ESCUELA POLITECNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PLAN DE CONTINGENCIA PARA EL SISTEMA DE CABLEADO ESTRUCTURADO EN EL EDIFICIO MENA-MERIZALDE

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

VALLEJO GUAYASAMÍN ROBERTO CORAL

vallejoroberto@gmail.com

DIRECTOR: ING. CARLOS FLORES

carlos.flores@epn.edu.ec

Quito, Febrero 2009

DECLARACIÓN

Yo, Roberto Coral Vallejo Guayasamín, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____

Roberto Coral Vallejo Guayasamín

CERTIFICACIÓN

Certifico que el presente trabajo, “PLAN DE CONTINGENCIA PARA EL SISTEMA DE CABLEADO ESTRUCTURADO EN EL EDIFICIO MENA-MERIZALDE”, fue desarrollado por el señor Roberto Coral Vallejo Guayasamín, bajo mi supervisión.

_____

ING. CARLOS FLORES

DIRECTOR DEL PROYECTO

INDICE

Página

INTRODUCCIÓN…….. i

CAPÍTULO I

1. DESCRIPCION DEL PROCESO DE LA INSTALACION DEL CABLEADO ESTRUCTURADO EN EL EDIFICIO MENA-MERIZALDE……. 1
   1.1. ASPECTOS GENERALES…….. 1
      1.1.1. Definición de un Sistema de Cableado Estructurado…… 1
      1.1.2. Características de un Sistema de Cableado Estructurado….. 2
      1.1.3. Ventajas de un Sistema de Cableado…… 3
   1.2. IMPLEMENTACION DEL SISTEMA DE CABLEADO ESTRUCTURADO…….. 4
      1.2.1. Planteamiento del Problema…… 4
         1.2.1.1. Análisis del Edificio Mena-Merizalde…… 5
         1.2.1.2. Dimensionamiento de la Red…….. 8
      1.2.2. Descripción del Sistema de Cableado……... 9
         1.2.2.1. Componentes del Cableado…… 10
            1.2.2.1.1. Componentes Pasivos del Sistema……... 10
      1.2.3. Diseño del Cableado…….. 25
         1.2.3.1. Cableado Horizontal…… 25
         1.2.3.2. Cableado Vertical…… 25
         1.2.3.3. Cuarto de Equipos …… 26
         1.2.3.4. Cuarto de Telecomunicaciones…… 26
            1.2.3.4.1. Cuarto de Telecomunicaciones CT-01: Departamento Técnico…….. 27
            1.2.3.4.2. Cuarto de Telecomunicaciones CT-02: Departamento de Importaciones…… 28
            1.2.3.4.3. Cuarto de Telecomunicaciones CT-03: Departamento de Contabilidad…….. 28
      1.2.4. Comprobación de Errores…… 29
      1.2.5. Certificación…… 30

CAPÍTULO II

2. PLAN DE REDUCCIÓN DE RIESGOS…… 31
   2.1. DEFINICIONES INICIALES…….. 31
   2.2. REALIZACIÓN DEL ANÁLISIS DE RIESGOS…….. 32
      2.2.1. Activos…….. 34
         2.2.1.1. Tipo de Activos…… 36
         2.2.1.2. Dependencia entre Activos…….. 37
         2.2.1.3. Valoración de los Activos…… 38
         2.2.1.4. Dimensiones de un Activo…… 39
         2.2.1.5. Determinación del Valor de un Activo…… 41
            2.2.1.5.1. Valoración Cualitativa…… 42
            2.2.1.5.2. Valoración Cuantitativa…… 42

2.2.1.5.3. El valor de la interrupción del Servicio…….. 43
2.2.1.5.4. Costo de Interrupción de la Disponibilidad…… 43
2.2.2. Amenazas…… 44
2.2.2.1. Valoración de las Amenazas…… 45
2.2.2.1.1. Análisis de Amenazas al Sistema de Cableado Estructurado…….... 46
2.2.2.1.2. Amenazas Internas…….... 46
2.2.2.1.3. Estándares de Prueba de cable..…… 47
2.2.2.1.4. Amenazas Externas……..…… 45
2.2.3. Determinación del Impacto……..... 53
2.2.3.1. Impacto Acumulado……... 53
2.2.3.2. Impacto Repercutido……... 54
2.2.3.3. Agregación de Valores de Impacto…….. 54
2.2.4. Determinación del Riesgo…..…… 55
2.2.4.1. Riesgo Acumulado…… 55
2.2.4.2. Riesgo Repercutido…….…….... 56
2.2.4.3. Agregación de Riesgos…….. 56
2.2.5. Salvaguardas……..…….. 57
2.2.5.1. Reducción de la frecuencia de las Amenazas…… 57
2.2.5.2. Limitación del daño causado…… 57
2.2.5.3. Impacto Residual……..... 58
2.2.5.4. Riesgo Residual…….. 59
2.2.5.5. Salvaguardas sugeridas por los fabricantes de elementos de cableado..... 60
2.2.5.6. Salvaguardas generales para el Edificio Mena-Merizalde…….. 61
2.2.5.6.1. Salvaguardas para afirmar la seguridad física……..... 61
2.2.5.6.2. Salvaguardas para afirmar la seguridad física por acción de terceros…….. 66
2.3. GESTIÓN DE RIESGOS…… 72
2.3.1. La interpretación de los valores de impacto y riesgo residuales……..…... 72
2.3.2. Selección de salvaguardas……..... 73
2.3.3. Tipos de salvaguardas……..…. 74
2.3.4. Pérdidas y ganancias……..…… 74
2.3.5. La actitud de la Dirección……... 77

CAPÍTULO III

3. PLAN DE RECUPERACIÓN DE DESASTRES…… 79
3.1. ACTIVIDADES PREVIAS AL DESASTRE…… 80
3.1.1. Establecimiento del Plan de Acción…….. 80
3.1.1.1. Entorno del Sistema……... 80
3.1.1.2. Sistemas de Información…….. 82
3.1.1.3. La Información…..…… 83

3.1.2. Formación de Equipos Operativos…….…… 86
3.1.3. Formación de Equipos de Evaluación…… 87
3.2. ACTIVIDADES DURANTE EL DESASTRE…….... 87
3.2.1. Plan de Emergencias……..…….. 88
3.2.2. Formación de Equipos……..... 89
3.2.3. Entrenamiento……..…… 89
3.3. ACTIVIDADES DESPUES DEL DESASTRE…….....…. 90
3.3.1. Evaluación de Daños…….. 90
3.3.2. Priorización de Actividades del Plan de Acción…..…….. 90
3.3.3. Ejecución de Actividades…… 91
3.3.4. Evaluación de Resultados…… 91
3.3.5. Retroalimentación del Plan de Acción…… 92
3.3.6. Manual de funciones de la empresa JH&H……..... 92

CAPÍTULO IV

4. CONCLUSIONES Y RECOMENDACIONES…….……..... 95
4.1. CONCLUSIONES……..... 95
4.2. RECOMENDACIONES…….…….. 99

BIBLIOGRAFÍA…….…… 101

REFERENCIAS DE INTERNET…….…… 102

ANEXOS…….…… 103

ÍNDICE DE FIGURAS

CAPÍTULO I

Figura 1.1. Distribución de cables en el conector..…….8

Figura 1.2. Inserción de cable en RJ-45…….9

Figura 1.3. Esquema de colores del cable UTP según estándar…… 9

Figura 1.4. Diagrama de enlace con Patch cord…… 10

Figura 1.5. Terminaciones para cable cruzado…… 10

Figura 1.6. Bastidor Panduit CMR 19X84……..…… 11

Figura 1.7. Gabinete de Pared Great Lakes GL24WM…… 12

Figura 1.8. Patch Panel Panduit CP24BLY…… 12

Figura 1.9. Conector Macho RJ-45 Panduit SP6888-C…….. 13

Figura 1.10. Conector Hembra RJ-45 Panduit CJ6XX88TGRD……. 13

Figura 1.11. Caja Universal Panduit JB11W-A……. 14

Figura 1.12. Módulo Doble Panduit CFPE2IW-LY……. 14

Figura 1.13. Módulo Simple Panduit CFPE1IW-LY……. 15

Figura 1.14. Organizador Vertical Panduit WMPVF45…….. 16

Figura 1.15. Organizador Horizontal Panduit WMPH2…….. 16

Figura 1.16. Accesorios del Sistema Pan-Way Twin-70…….. 17

Figura 1.17. Accesorios para acople entre ductos Conduit y Canasta Metálica…….. 19

