del sistema.

6.2.1.1.5 Función de gestión del almacenamiento.

Los recursos que se necesitan para el almacenamiento de los datos.

Objetivos de la función:

- Proporcionar la clasificación, almacenamiento, restauración y recuperación de los datos.
- Proporcionar el almacenamiento histórico de los datos.
- Asegurar físicamente todos los respaldos de datos.
- Mantener y rastrear los datos en el ambiente de producción.

Resultados esperados:

- Definición de los requerimientos de almacenamiento alineados con las necesidades del negocio.
- Monitoreo, mantenimiento y optimización de la infraestructura de almacenamiento.
- Almacenamiento en concordancia con las políticas de seguridad.
- Sistemas de clasificación de datos.

El principal proceso de esta función es el respaldo de los datos.
El respaldo consiste en copiar los datos a un medio diferente del almacenamiento operativo con el fin de protegerlos contra pérdidas imprevistas o corrupción de los mismos.

Hay dos grupos grandes de almacenamiento:

- Datos guardados en servidores. Son de uso común. Su respaldo debe ser responsabilidad del Rol de Operaciones.
- Datos guardados en las computadoras personales.
  Son de uso particular de cada empleado. Su respaldo debe ser responsabilidad del empleado.

6.2.1.2 Rol de Seguridad.

El principal responsable de asegurar que exista seguridad en el acceso a la información de la institución es el rol de seguridad tanto de manera lógica, como física, pero en esta ocasión estudiaremos la seguridad de la parte lógica, ya que el acceso físico esta contemplado en la sección: 4.1 Áreas seguras infraestructura civil de tratamiento de la información. De este documento.

El modelo de roles se detalla en el documento Microsoft Operations Framework 4.0, Sección: “Team Service Management Function“.

El rol de seguridad tiene las siguientes atribuciones:

- Asegura la confidencialidad, integridad y disponibilidad de los datos.
- Propone políticas, como definir el procedimiento a seguir cuando alguien se le retiran los privilegios de acceso a la información.

El rol de seguridad debe ser el responsable de las siguientes funciones de servicio:

- Función de administración de la seguridad.
- Función de gestión de la seguridad.

Ambas se detallan a continuación.

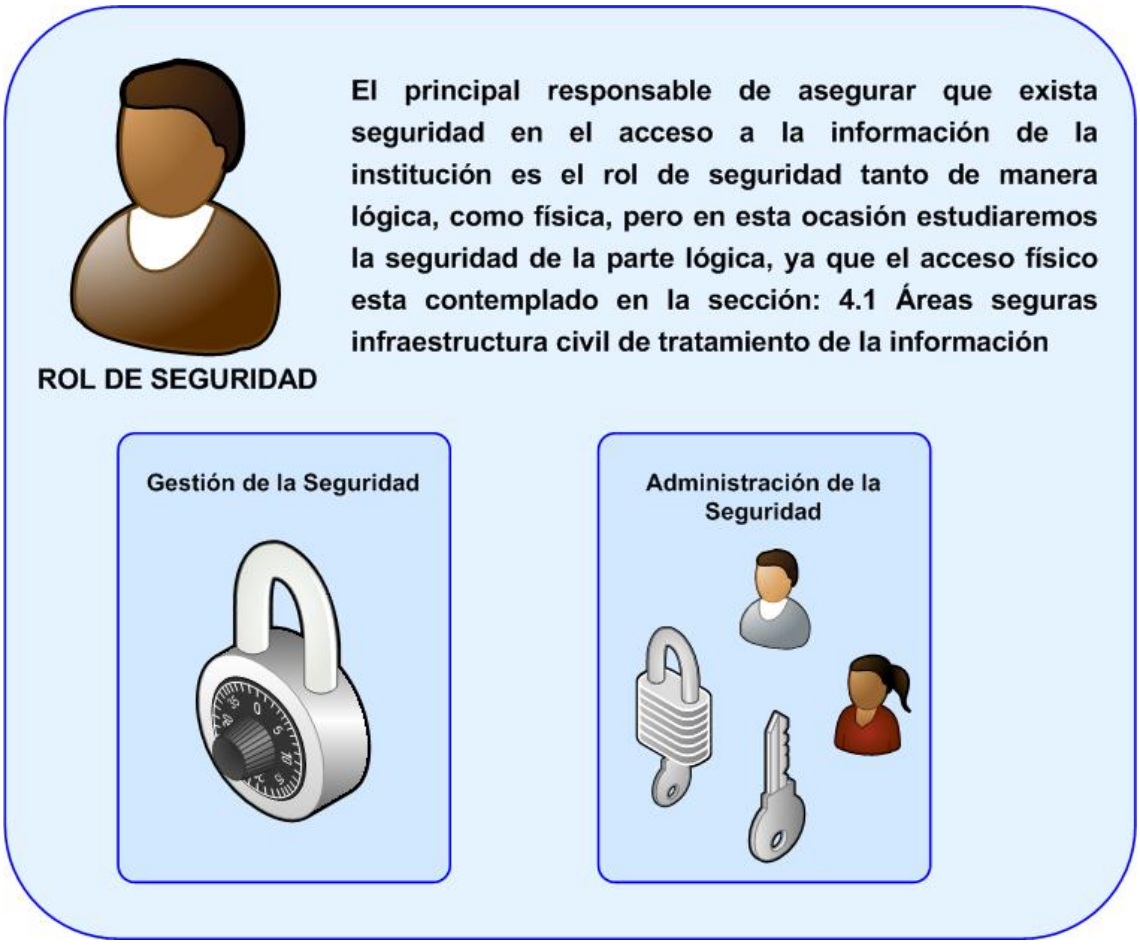


Fig.6.4 Rol de Seguridad, Gestiona y promueve la seguridad material de todo el entorno de TI, en interactividad con el Rol de Operaciones.

6.2.1.2.1 Función de gestión de la seguridad

El Rol de Seguridad debe ser el responsable de establecer los lineamientos de seguridad, de evaluación de riesgos y de respuesta a los incidentes de seguridad.

Objetivos de la función:

- Establecer los lineamientos de seguridad de la información.
- Definir los controles de seguridad y explicar la razón para utilizarlos.
- Establecer los procedimientos de gestión de la seguridad.

- Definir un programa de gestión de la seguridad, estableciendo:
- Reglas para los datos seguros.
- Procedimientos para manejar los riesgos de seguridad.
- Procedimientos para manejar los incidentes de seguridad cuando ocurran.
- Establecer indicadores y la forma de medirlos.

Resultados esperados:

- Adherencia de todo el personal a las políticas de seguridad.
- Indicadores de seguridad de la institución.
- Reconocimiento de que todos somos responsables de la seguridad,
- Conocimiento y conciencia de las políticas de seguridad.

A continuación se detalla las políticas con las que espera alcanzar estos resultados.

Asignación de responsabilidades

La seguridad de la información es una responsabilidad de la institución compartida por todos los miembros del equipo que administra la información en calidad de administradores. El apoyo necesario para esta política es se implementa por medio de un comité que debe ser instituido en la institución, este comité tiene que tener elementos en su mayoría personal de TI y del área administrativa y académica, se le conoce como Comité de Tecnología de Información.

El Comité de Tecnología de Información promueve la seguridad dentro de la institución por medio de las siguientes acciones:

- Revisar y aprobar las políticas y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes.
- Monitorear los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- La eficacia de las políticas, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados.
- Los efectos de los cambios en la tecnología.

El Rol de Seguridad debe ser el responsable de coordinar todas las actividades relacionadas con la seguridad.

Cada uno de los recursos de información de la institución tiene un responsable. El responsable del recurso es también responsable de la seguridad de ese recurso.

Seguridad frente al acceso por parte de terceros

Los tipos de acceso por parte de terceros pueden ser:

- Acceso físico, cuando se da acceso a las oficinas y al cuarto de servidores.
- Acceso lógico, cuando se da acceso a las bases de datos y sistemas de información de la organización.

Ejemplos de terceras partes a los que se da acceso lógico:

- Personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones.
- Socios comerciales, quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

6.2.1.2.2 Función de administración de la seguridad

El Rol de Seguridad debe ser el responsable de monitorear los cambios y las actividades sospechosas o que violan la política de seguridad.