CAPÍTULO II

Figura 2.1. Diagrama de bloques de Análisis de Riesgos……. 29

Figura 2.2. Gráfica del costo de las interrupciones……. 38

Figura 2.3. Gráfica de simulación de transmisión…….. 42

Figura 2.4. Representación de transmisiones por diferentes pares…… 42

Figura 2.5. Diagrama de bloque análisis de riesgo, incluyendo salvaguardas…… 52

Figura 2.6. Ficha de registro de visitantes…….. 64

Figura 2.7. Punto de equilibrio del costo riesgo/ salvaguarda……. 68

Figura 2.8. Gráfica de diferentes tipos de salvaguardas…….. 69

INTRODUCCION

En el mundo actual, tan competitivo, las empresas deben mejorar sus comunicaciones interiores y exteriores para aspirar a un crecimiento en el mercado. La productividad es clave en el mejoramiento de la rentabilidad, y la mejor manera de incrementarla es apoyarse en las aplicaciones que ofrece la tecnología contemporánea, como Internet de banda ancha, imágenes tridimensionales, televisión bajo demanda, programas multimedia, diseño asistido por ordenador, audio y vídeo hasta la estación de trabajo.

Es evidente que las tecnologías mencionadas anteriormente requieren de un mayor soporte y por lo tanto mayor exigencia de la red.

La seguridad de la red de área local es uno de los factores más importantes que cualquier administrador o instalador de red debe considerar.

Por otra parte, son frecuentes los cambios que se deben realizar en las instalaciones de red, especialmente en su cableado, debido a la evolución de los equipos y a las necesidades de los usuarios de la red. Esto nos lleva además a tener en cuenta la flexibilidad, que es otro factor importante.

Por lo tanto, un sistema de cableado bien diseñado debe tener estas dos cualidades: seguridad y flexibilidad. A estos parámetros se le pueden añadir otros, menos exigentes desde el punto de vista del diseño de la red, como son el costo económico, la facilidad de instalación, la rapidez para su implementación, entre otras.

En ocasiones, trasladar una estación de trabajo a otro lugar, repercute en profundos cambios en el cableado de un edificio, y transformar la estructura de comunicaciones por cable no representa una tarea sencilla ni económica.

Un Sistema de Cableado Estructurado es una metodología, basada en estándares y normas, de diseño e instalación para un sistema que integre la transmisión de voz, datos y vídeo.

Un Sistema de Cableado Estructurado, diseñado e instalado en forma correcta, proporciona una infraestructura adecuada para el desempeño eficaz de la red y la flexibilidad de acomodarla para un futuro crecimiento por un período extendido de tiempo.

Tradicionalmente, la infraestructura de cableado de un edificio corporativo es en lo último en lo que se piensa; de hecho, los cables no son contemplados en el presupuesto de construcción inicial, su planeación e instalación se realiza cuando el edificio está listo para ocuparse y, en general, se utilizan varios tipos de cables para distintas funciones. Se podría afirmar que el cable ocupa una de las últimas jerarquías en la preocupación de los realizadores del edificio y sus dueños.

CAPITULO I

1. DESCRIPCION DEL PROCESO DE LA INSTALACIÓN DEL CABLEADO ESTRUCTURADO EN EL EDIFICIO MENA-MERIZALDE

1.1. ASPECTOS GENERALES

1.1.1. Definición de un Sistema de Cableado Estructurado

Por definición, un Sistema de Cableado Estructurado implica que todos los servicios en el edificio: voz, datos, vídeo, audio, tráfico de Internet, seguridad, control y monitoreo, estén disponibles desde y hacia cualquier punto de conexión del edificio. Esto es posible distribuyendo cada servicio a través del edificio por medio de un cableado estructurado estándar con cables de cobre o fibra óptica[1].

Esta infraestructura es diseñada, o estructurada para maximizar la velocidad, eficiencia y seguridad de la red. Cabe mencionar que ninguna inversión en tecnología dura más que el sistema de cableado, pues ningún otro componente de la red tiene un ciclo de vida tan largo, por ello merece una atención especial, porque además es la base sobre la cuál las demás tecnologías operarán.

Los Sistemas de Cableado Estructurado, diseñados para facilitar los frecuentes cambios y ampliaciones, son los cimientos sobre los que se construyen las modernas redes de información. A pesar del constante cambio tecnológico que se debe afrontar día a día, el Sistema de Cableado Estructurado puede aliviar las interrupciones en el trabajo y las caídas de la red debidas a las reestructuraciones en las áreas de trabajo.

El Sistema de Cableado Estructurado es la plataforma sobre la cual se construye la estrategia general de sistemas de información. Del mismo modo que el intercambio de información es vital para una empresa, el sistema de cableado estructurado lo es para la red.

---

[1] http://www.arqhys.com/archives.pdf

Con una infraestructura de cableado flexible, se puede soportar multitud de aplicaciones de voz, datos y vídeo independientemente del fabricante de los equipos. No importa cuánto crecimiento tenga la red a lo largo de su ciclo de vida, un cableado fiable y flexible se adaptará a las crecientes necesidades futuras.

Mediante una topología adecuada, que en la mayoría de casos es de tipo estrella, con nodos centrales a los que se conectan todas las estaciones, se facilita la interconexión y administración del sistema.

1.1.2. Características De Un Sistema De Cableado Estructurado

Entre las características generales de un Sistema de Cableado Estructurado destacan las siguientes:

- La configuración de nuevos puestos se realiza hacia el exterior desde un nodo central, sin necesidad de variar el resto de los puestos. Sólo se configuran las conexiones del enlace particular.

- Los ciclos de vida de los elementos que componen una oficina corporativa dejan de representar una prioridad, pues las innovaciones de equipo siempre tendrán detrás una estructura de cableado que podrá recibirlos, sin grandes complicaciones.

Es preciso definir los ciclos de vida de los procesos e infraestructura de un edificio corporativo, los cuales se dividen así[2]:

- Estructura del edificio: 40 años
- Administración del edificio: 5-7 años
- Telecomunicaciones: 3-5 años
- Automatización de oficina: 1-2-3 años

- La localización y corrección de daños se simplifica ya que los problemas se pueden detectar al encontrarse en un espacio centralizado.

[2] http://hermosillovirtual.com/lam/cableado.htm

- Mediante una topología física en estrella se hace posible configurar distintas topologías lógicas tanto en bus como en anillo, simplemente reconfigurando centralizadamente las conexiones.

1.1.3. Ventajas de un Sistema de Cableado Estructurado

Las principales ventajas que posee un Sistema de Cableado Estructurado son:

Transparencia de Información: representa un diseño de arquitectura abierta, pues la información que se transmite, es indiferente una a otra para el sistema de cableado.

Confiabilidad: es confiable porque está diseñado, en mayor medida, en topología de estrella, la que en caso de un daño o desconexión, éstas se limitan sólo a la sección afectada, y no al resto de la red.

Economía: se gastan recursos en una sola estructura de cableado, y no en varias como en los edificios con cableado convencional. En casos de actualización o cambios en los sistemas empresariales, sólo se cambian los módulos correspondientes y no todos los cables de la estructura del edificio.