Objetivos de la función:

- Asegurar la confidencialidad y la integridad de los datos de la institución.
- Detectar y prevenir acceso no autorizado a la información y a las instalaciones.

Resultados esperados:

- Monitoreo y auditoria de las actividades del sistema para verificar que cumplan con las políticas.
- Reporte de incidentes de seguridad.

A continuación se detalla las políticas con las que espera alcanzar estos resultados.

Controles contra software malicioso

La protección contra software malicioso debe basarse en hacer conciencia en los usuarios en materia de seguridad y en controles adecuados de acceso al sistema y administración de cambios.

El encargado del rol de Seguridad debe ser el responsable de los siguientes controles:

- Todos los equipos deben de usar software con licencia.
- Debe aplicarse todos los parches del sistema operativo en cuanto estén disponibles.
- Debe instalarse en cada equipo un programa de protección contra virus.
- Debe realizarse las actualizaciones del antivirus en cuanto estén disponibles.
- Debe asegurarse la autenticidad de cualquier archivo o software obtenido a través de redes externas o por un medio informático removible.
- Debe verificarse la presencia de software malicioso en cualquier archivo o programa obtenido externamente antes de su uso.

Estos controles son especialmente importantes para los servidores que brindan soporte a un gran número de estaciones de trabajo.

Seguridad del sitio WEB en relación al rol de seguridad.

Se deben tomar precauciones para la protección de la integridad de la información publicada en el sitio WEB de la institución, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la institución.

Registro de usuarios

El Rol de Seguridad debe ser el responsable de los siguientes controles:

- Agregar nuevos usuarios, solamente si el movimiento está autorizado por el Jefe o Gerente del área por medio del documento Altas, bajas y cambios de usuarios.
- Cancelar los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la institución, con base en el documento Altas, bajas y cambios de usuarios.
- Entregar a los usuarios un detalle escrito de sus derechos de acceso por medio del documento Derechos por usuarios.
- Utilizar identificación de usuario único de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones.
- Verificar que el nivel de acceso otorgado es adecuado para el propósito de la institución y es coherente con la política de seguridad de la institución.
- Verificar periódicamente, y cancelar cuentas de usuarios.

6.3 Servicios Web.

Existen múltiples definiciones sobre lo que son los Servicios Web, lo que muestra su complejidad a la hora de dar una adecuada definición que englobe todo lo que son e implican.

Una posible definición sería hablar de ellos como un conjunto de aplicaciones o de tecnologías con capacidad para ínter operar en la Web.
Estas aplicaciones o tecnologías intercambian datos entre sí con el objetivo de ofrecer unos servicios. Los proveedores ofrecen sus servicios como procedimientos remotos y los usuarios solicitan un servicio llamando a estos procedimientos a través de la Web.

Estos servicios proporcionan mecanismos de comunicación estándares entre diferentes aplicaciones, que interactúan entre sí para presentar información dinámica al usuario. Para proporcionar interoperabilidad y extensibilidad entre estas aplicaciones, y que al mismo tiempo sea posible su combinación para realizar operaciones complejas, es necesaria una arquitectura de referencia estándar.

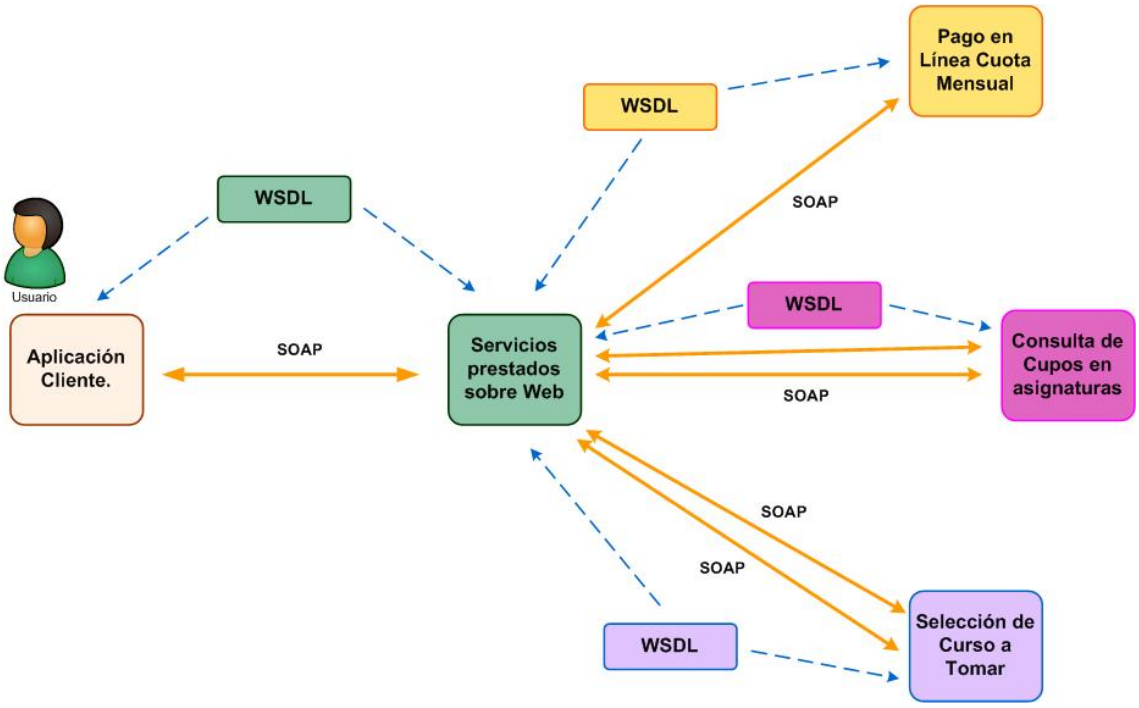


Fig.6.5 Servicios Web en Funcionamiento, para un ejemplo de consulta realizada en línea sobre una institución de educación superior.

6.3.1 Estándares de los Servicios Web.

Son lenguajes Web, protocolos y tecnologías inter-operativas e internacionales creadas con la finalidad de guiar la Web hacia su máximo potencial a través del desarrollo de protocolos y pautas estandarizadas.

Con el objetivo de que la Web alcance su máximo potencial, las tecnologías Web más destacadas deben ser compatibles entre sí y permitir que cualquier hardware y software para acceder a la Web funcione conjuntamente.

A continuación describimos los estándares que son mayormente principales y por ende, mas usados en la web.

6.3.1.1 SOAP

Siglas de Simple Object Access Protocol, es un protocolo estándar creado por Microsoft, IBM y otros, está actualmente bajo el auspicio de la W3C que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML. SOAP es uno de los protocolos utilizados en los servicios Web.

6.3.1.2 WSDL

Son las siglas de Web Services Description Language, un formato XML que se utiliza para describir servicios Web (se lee wisdel). La versión 1.0 fue la primera recomendación por parte del W3C y la versión 1.1 no alcanzó nunca tal estatus. La versión 2.0 se convirtió en la recomendación actual por parte de dicha entidad.
WSDL describe la interfaz pública a los servicios Web. Está basado en XML y describe la forma de comunicación, es decir, los requisitos del protocolo y los formatos de los mensajes necesarios para interactuar con los servicios listados en su catálogo. Las operaciones y mensajes que soporta se describen en abstracto y se ligan después al protocolo concreto de red y al formato del mensaje.
Así, WSDL se usa a menudo en combinación con SOAP y XML Schema. Un programa cliente que se conecta a un servicio web puede leer el WSDL para determinar que funciones están disponibles en el servidor. Los tipos de datos especiales se incluyen en el archivo WSDL en forma de XML Schema. El cliente puede usar SOAP para hacer la llamada a una de las funciones listadas en el WSDL.

6.3.1.3 XML.

Sigla en inglés de Extensible Markup Language («lenguaje de marcas extensible»), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de lenguajes específicos (de la misma manera que HTML es a su vez un

lenguaje definido por SGML). Por lo tanto XML no es realmente un lenguaje en particular, sino una manera de definir lenguajes para diferentes necesidades. Algunos de estos lenguajes que usan XML para su definición son XHTML, SVG, MathML.