Operabilidad: se evita romper paredes o realizar cambios extremos para cambiar circuitos o cables, lo que además, provoca cierres temporales o incomodidades en el lugar de trabajo.

Flexibilidad: un sistema de cableado estructurado permite mover personal de un lugar a otro, o agregar servicios a ser transportados por la red sin la necesidad de incurrir en altos costos de reconfiguración.

Velocidad: dentro de un sistema de cableado estructurado es posible utilizar al máximo los recursos de la red, en especial en lo referente a velocidad de transmisión de la información

1.2. IMPLEMENTACION DEL SISTEMA DE CABLEADO ESTRUCTURADO

Una vez analizadas las características y ventajas de un Sistema de Cableado Estructurado, es necesario entonces comenzar con el procedimiento de la implementación del mismo. Para ello se debe seguir una serie de pasos que en algunas ocasiones, provienen más de la experiencia del instalador y que pueden variar entre uno y otro.

De todas maneras se puede generalizar algunas acciones a tomar en el proceso de implementar un sistema de cableado estructurado, siendo las principales las siguientes[3]:

- Planteamiento del Problema
- Descripción del Sistema de Cableado
- Diseño del Cableado
- Comprobación de Errores
- Certificación

1.2.1. PLANTEAMIENTO DEL PROBLEMA

El primer paso dentro de la implementación de un Sistema de Cableado Estructurado es realizar un análisis del lugar donde se llevará a cabo la instalación.

Se deberá cumplir con una visita al sitio de la obra con el fin de evaluar las dificultades que se pueden presentar en el transcurso de su ejecución y recabar todas las consideraciones necesarias.

Con el objeto de realizar un trabajo adecuado, en el presente proyecto de titulación no se darán directrices generales de un edificio en general, sino que se escogió uno en particular, el Edificio Mena-Merizalde, correspondiente a un trabajo realizado por el Grupo Jiménez-Andrade, el cual servirá para todo el análisis subsiguiente.

---

[3] Manual para Certificación PANDUIT 2005

1.2.1.1. Análisis del Edificio Mena-Merizalde

Situación Actual del edificio

El edificio Mena-Merizalde ubicado en el norte de la ciudad de Quito, consta de 3 pisos administrativos y operativos, dichas instalaciones son utilizadas por la compañía JH&H, empresa dedicada a la comercialización y mantenimiento de equipos electrónicos orientados al sector petrolero.

Cada planta posee un área de 34 m de frente por 33 de fondo. La altura de los techos en todos los pisos, salvo en lugares específicos, es de 3.65 metros. Todos los techos son falsos o dobles Todos los pisos son de hormigón, con un piso falso sobrepuesto.

Sistema de tierra:

Este sistema está compuesto por un solo barraje primario que recorre el edificio desde la terraza hasta el subsuelo, se halla compuesto por un cable calibre 00 (Doble cero) sin revestimiento, en cada piso se desprenden de él, las ramificaciones respectivas que luego alimentarán todos y cada uno de los tomacorrientes, así como la alimentación de cada uno de los equipos y los respectivos blindajes de los mismos.

Cuando el barraje primario llega al sótano este se conecta en forma directa y bajo las más estrictas normas técnicas, a la malla de aterrizamiento que se halla ubicada debajo del piso en el subsuelo.

Sistemas de Seguridad:

La compañía JH&H no cuenta con políticas de seguridad que resguarden el sistema de información, sino únicamente existen procedimientos aislados como contratación de personal de seguridad y cámaras de vigilancia, para proteger los bienes físicos del edificio.

Además, el personal no posee información alguna sobre normas o procedimientos para salvaguardar el sistema de información.

Para completar el análisis del edificio, es necesario describir las diferentes áreas dentro de cada planta, el espacio que utilizan, el número de usuarios y la función que cumplen dentro de la organización, estas consideraciones son importantes pues servirán para la determinación de la cantidad de puntos de red necesarios.

En el edificio Mena-Merizalde opera funcionan varias dependencias de carácter administrativo, comercial y técnico, distribuidas de la siguiente forma:

Subsuelo:

Están localizadas las oficinas del Departamento Técnico y Servicio Técnico. Las actividades que se realizan en estas oficinas son de mantenimiento preventivo a los equipos que la empresa JH&H comercializa, además se efectúan reparaciones si los daños son leves, caso contrario los equipos son enviados a los países de procedencia para su revisión.

La oficina de servicio técnico cuenta con seguridad reforzada en la puerta de ingreso, no tiene accesos adyacentes a exteriores y además existe espacio que no ha sido utilizado por la empresa.

En estas oficinas así mismo existen otras dependencias tales como: Bodegas y Comedor.

El total de personas que intervienen en las actividades de este piso es 6 personas:

- 1 Jefe de Departamento Técnico
- 4 Técnicos de Servicio
- 1 Jefe de Bodega

Planta Baja:

Se encuentran distribuidas las oficinas de Atención al Cliente, donde se receptan los requerimientos y necesidades de las empresas usuarias de los servicios que presta JH&H, en mayor medida tramitadas vía telefónica y correo electrónico.

Marketing y Ventas, espacio destinado a la difusión de los servicios y productos de la Organización, además se tiene contacto con todas las empresas proveedoras de los equipos que se comercializa.

Recepción, área determinada para acoger los visitantes de la empresa y la Sala de Reuniones que sirve para propósitos varios.

En la Planta Baja trabajan 17 personas:

- 1 Recepcionista
- 8 Personas en Atención al Cliente
- 4 Personas en Ventas
- 1 Jefe de Importaciones
- 1 Ayudante de Importaciones
- 1 Jefe de Marketing
- 1 Asistente de Marketing

Planta Alta:

Están ubicadas en esta sección la Dirección Administrativa, Gerencia General y el Departamento de Contabilidad. Estos departamentos tienen contacto directo con proveedores y clientes vip.

En la Planta alta laboran un total de 6 personas;

- 1 Director Administrativo
- 1 Gerente General
- 1 Secretaría de Gerencia
- 1 Contador
- 1 Asistente de Contabilidad
- 1 Asistente de Órdenes

El detalle de la distribución física del edificio se encuentra en los planos adjuntos en el Anexo A del presente proyecto, el mismo que servirá para la determinación de las dimensiones de los componentes pasivos y activos del sistema.

Al momento de realizar la verificación física de las instalaciones, se pudo constatar que en el edificio Mena-Merizalde no existe conexión de Red para la mayoría de las dependencias que allí funcionan, siendo la más sobresaliente la del Departamento Técnico pues al no contar con puntos de red, debe compartir los recursos de otras dependencias.

Además, un gran número de oficinas carece de equipos de computación, como es el caso del Departamento de Importaciones; por otro lado, existen secciones que a pesar de que cuentan con computadores, algunos de estos no cumplen con los requerimientos mínimos de hardware y software para ser conectados a la red, teniendo como consecuencia, que las actividades de carácter investigativo y administrativo tanto para el personal interno como externo, se vean limitadas debido a la imposibilidad de aprovechar los recursos que podrían ofrecer otras redes, tales como las de empresas afines, proveedores o la propia internet.

Sin embargo, debe mencionarse que en algunas áreas del edificio, la conexión a redes ya existe, aunque en forma rústica y desordenada, específicamente en las áreas correspondientes a Ventas y Atención al Cliente que de forma imprescindible necesitan de interconexión para gestionar las peticiones de clientes y proveedores.

Con la intención de integrar a las distintas dependencias del Edificio Mena-Merizalde que carecen de conexión a redes, se plantea diseñar una red para este edificio que abarque todas las áreas comprendidas en el subsuelo y las otras dos plantas pertenecientes al edificio.

1.2.1.2. Dimensionamiento de la Red

Las necesidades que las dependencias de cada uno de los pisos requiere de acuerdo al diseño planteado por el Grupo Jiménez-Andrade en base a los datos de la situación actual del edificio son:

Subsuelo:

- Departamento Técnico.
- Servicio Técnico.
- Bodegas
- Comedor

En las áreas mencionadas anteriormente, laboran un total de 6 personas, cada una de ellas debe contar con 2 puntos de red, adicionalmente se deben dejar por lo menos 2 puntos de guarda, por lo tanto:

 # de puntos de red = (6 * 2) + 2 = 14 puntos de red

Planta Baja:

- Recepción.
- Cubículos de Atención al Cliente
- Departamento de Ventas.
- Departamento de Marketing.
- Departamento de Importaciones.
- Sala de Reuniones.

En la Planta Baja se dispone el área de trabajo para 17 personas, cada una con un requerimiento de 2 puntos de red, además hay que adicionar 4 puntos para el área de sala de reuniones y 4 puntos de guarda, por lo tanto:

 # de puntos de red = (17 * 2) + 4 + 4 = 42 puntos de red

Planta Alta:

- Dirección Administrativa.
- Gerencia General.
- Departamento de Contabilidad.

En Planta Alta se necesita de 2 puntos de red para cada una de las 6 personas que trabajan en el piso y de 2 puntos de guarda.

 # de puntos de red = (6 * 2) + 2 = 14 puntos de red.

Por lo tanto el número total de puntos de red que se necesitan para todo el sistema es de 70, distribuidos 14 para subsuelo, 42 para planta baja y 14 para planta alta.

1.2.2. DESCRIPCION DEL SISTEMA DE CABLEADO

Para definir el Sistema de Cableado al cual se regirá el proyecto, se considerarán las normas que establece el sistema de cableado estructurado, específicamente se adoptará la norma 568-A que junto con todos sus documentos adicionales han sido condensados en el nuevo estándar ANSI/TIA/EIA 568B[4].

La norma 568B ha sido publicada en tres partes:

- ANSI/TIA/EIA 568B.1. Estándar de cableado de telecomunicaciones para edificios comerciales. Requisitos generales.
- ANSI/TIA/EIA 568B.2. Estándar de cableado de telecomunicaciones para edificios comerciales. Componentes para cableados de pares trenzados balanceados.
- ANSI/TIA/EIA 568B.3. Estándar para componentes de cableado de fibra óptica.

En resumen, este estándar especifica requisitos mínimos para cableados de telecomunicaciones dentro de edificios comerciales en un ambiente de campus. Incluye sitios con una extensión geográfica de 3000 m^2 hasta 1000000 m^2 de espacio de oficina y con una población de hasta 50000 usuarios individuales.

Los sistemas de cableado de telecomunicaciones especificados en este estándar son propuestos para tener una vida útil de más de 10 años.

---

[4] Manual para Certificación ORTRONICS 2007

1.2.2.1. COMPONENTES DEL CABLEADO[5]

Los componentes del cableado pueden dividirse en dos grandes grupos: componentes activos y componentes pasivos.

1.2.2.1.1. Componentes Pasivos del Sistema

Debido a las actividades que realiza la empresa JH&H, comercialización y mantenimiento de equipos electrónicos, necesita de una red eficiente que provea de un tratamiento de la información de manera inmediata.

Gracias a la información estadística que el Grupo Jiménez-Andrade posee acerca de instalaciones previas en edificios similares dedicadas a la misma actividad y después del haber recabado los datos correspondientes a la situación actual del edificio Mena-Merizalde y las necesidades de la empresa que utiliza las instalaciones en cuanto a procesamiento de información, se determinó que el canal que se ajusta a tales requerimientos es de al menos 200 MHz.

Se presentó entonces dos alternativas que superen dichas exigencias para satisfacer de igual manera necesidades que se puedan presentar a futuro, implementar el cableado estructurado con componentes de categoría 6, canal de 250 MHz o con categoría 6A, canal de 550 MHz.

Se realizaron presupuestos a priori para todo el sistema y se presentaron las proformas correspondientes a la Dirección de la Organización, y debido a que la correspondiente a categoría 6A económicamente es superior a la otra en un 50%, la empresa JH&H decidió implementar el sistema con componentes pasivos y activos de categoría 6 y deberán traer impreso su categoría y el fabricante.

Cable

Debido a que se instalará el sistema con categoría 6, el cable a utilizar debe cumplir con las siguientes características:

---

[5] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

- Cable UTP de 4 pares, trenzado, Categoría 6, calibre #24 AWG similar a PANDUIT PUL6004WH-EDY.
- Cumplir con todos los estándares de categoría 6 ANSI/TIA/EIA 568-B.2-1, ISO11801 e IEC 61156, que especifica el balance que deben mantener los pares trenzados y aclara que el cable puede estar hecho entre 22 y 24 mm de diámetro y no mayor a 90 m de longitud, mientras que el cable supere las pruebas de desempeño que se detallarán posteriormente.

Cable de Enlace (Patch Cord)

Se utilizarán cables categoría 6, que cumpla con los requerimientos establecidos en el punto anterior y con terminaciones RJ-45. Dichos cables deberán estar certificados, por lo cual únicamente se aceptaran cables de enlace manufacturados en fábrica o por el instalador que cuente con certificación.

Para cada salida de voz y/o datos, se deben proporcionar los siguientes cables de enlace:

Patch Panel/Equipo activo: cable de enlace, Categoría 6, de 1.5 metros de longitud, similar a Panduit UTPSP5RDY. Se determinó esta longitud para el patch cord debido a la sugerencia del fabricante para obtener los mejores resultados de desempeño y poder certificarlo.

Toma de Datos/Equipo del usuario: cable de enlace, Categoría 6, de 3 metros de longitud, similar a Panduit UTPSP10RDY. Longitud dispuesta por el fabricante para certificación.

Fabricación de Patch Cords[6]

Dentro de la instalación y utilización de un Sistema de Cableado Estructurado, un punto importante es el de la fabricación de los Patch Cords, que se utilizarán tanto para la conexión entre equipos en los cuartos de telecomunicaciones y en el cuarto de equipos, como en las estaciones de trabajo.

[6] http://pagead2.googlesyndication.com

Es necesario entonces, definir la manera correcta en la que debe realizarse el procedimiento para armar un Patch Cord que cumpla con las normas para transmisión de datos con la configuración T568A o T568B, que son normas para la distribución de los pares trenzados dentro del conector RJ-45 y que se diferencian únicamente en la disposición de uno de ellos tal como se señalará en la figura 1.3..

Los pasos a seguir son los siguientes:

- Cortar el trozo de cable, de la medida necesaria. Los estándares 568-B recomiendan que la longitud máxima para un cable de conexión host-red no supere los 3 metros.

- Pelar los extremos del cable, quitando el revestimiento exterior de plástico en una longitud adecuada, aproximadamente 3 centímetros. La idea es que el cable, al ser insertado posteriormente en el Jack, tenga protección externa justo hasta la entrada a los pines.

- Si una porción de cable queda sin revestimiento, el cable se encontrará suelto, incrementándose las pérdidas de señal; y si queda menos las conexiones no se realizarán de forma correcta.

- Separar los cables, destrenzarlo y disponerlos según el esquema adecuado.

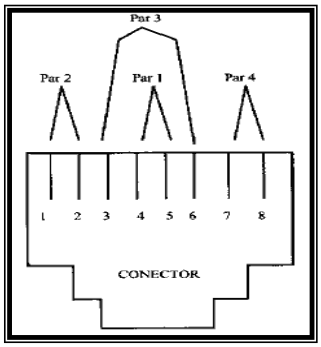


Figura 1.1. Distribución de cables en el conector

- Aplanar y recortarlos de tal forma que la longitud de los hilos no trenzados sea de unos 12 milímetros, distancia recomendada para conexión adecuada. No es necesario pelar los extremos de los hilos, ya que al ser presionados luego con la grimpadora se realiza este proceso de forma automática.