XML no ha nacido sólo para su aplicación en Internet, sino que se propone como un estándar para el intercambio de información estructurada entre diferentes plataformas. Se puede usar en bases de datos, editores de texto, hojas de cálculo y casi cualquier cosa imaginable.

XML es una tecnología sencilla que tiene a su alrededor otras que la complementan y la hacen mucho más grande y con unas posibilidades mucho mayores. Tiene un papel muy importante en la actualidad ya que permite la compatibilidad entre sistemas para compartir la información de una manera segura, fiable y fácil.

6.3.1.4 Simple Mail Transfer Protocol (SMTP)

Protocolo simple de transferencia de correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. La comunicación entre el cliente y el servidor consiste enteramente en líneas de texto compuestas por caracteres ASCII. El tamaño máximo permitido para estas líneas es de 1000 caracteres.

Las respuestas del servidor constan de un código numérico de tres digitos, seguido de un texto explicativo. El número va dirigido a un procesado automático de la respuesta por autómata, mientras que el texto permite que un humano interprete la respuesta. En el protocolo SMTP todas las órdenes, réplicas o datos son líneas de texto, delimitadas por el carácter <CRLF>. Todas las réplicas tienen un código numérico al comienzo de la línea.

En el conjunto de protocolos TCP/IP, el SMTP va por encima del TCP, usando normalmente el puerto 25 en el servidor para establecer la conexión.

6.3.2 Recomendación de Microsoft para servidores Web.

La creciente sofisticación y el poder de los últimos virus han demostrado que, incluso unas pocas docenas de servidores inseguros, representan una amenaza al entorno del cliente. En el entorno de todos los clientes hay dos tipos de sistemas: los que son administrados y los que no lo son. Desgraciadamente, los últimos virus han ayudado a los clientes a identificar los sistemas que no están administrados.

Los sistemas no administrados se dividen en sistemas "disimulados" y sistemas de pruebas.

- Los sistemas "disimulados" se implantan utilizando procesos no estandarizados y van en contra de la política de la institución. Los sistemas "disimulados" son especialmente peligrosos porque es muy improbable que se estén siguiendo los estándares corporativos para la implementación y las actualizaciones de seguridad.

- Los sistemas de pruebas son aquéllos que son autorizados como una parte normal del desarrollo del sistema y de los esfuerzos de pruebas, pero para los que no hay una estructura de soporte formalizada que asegure que los servicios son implantados de forma segura y permanecen seguros.

Recomendación: Microsoft recomienda que los clientes implementen una estrategia agresiva para identificar los sistemas disimulados.

Los sistemas "disimulados" permiten que los virus se propaguen por medios distintos de las vulnerabilidades del servidor Web. Estos sistemas suponen un peligro claro para la estabilidad del entorno informático y deben ser localizados y abordados.

Estrategias para localizar los servidores "disimulados":

Implementar una exploración activa de los puertos del espacio de direcciones para identificar los servidores que están ejecutando servicios desaprobados. Hay disponibles excelentes herramientas de rastreo, como el Internet Security Scanner de Internet Security Systems.

Implementar una exploración pasiva de los puertos utilizando herramientas de control, como los monitores de redes remotas. Esto es menos agresivo y complicado para la red que la exploración activa de puertos, pero en muchos casos no identificarán tantos servidores " disimulados " como la exploración activa.

Incrementar el número de auditorias aleatorias que se hacen personalmente. Estas auditorias pueden automatizarse para aumentar el número de máquinas exploradas.

Recomendación: Microsoft recomienda a sus clientes que implementen un plan de administración tanto para los sistemas de pruebas como para los de desarrollo que actualmente no estén administrados.

Los mismos principios básicos que se usan para garantizar la seguridad en los sistemas de producción de Internet e intranet deben aplicarse a los sistemas de pruebas y desarrollo.

6.3.2.1 Internet Information Services.

IIS, es una serie de servicios para los ordenadores que funcionan con Windows. Originalmente era parte del Option Pack para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.

Este servicio convierte a un ordenador en un servidor de Internet o Intranet es decir que en las computadoras que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente (servidor web).