- Insertar los cables en el conector RJ-45 y empujarlos hasta el fondo, asegurándose de que llegan hasta el final, de tal forma que se puedan ver los hilos cuando se mira el conector desde el extremo.

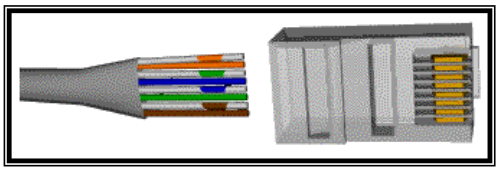


Figura 1.2. Inserción de cable en RJ-45[7]

- Inspeccionar que la distribución de hilos por colores esté de acuerdo con el esquema.

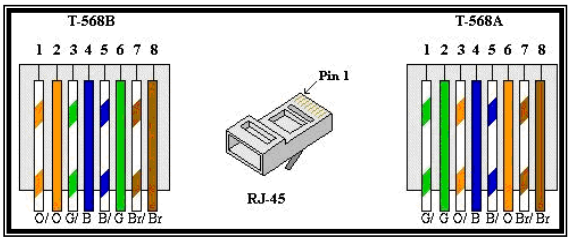


Figura 1.3. Esquema de colores del cable UTP según estándar[8]

- Acoplar los hilos al conector con la grimpadora, ejerciendo una buena presión en ésta, para que la conexión se realice correctamente.

- Realizar lo mismo con el otro extremo del cable.

- Una vez tenemos el cable, éste se conectará por un extremo en el conector de la tarjeta de red del host, y por el otro generalmente en la toma Jack RJ-45 hembra, situado en la pared, que será la que nos dé acceso a la red.

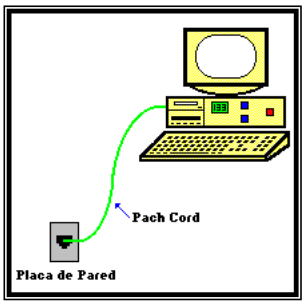


Figura 1.4. Diagrama de enlace con Patch cord

[7] http://www.axioma.co.cr/strucab/scmenu.htm

[8] http://www.axioma.co.cr/strucab/scmenu.htm

- Si tenemos que instalar dicha toma, el proceso es análogo al que se vio en la construcción de un cable, con la diferencia que ahora el propio Jack lleva unos códigos de colores que indican dónde debe ir cada hilo. Para insertar los hilos en los pines internos se usa una herramienta de punción especial, que corta el hilo y lo pela de forma automática. Una vez conectados los hilos, tan sólo queda acoplar el Jack en la caja atornillada a la pared.

- Si necesitamos un cable cruzado para conectar la tarjeta Ethernet de un PC directamente a otro, es necesario armar una punta del cable con la configuración T568A y el otro extremo configuramos la T568B, configuración que se detallará en la realización de Patch Cords.

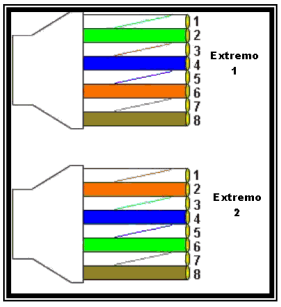


Figura 1.5. Terminaciones para cable cruzado

Rack

De acuerdo a las dimensiones de las habitaciones, las mismas que superan los dos metros de altitud, es adecuado colocar un Bastidor Estándar EIA de 19'' similar a Panduit CMR19X84, con las siguientes dimensiones: 84.0" x 20.3" x 3.0" (213.4cm x 51.4cm x 7.6cm), con el objeto de aprovechar al máximo el espacio físico.

Figura 1.6. Bastidor Panduit CMR19X84[9]

[9] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

Dicho equipo se fijará apropiadamente al piso adicionando una placa para piso de 55,9 cm. Se deberá dejar un espacio mínimo de 15,2 cm. entre el bastidor y la pared, para la ubicación del equipamiento, además de otros 30,5 a 45,7 cm. para el acceso físico de los trabajadores y del personal de mantenimiento, permitiendo acceder fácilmente tanto a la parte delantera como a la parte trasera de los equipos.

Gabinete de Pared

Se proporcionará un "Gabinete de Pared" para la instalación del equipo necesario, (conmutadores, paneles de conexión, etc.) en caso de que la red tenga un crecimiento no planificado al momento del dimensionamiento en 1.2.1.2, el gabinete debe cumplir con las siguientes características:

- Gabinete de pared similar a Great Lakes modelo GL24WM.
- De doble cuerpo.
- Capacidad de 6UR.

Figura 1.7. Gabinete de Pared Great Lakes GL24WM[10]

Patch Panels

Los Patch Panels a utilizar deben cumplir con las siguientes características:

- Panel de conexión metálico de 24 puertos, Categoría 6, similar a Panduit CP24BLY, debido a que la cantidad de puntos en cada sección es de 14, 42 y 14, respectivamente, superando el número de puertos que ofrece el compartimiento de 12 puertos que es el predecesor, por lo que con uno de 24 puertos se abarca ese requerimiento en forma óptima.

[10] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

- Debe proveer un área para la identificación de cada uno de los puertos.
- Instalable en Rack EIA 19''.
- Debe tener los 24 módulos Mini-Com (Cat. 6).

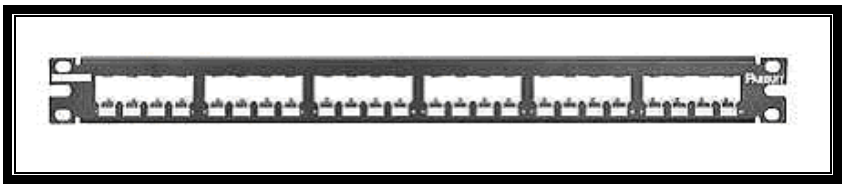


Figura 1.8. Patch Panel Panduit CP24BLY

Conectores RJ-45

Tanto las salidas para datos así como las de voz usarán conectores RJ-45 CAT 6, los mismos deberán cumplir todos los requerimientos establecidos en los estándares TIA/EIA-568-B.2- Adendum 10 e ISO 11801 Clase E, que expresa la posibilidad de terminaciones de cables sólidos AWG 22, 24 y 26, ya sea con T568A o T568B.

Dentro de él estarán los siguientes módulos:

Conector Macho:

Para las conexiones entre el Patch Panel y el equipo activo y para la conexión entre la toma final y el equipo del usuario se implementará un conector Categoría 6, similar a Panduit SP688-C.

Estos dispositivos se deberán implementar en los patch cords descritos anteriormente.

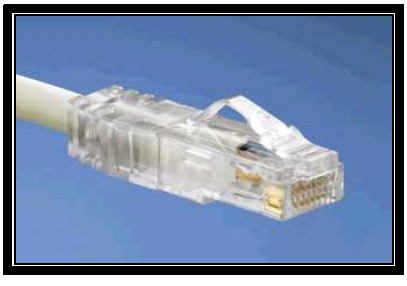


Figura 1.9. Conecto Macho RJ-45 Panduit SP688-C[11]

[11] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

Conector Hembra:

Este conector será de Categoría 6 igual a Panduit CJ6X88TGRD. Es sugerencia del fabricante, instalar dos por cada caja de conexión: voz y datos.

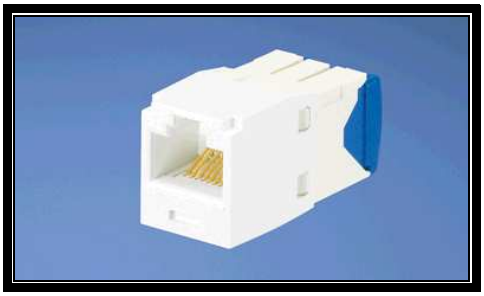


Figura 1.10. Conector Hembra RJ-45 Panduit CJ6X88TGRD.[12]

Accesorios para toma de Datos

Caja Universal para conectores RJ-45:

Caja plástica de una sola pieza, igual a Panduit JB1IW-A.

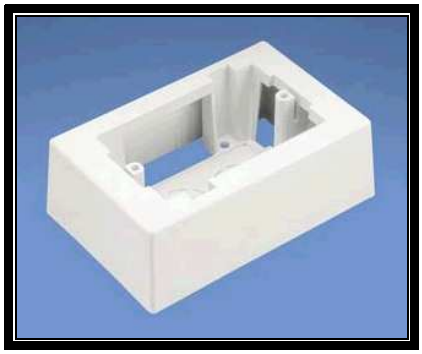


Figura 1.11. Caja Universal Panduit JB1IW-A[13].

Placa doble para conectores RJ-45:

Para todas las tomas de usuario que se instalen, se utilizarán placas dobles, para cubrir las necesidades de voz y datos simultáneamente. Estas placas deben ser de plástico de una sola pieza, equivalente a Panduit CFPE2IW-LY.

---

[12] UCRCI-Especificaciones Técnicas para Instalación de Cableado Estructurado 2007

[13] UCRCI-Especificaciones Técnicas para Instalación de Cableado Estructurado 2007

Figura 1.12. Módulo Doble Panduit CFPE2IW-LY.[14]

Placa sencilla para conectores RJ-45:

En casos especiales, por ejemplo tomas para puntos de acceso inalámbricos, como en Access Point, puentes inalámbricos, etc, en los que no se requiera de dos líneas, se utilizara una placa simple de plástico de una sola pieza, similar a Panduit CFPE1IW-LY.

Figura 1.13. Módulo Simple Panduit CFPE1IW-LY[15]

Organizadores

Será requisito imprescindible la utilización de organizadores verticales y horizontales en la terminación y armado de los conductores UTP en los Patch Panels, equipos activos y en el Rack en general.

---

[14] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

[15] UCRCI-ESPECIFICACIONES TÉCNICAS PARA INSTALACIÓN DE CABLEADO ESTRUCTURADO 2007

Organizador Vertical:

Organizador vertical equivalente a Panduit WMPVF45 que cumpla con las siguientes características:

- Encajable en Rack EIA de 19'' instalado anteriormente.
- Dimensiones: 2018.2x129x108mm
- Funcional tanto para cable UTP como para fibra óptica.

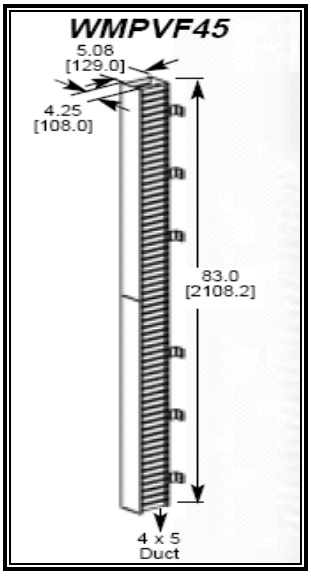


Figura 1.14. Organizador vertical Panduit WMPVF45[16]

Organizador Horizontal:

Organizador horizontal igual a Panduit WMPH2, que cumpla con las siguientes características:

- Instalable en Rack EIA de 19'', instalado anteriormente.
- Dimensiones: 88.1 x 207.5 x 508mm.
- Permitir organizar los cable tanto al frente como en la parte posterior.
- Funcional tanto para cable UTP como para fibra óptica.

[16] Manual para Certificación ORTRONICS

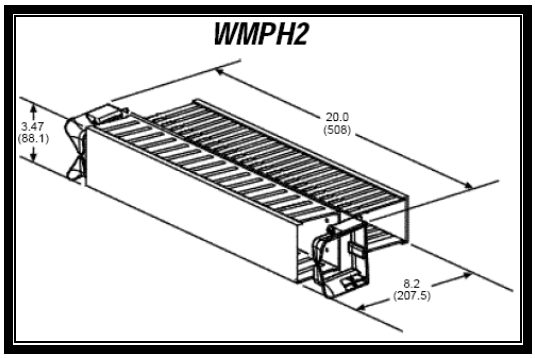


Figura 1.15. Organizador horizontal Panduit WMPH2

La organización trasera se utilizará exclusivamente para distribuir el cableado horizontal hacia los Patch Panels, mientras que la organización frontal se utilizará para la distribución de los Patch Cords.

Ductos tipo Canaleta Plástica

Canaleta plástica con características equivalentes a Pan-Way, Twin-70 de Panduit, de acuerdo con los tamaños previstos en el análisis del edificio, de la sección 1.2.1.1. de este capítulo. Todos los accesorios: codos, uniones, tapas, etc. deben pertenecer al mismo sistema de ductos y deben cumplir con los radios de curvatura mínimos establecidos en el estándar TIA/EIA 568-B, de 25 mm de radio.

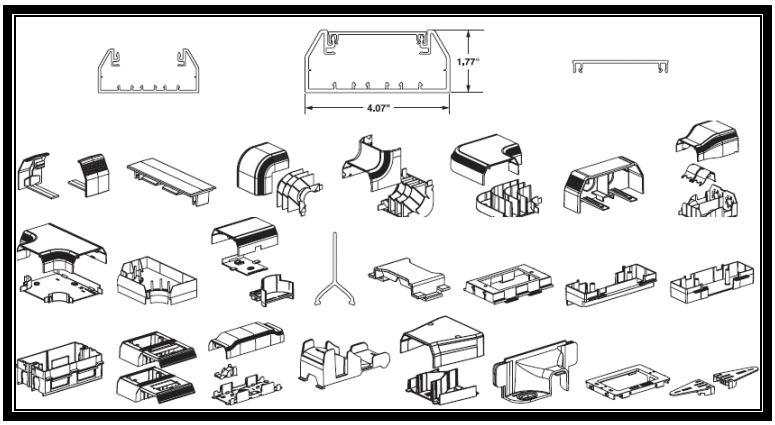


Figura 1.16. Accesorios del Sistema Pan-Way Twin –70[17].

[17] Manual para Certificación ORTRONICS

El ducto debe fijarse por medio de tornillos a una distancia no mayor de 60 cm entre puntos de sujeción. Para la transición de la canaleta plástica y la tubería Conduit PVC dentro del cielo raso, será requisito la utilización de los adaptadores de cielo, diseñados por el fabricante.

En todos los casos, la canaleta se construirá en forma continua, unificando perfectamente todas sus partes de tal manera que los conductores siempre se encuentren cubiertos por las paredes de la misma.

No se permitirá utilizar las paredes de concreto, fibrolit, madera o metal como parte de la canalización, bajo ninguna circunstancia y cuando se especifique canaleta para contener sistemas de potencia y cableado estructurado, solo se permitirá que viajen los conductores de potencia para los equipos sensitivos, conjuntamente con el UTP del Cableado Estructurado.

Es totalmente prohibido que circuitos de uso general, limpieza, electrodomésticos y otros viajen por esta canalización y se autorizará el uso de canaletas y accesorios que cumplan de extremo a extremo la separación garantizada de ambos sistemas, utilizándose componentes propios del sistema o recomendados por el fabricante.

Según la norma ANSI/TIA/EIA 568B, será requisito que los accesorios tengan radio de curvaturas de 25 mm para que no exista pérdidas en la transmisión.

Las canalizaciones para tal motivo que se aceptarán, serán aquellas estrictamente diseñadas y aprobadas para transportar conductores de potencia y cableado estructurado en una misma canalización, iguales a Panduit, sistema PAN-WAY Twin-70, en sus diferentes dimensiones y los accesorios recomendados por el fabricante.

Se debe verificar que se cumplan los índices de separación entre líneas para telecomunicaciones y líneas de energía, según lo establecido en la tabla 1.