El servidor web se basa en varios módulos que le dan capacidad para procesar distintos tipos de páginas, por ejemplo Microsoft incluye los de Active Server Pages (ASP) y ASP.NET. También pueden ser incluidos los de otros fabricantes, como PHP o Perl.

CONCLUSIONES.

- Una solución informática no debe basarse en una limitada visión de hardware y software, sino mas bien, de debe velar por cada uno de los aspectos de su adecuado entorno, donde estará ubicada la información. Para ello debe hacerse un estudio a cabalidad de las necesidades, basándonos en los lineamientos que se entregan en este documento.

- La ubicación física, demanda energética y la infraestructura en general, son los aspectos que más consideración e importancia se les debe de dar al momento de generar un plan de creación de un Cuarto de Equipos, ya que de ello depende la apropiada ambientación y preparación del recinto que albergará la importante solución informática.

- La capa mas cercana de seguridad física que debe poseer la solución informática, debe constar en un gabinete adecuado y con características físicas, capaces de resguardar con precisión la integridad material de todos los equipos alojados en el, este a su vez debe tener la capacidad de poder alojar cada una de las partes necesarias para la correcta ventilación de los equipos alojados en el, manejo de cableado escalable y suministro eléctrico.

- Una infraestructura civil que sea la ubicación final de la información y sus equipos que procesan su información, debe pertenecer a un estilo sobrio exterior y ser a su vez, una fuerte estructura que brinde seguridad a todo lo que el recinto contenga, además de estar estratégicamente ubicado para que fluya el cableado de la mejor manera a todos los rincones de la institución y donde sean requeridos los servicios de TI, poseer consideraciones de crecimiento en cableado de datos, suministro de energía y control ambiental para el tipo de equipos que contenga.

- Seguridad de trafico y transacciones de datos, es una vista lógica de la información, es la prioridad paralela que se brindara en la primera capa de protección lógica a los datos que son entregados en los servicios de TI, esto se puede realizar por medio de configuraciones de protección de red, control de accesos y monitoreo de solicitudes al servidor o combinación de estas, todo para garantizar la integridad de los datos.

RECOMENDACIONES.

- En miras de proporcionar el mejor suministro energético y con la más alta calidad en energía eléctrica a entregar, se exhorta establecer una red eléctrica, separada y exclusiva para los equipos de procesamiento de datos, para evitar la filtración de ruido en las señales y procurar la no corrupción de la información. Además de proteger los equipos de una sobre carga eléctrica no controlada.

- La selección de las vías de comunicación de los datos, debe ser apropiada a la cantidad y tipo de transacciones que se esperan dar entre el servidor de información y el cliente del mismo, esto debe ser examinado en los datos, analizado y concluir la tecnología de comunicación a utilizar, ancho de banda necesario y proveedor a suministrar el servicio de comunicación, todo dentro de un marco de proyección de crecimiento continuo, escalable y sostenible.

- Los procedimientos y lineamientos a seguir en materia de seguridad general de los datos y recinto, deben ser establecidos en consenso por el equipo que planifique y ejecute el desarrollo de este proyecto. Tomando todas las consideraciones posibles en puntos que se razonen frágiles en protección de la información, y reforzándolos con medidas que procuren la disminución de estos aspectos críticos. Además el monitoreo constante del cumplimiento de estas normas es vital para asegurar la integridad de los datos y la información que se maneja, pero mas importante aun es la constante revisión y mejora constante de estos procedimientos y lineamientos de seguridad.

FUENTES DE INFORMACION.

BIBLIOGRAFICAS.

- **National Electrical Code Handbook, 10th Edition**
  International Electrical Code Series
  MarkW.Earley,P.E., Editor-in-Chief - JeffreyS.Sargent, SeniorEditor – JosephV.Sheehan,P.E., Editor - JohnM.Caloggero, Editor
  With the complete text of the 2005 edition of the National Electrical Code.

- **Essential Rack**
  System Requirements for Next Generation Data Centers
  White Paper #7 APC 2003.

- **Surviving Security: How to Integrate People, Process, and Technology, Second Edition**
  by Amanda Andress (ed) ISBN:0849320429
  Auerbach Publications © 2004.

- **Windows Server System Reference Architecture**
  Chapter 11 - Web Application Services
  Planning Guide
  Published: June 2004

- **The Computer Engineering Handbook.**
  Edited by Vojin G. Oklobdzija
  CRC Press
  Boca Raton – London - New York – Washington D.C.
  2002.

- **Security in Telecommunications and information technology**
  An overview of issues and the deployment of
  Existing ITU – T Recommendations for secure communications
  October 2004.

REFERENCIAS WEB.

- **DELL, Sistemas de Bastidor.**
  http://support.dell.com/support/edocs/systems/smarcon/sp/index.htm

- **Data Center University by APC.**
  http://lms.globalknowledge.com/ilearn/en/learner/jsp/clients/APC/customer/login.jsp

- **PTS, Data Center Solutions.**
  http://www.ptsdcs.com/index.asp

GLOSARIO

A

ANSI: El Instituto Nacional Estadounidense de Estándares (ANSI, por sus siglas en inglés: American National Standards Institute) es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

B

BIOS: Es el bloque de instrucciones grabadas en la memoria de solo lectura.

C

CRAC: Aire Acondicionado de Cuarto de Computadores, por sus siglas en ingles, monitor y preservador de la temperatura en una sala de equipo informático.

CE: Cuarto de Equipos, iniciales.

D

DAS: Direct Attached Storage (DAS) es el método tradicional de almacenamiento y el más sencillo. Consiste en conectar el dispositivo de almacenamiento directamente al servidor o estación de trabajo, es decir, físicamente conectado al dispositivo que hace uso de él.

DMZ: Del inglés DeMilitarized Zone o Zona Desmilitarizada. En seguridad informática, una zona desmilitarizada (DMZ) o red perimetral es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

DBA: Siglas en ingles que obedecen a Administrador de la Base de Datos. Persona Responsable del diseño físico, administración, y de la selección, evaluación e implementación de los Sistemas de Administración de las Bases de Datos.

E

ETI: Equipos de Tecnología de la Información.

EIA: Electronics Industries Association. (EIA)es una organización comercial nacional que incluye el espectro completo de los fabricantes de los E.E.U.U. La asociación es una sociedad de asociaciones y de las compañías electrónicas y de alta tecnología que misión está

promoviendo el desarrollo de mercado y la competitividad de la industria de alta tecnología de los E.E.U.U

ETSI: Instituto Europeo de Normas de Telecomunicaciones es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial.

Ethernet: Es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI.

E1: Lleva datos en una tasa de 2048 millones de bits por segundo (Mbps) y puede llevar 32 canales de 64 Kbps * cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos en SS7 o Sistema de Señalización Número 7 (tambien denominado CCS).

G

GRT: Iniciales de Guía de Referencia Técnica.

H

HTTPS: Hypertext Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), mas conocido por su acrónimo HTTPS, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

Hz: El hercio, hertzio o hertz es la unidad de frecuencia del Sistema Internacional de Unidades. Proviene del apellido del físico alemán Heinrich Rudolf Hertz, quien descubrió la propagación de las ondas electromagnéticas. Su símbolo es Hz (escrito sin punto como todo símbolo).

I

ISA: Internet Security and Acceleration es un firewall de stateful packet inspection, es decir, analiza el encabezado de los paquetes IP y de application layer, analizan la trama de datos en busca de tráfico sospechoso. Adicionalmente, ISA Server es un firewall de red, VPN y web cache como contenedor de sitios web.

K

KBPS: Un kilobits por segundo es una unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de

transferencia de información a través de una red. Su abreviatura y forma más corriente es kbps.

M

Memoria: La memoria de acceso aleatorio, o memoria de acceso directo (en inglés: Random Access Memory, cuyo acrónimo es RAM), o más conocida como memoria RAM, se compone de uno o más chips y se utiliza como memoria de trabajo para programas y datos.Es un tipo de memoria temporal que pierde sus datos cuando se queda sin energía (por ejemplo, al apagar la computadora), por lo cual es una memoria volátil.

MPLS: Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MOF: Microsoft Operations Frameworks, es una guía para hacer de las actividades del entorno de TI, confiables, y efectivas en costo.