Condición	Separación Mínima		
	< 2 KVA	2-5 KVA	> 5 KVA
Líneas eléctricas no blindadas o equipos eléctricos cercanos a vías de transmisión no metálicas o abiertas	127 mm. (5 plg.)	305 mm. (12 plg.)	610 mm (24 plg.)
Líneas eléctricas no blindadas o equipos eléctricos cercanos a una vía de telecomunicaciones de conducto metálico y aterrizado	64 mm. (2.5 plg.)	152 mm. (6 plg.)	305 mm. (12 plg)
Líneas de energía en conducto metálico aterrizado (o equivalentemente blindado) cercano a una vía de transmisión con conducto metálico aterrizado		76 mm. (3 plg)	152 mm. (6 plg)

Tabla 1.1. Separación mínima entre una vía de telecomunicaciones y un alambrado eléctrico de 480 V o menor.[18]

Canalizaciones Conduit

La Canalización tipo Conduit será de cloruro de polivinilo tipo PVC, similar a las distribuidas por Amanco y Durman Esquivel.

Para dicha canalización se respetará el siguiente lineamiento en cuanto a la cantidad de cables UTP según su diámetro:

Diámetro tubería Conduit	Máximo de cables
19 mm (3/4)	3
25 mm (1)	6
32 mm (1 ¼)	10

Tabla 1.2. Máximo de cables respecto al diámetro de tubería

Será requisito indispensable que todas las tuberías Conduit sean acopladas firmemente a la canasta de Cableado Estructurado, utilizando los conectores EMT de presión, adicionando un adaptador de canasta, igual o mejor al FLEX TRAY, de acuerdo con la tabla 1.3.:

[18] http://www.cecsa.net/frame_infocliente.html

Modelo	Diámetro del Conduit
FTEMTDO75	19 mm (3/4 plg)
FTEMTDO100	25 mm (1 plg)
FTEMTDO125	32 mm (1 ¼ plg)

Tabla 1.3. Modelo de adaptador respecto al diámetro del conduit

Figura 1.17. Accesorios para acople entre ductos Conduit y Canasta metálica.

En la trayectoria del cableado, no se aceptarán más de dos curvas de 90º entre cajas de salida. En caso necesario, se adicionarán cajas de registro para cumplir con lo anterior.

Canastilla Metálica

Las canastillas metálicas para transportar los cables UTP y/o Fibra Óptica, deberán ser metálicas electrosoldadas en Zinc galvanizado, similares a EZTray de Cablofil o Flextray.

Para su instalación se debe cumplir con lo siguiente:

- Debe ser continua de extremo a extremo, asegurándose el transporte seguro de los conductores UTP.
- Deberá permitir diversidad de formas para su instalación, así como contar con accesorios para su correcta fijación a las estructuras por las que deba viajar.
- En todos los casos se adicionarán los accesorios para suspensión recomendados por el fabricante; sean estos colgantes, de pared u otros.

- La canastilla deberá estar soportada en forma segura a intervalos no mayores de 150 cm, a menos que esté especialmente aprobada para soportar intervalos mayores.
- En ningún caso se aceptará que la canastilla sujete a la estructura del cielo suspendido o a ningún otro sistema de fijación del sistema eléctrico como tuberías, aeroductos, pues el soporte de la canastilla a la estructura del edificio será completamente independiente.
- Se permitirá que la canasta atraviese paredes de ser necesario, siempre y cuando se asegure la continuidad de la misma.
- Los diferentes propósitos definidos para el cableado UTP, se distribuirán en la canastilla de manera tal que viajen agrupados según su función: Datos, Voz. Únicamente se utilizarán amarras tipo Velcro para la fijación o amarre del UTP a la canasta.
- Las Canastillas para Cableado Estructurado, deberán acoplarse en forma adecuada con el Rack existente o por instalar, a cero metros.

1.2.3. DISEÑO DEL CABLEADO[19]

Para realizar el diseño del cableado de todo el edificio se tomarán en cuenta todas las consideraciones del la sección 1.2.1.1. de este capítulo, las proyecciones que se pueden realizar en base a los datos obtenidos para considerar puntos de respaldo ya sea por daño o expansión, que fueron ya tomadas en cuenta al dimensionar la red, además de la experiencia del técnico instalador en situaciones similares.

1.2.3.1. Cableado Horizontal

El cableado horizontal está formado por los cables que se extienden a través del techo de cada una de las plantas, desde el cuarto de telecomunicaciones ubicado en cada planta hasta las respectivas estaciones de trabajo del edificio. Este cableado consta de cables de par trenzado UTP categoría 6, dispuestos en topología estrella.

---

[19] Manual para Certificación SIEMON

Las canaletas son utilizadas para distribuir y soportar el cableado horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Cada punto terminal de conexión está conectado al Patch Panel del cuarto de equipo al que depende.

El cableado horizontal del edificio cumple con la máxima distancia horizontal permitida entre el Patch Panel y el punto terminal de conexión que es de 90 metros; y con la longitud máxima desde el punto terminal hasta la estación de trabajo que es de 3 metros, tal como se señala en la norma 568B.1.

1.2.3.2. Cableado Vertical

El cableado vertical para el edificio, está formado por cable UTP que sube desde el cuarto de equipos y que recorre todo el trayecto recogiendo cada uno de los cuartos de telecomunicaciones de las diferentes plantas.

1.2.3.3. Cuarto De Equipos

El Cuarto de equipos se ubicará en el área de Servicio Técnico, debido a que del análisis realizado en 1.2.1.1. es la que presenta mejores características en cuanto a seguridad y disponibilidad.

El área donde funcionará el Cuarto de Equipos es estratégico en cuanto a la seguridad que brinda a los equipos de comunicación de la red; además, en esa dependencia se encuentra laborando personal capacitado para solventar algún tipo de problema que pueda presentarse con éstos.

Se consideró también, como factor influyente a la hora de definir al área de Servicio Técnico como sitio de ubicación para el Cuarto de Equipos, el hecho de que allí se cuenta con un punto de fibra óptica, proveniente del proveedor, lo que va a permitir conectar la red y adaptarla a la velocidad de 100 Mbps. Este cuarto administrará y controlará toda la red del Edificio.

En ese cuarto estará presente el siguiente hardware:

- Un switch marca cisco 1990, con entrada de fibra óptica y 24 puertos de salidas UTP a 100 Mbps, pues se estableció anteriormente la necesidad de cada planta y la dimensión de este switch se ajusta a tales requerimientos.
- Un UPS.

Desde este Cuarto de Equipos se le proporcionan dos cables independientes a cada cuarto de telecomunicaciones de la red: uno para uso regular y otro de respaldo.

1.2.3.4. Cuartos de Telecomunicaciones

Se requiere ubicar tres Cuartos de Telecomunicaciones, uno por cada planta; de modo que se facilite la administración de la red, y de acuerdo a los datos obtenidos de la situación actual del edificio, los lugares que prestan mejores características para su establecimiento, debido a las seguridades que presentan, la disponibilidad del espacio y la ubicación estratégica que tienen para convertirse en un punto central de la carga de cada planta, son:

- Departamento Técnico, subsuelo
- Departamento de Importaciones, planta baja
- Departamento de Contabilidad, planta alta

1.2.3.4.1. Cuarto de Telecomunicaciones CT-01: Departamento Técnico

Es necesario colocar un Cuarto de Telecomunicaciones en esta área, la cual se ubica específicamente junto al Departamento Técnico, para que administre los distintos puntos de conexión que se ubicaran en esa área, en el área de Servicio Técnico y Bodegas.

De acuerdo al dimensionamiento de la red, realizado anteriormente, los equipos ubicados en este Cuarto de Telecomunicaciones, deberán dar soporte a 14 puntos de conexión distribuidos así:

- 2 Puntos de conexión en el Departamento Técnico
- 8 Puntos de conexión en Servicio Técnico
- 2 Puntos de conexión en el Bodega
- 2 Puntos de conexión en el Comedor (de respaldo)

Cabe mencionar que en el Departamento Técnico existe en la actualidad una estación conectada en red, con acceso a Internet, a través de una línea telefónica exclusivamente dispuesta para ello. Se integrará como un punto más de dicha red, bajo los mismos parámetros que se emplearán para las demás estaciones. Es debido a ello, que en lo posterior no se tomará en cuenta la conexión existente.