N

NEC: Nacional Electrical Code: Guía segura para la instalación de cableado y el equipo; no pretende ser una especificación del diseño, sino más bien para la práctica de la protección de personas y de los edificios y su contenido de los riesgos derivados del uso de electricidad para la calefacción, luz, electricidad, y otros . Proporciona normas, recomendado por la National Fire Protection Association, que regula la instalación de cableado eléctrico interior. Estas normas, sujetas a revisión cada tres años, un nivel de la Junta Nacional de Bomberos Underwriters, se han incorporado a muchas ordenanzas municipales; ciudad o regulaciones estatales tienen prioridad cuando se diferencian de las normas del Código.

NEBS: Es un sistema de requisitos técnicos con un propósito básico: para hacer los interruptores de la red a prueba de balas. El estándar fue desarrollado internamente en los laboratorios de Bell.

P

Procesadores: Es el cerebro del computador, se encarga de convertir la materia prima de éste y dar un producto que puede ser sometido a otro procesamiento o ser el producto final del sistema o maquina. Realiza cálculos matemáticos a altísimas velocidades.

Proxy: El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

R

RAID: Originalmente del inglés Redundant Array of Inexpensive Disks, conjunto redundante de discos baratos', en la actualidad también de Redundant Array of Independent Disks, 'conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usa múltiples discos duros entre los que distribuye o replica los datos.

RACK: Un rack es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante.

RJ45: El RJ45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

S

SSL: Secure Sockets Layer (SSL) y Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario.

SQL: El Lenguaje de consulta estructurado (SQL [/esekuele/ en español, /sicuèl/ en inglés] Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones sobre las mismas.

T

TIA: La Telecommunications Industry Association (Asociación de la Industria de Telecomunicaciones o TIA) es una asociación de comercio en los Estados Unidos que representa casi 600 compañías. También produce nXtcomm, un trade-show para la industria de telecomunicaciones que reemplaza a la GLOBALCOMM (anteriormente SUPERCOMM) y TelecomNext.

TI: Tecnologías de la Información y la Comunicación (TIC), se encargan del estudio, desarrollo, implementación, almacenamiento y distribución de la información mediante la utilización de hardware y software como medio de sistema informático.

TCP/IP: El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

U

USB: Universal Serial Port: (bus universal en serie) es un puerto que sirve para conectar periféricos a una computadora. Fue creado en 1996 por siete empresas: IBM, Intel, Northern Telecom, Compaq, Microsoft, Digital Equipment Corporation y NEC.

UPS Un SAI (Sistema de Alimentación Ininterrumpida), o más conocido por sus siglas en inglés UPS (Uninterruptible Power Supply), es un dispositivo que, gracias a su batería, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos existentes en la red eléctrica.

UTP: UTP RJ45 (del inglés: Unshielded Twisted Pair, par trenzado no apantallado) es un tipo de cableado utilizado principalmente para comunicaciones. Se encuentra normalizado de acuerdo a la norma Americana TIA/EIA-568-B y a la internacional ISO-11801.

V

VPN: Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

W

Web Service: Servicio de TI es un conjunto de actividades que buscan responder a una o más necesidades de un cliente por medio de un cambio de condición en los bienes informáticos potenciando el valor de estos y reduciendo el riesgo inherente del sistema.

X

XML: Sigla en inglés de Extensible Markup Language («lenguaje de marcas extensible»), es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium.

Nombre de archivo: CAPITULO VII
Directorio: C:\Documents and Settings\Roberto Andres\Escritorio\Correcciones\CAP7
Plantilla: C:\Documents and Settings\Roberto Andres\Datos de programa\Microsoft\Plantillas\Normal.dot
Título: CAPITULO
Asunto:
Autor: Roberto Andres Alvarenga Sandoval
Palabras clave:
Comentarios:
Fecha de creación: 10/05/2008 22:34:00
Cambio número: 3
Guardado el: 10/05/2008 22:34:00
Guardado por: ROBERTO ALVARENGA
Tiempo de edición: 46 minutos
Impreso el: 12/05/2008 23:08:00
Última impresión completa
Número de páginas: 187
Número de palabras: 34,733 (aprox.)
Número de caracteres: 191,034 (aprox.)