El hardware que utilizará el cuarto de Telecomunicaciones es el siguiente:

- Un concentrador SuperStack II Dual Speed Hub 500 de 24 puertos, los cuales ofrecen la potencia del Fast Ethernet a 100 Mbps, debido a que es el que cuenta con la capacidad suficiente para satisfacer la necesidad de esta área.
- Un UPS (Fuente de Alimentación Ininterrumpida).
- Un Rack de piso LAN-PRO.
- Patch Panel LAN-PRO de 24 puertos.

1.2.3.4.2. Cuarto de Telecomunicaciones CT-02: Departamento de Importaciones

Al realizar el dimensionamiento de la red, se estableció la cantidad de puntos de red que la planta baja necesita. Este cuarto de telecomunicaciones administrará entonces un total de 42 puntos de conexión distribuidos así:

- En Recepción: 2 puntos de conexión
- En los cubículos de Atención al Cliente: 16 puntos de conexión
- En el Departamento de Ventas: 8 puntos de conexión.
- 4 puntos de conexión en el Departamento de Marketing
- 4 Puntos de Conexión en el Departamento de Importaciones
- 4 Puntos de conexión para la Sala de reuniones
- 4 puntos de respaldo

Los componentes activos que utilizará este Cuarto de Telecomunicaciones es el siguiente:

- Dos concentradores SuperStack II Dual Speed Hub 500 de 24 puertos, los cuales ofrecen Fast Ethernet a 100 Mbps.

- Un UPS (Fuente de Alimentación Ininterrumpida).
- Un Rack de piso LAN-PRO.
- Dos Patch Panel LAN-PRO de 24 puertos.

1.2.3.4.3. Cuarto de Telecomunicaciones CT-03: Departamento de Contabilidad

El Cuarto de Telecomunicaciones de esta área se lo ubicar específicamente en la planta alta del edificio, en una dependencia identificada anteriormente como cuarto de comunicaciones, Dentro del departamento de Contabilidad que en el levantamiento previo de información, pudo determinarse que no está siendo utilizada y que cuenta con las exigencias que el sistema demanda en cuanto a seguridad.

En función de lo anterior, y de la ubicación estratégica que presenta este sitio, se colocará allí el CT-03 que controlará y administrará todos los puntos que se ubicarán en la Dirección Administrativa, la Gerencia general y el Departamento de Contabilidad.

Para la planta alta se requiere ubicar un total de 14 puntos, los cuales se distribuirán como se detalla a continuación:

- En el área de Dirección Administrativa se ubicarán 2 puntos de conexión.
- En la Gerencia General 4, y
- En el Departamento de Contabilidad, 6.

El hardware que se utilizará para este C.T es el siguiente:

- Un concentrador SuperStack II Dual Speed Hub 500 de 24 puertos, los cuales ofrecen Fast Ethernet a 100 Mbps.
- Un UPS (Fuente de Alimentación Ininterrumpida).
- Un Rack de piso LAN-PRO.
- Un Patch Panel LAN-PRO de 24 puertos.

Las características de los equipos activos seleccionados, fueron escogidas en base a los datos recabados en la situación actual del edificio, y el detalle de las especificaciones técnicas de los equipos activos que se utilizarán en el sistema y el de sus posibles sustitutos futuros, se presentan en el Anexo B del presente proyecto.

1.2.4. COMPROBACION DE ERRORES

Al terminar la instalación tanto de componentes activos como pasivos del sistema, se procede a verificar físicamente que haya sido efectuada sin la existencia de errores durante todo el camino.

El primer paso para realizar una comprobación de errores es observar detenidamente cada terminación, ya sea en los jacks modulares, en las tomas de pared y en los patch panels para constatar que tales terminaciones se encuentren correctamente efectuadas.

Es necesario también realizar un recorrido físico a lo largo de toda la trayectoria del cable a fin de cerciorarse de que no existan malformaciones en los mismos, cruces indebidos que afecten la transmisión de los datos, curvas que incumplan con los requerimientos de las normas, cortes, rupturas o desprendimientos del cable en algún tramo del recorrido.

No se permiten tampoco empalmes ni derivaciones en el sistema de cableado y debe constatarse que los radios de curvatura en los cables, no excedan lo permitido por las recomendaciones de cada fabricante.

1.2.5. CERTIFICACION

Una vez que se ha realizado la instalación y se ha determinado que no existen daños aparentes en su trazado ni en sus terminaciones es necesario que un técnico instalador o una empresa reconocida, establezcan la competencia de todo el sistema y emita la certificación correspondiente.

La empresa que realizará la certificación en este caso, es la empresa Hendel, subcontratada por el Grupo Jiménez-Andrade, pues cuenta con los equipos necesarios para tal fin y el respaldo de las compañías proveedoras de los componentes de cableado.

Para que un sistema de cableado pueda certificarse, éste debe cumplir con las normas establecidas por los organismos internacionales de estandarización, sean IEEE, ISO, entre otros. Para este caso se cumplirá la norma ANSI/TIA/EIA 568B.

En resumen, ANSI/TIA/EIA 568B establece 10 pruebas para determinar la idoneidad del cableado, como longitud, mapa de cableado, next, fext, etc. que son parte de la norma, las mismas que se detallarán en el capítulo posterior.

Una vez que se han efectuado estas pruebas y el cableado las ha superado en su totalidad o en el porcentaje que lo requiera el diseñador, se ha concluido con el trabajo de instalación y el proveedor de los componentes del cableado, lo puede certificar y además, puede emitir un certificado de garantía por un determinado tiempo.

Para el caso de la instalación del cableado estructurado en el edificio Mena-Merizalde, se realizaron todas las pruebas y los datos fueron satisfactorios para la aprobación y correspondiente certificación por parte de la empresa Hendel y el respaldo de garantía de la marca ORTRONICS.

CAPITULO II

2. PLAN DE REDUCCION DE RIESGOS

2.1. DEFINICIONES INICIALES[20]:

Organización: Asociación de personas regulada por un conjunto de normas en función de fines determinados.

Activos: Recursos del sistema de información o relacionados con éste, necesarios para que una Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Amenaza: Eventos que pueden desencadenar un incidente en una Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto: Consecuencia que tiene la materialización de una amenaza sobre un activo.

Siniestro o Incidente: Evento con consecuencias en detrimento de la seguridad o desempeño de la red.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a una Organización.

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo.

Vulnerabilidad: Estimación de la exposición efectiva de un activo a una amenaza. Se determina por dos medidas: frecuencia de ocurrencia y degradación causada.

Servicio: proceso por el cual se brinda satisfacción para determinada necesidad.

---

[20] Glosario de Términos de Guía de Seguridad de los Sistemas de Información

2.2. REALIZACION DEL ANALISIS DE RIESGOS

El Análisis de Riesgos permite determinar cómo son, cuánto valen y en qué grado se encuentran protegidos los activos. En forma conjunta con los objetivos, la estrategia y política de la Organización y las actividades de Gestión de Riesgos permiten elaborar un Plan de Seguridad que, implantado y en operación, puede satisfacer los objetivos propuestos con el nivel de riesgo que acepte la dirección de la Organización.

Realizar un Análisis de Riesgos requiere de un trabajo laborioso y de alto costo, además de la colaboración de muchas áreas dentro de una Organización, desde el nivel técnico hasta el gerencial. Es necesario también, lograr una uniformidad de criterio entre todos, pues resulta importante cuantificar los riesgos y más aún, relativizarlos.

Esto es así porque típicamente en un Análisis de Riesgos aparece una multitud de datos y la forma de enfrentar la complejidad que este análisis representa, es centrarse en lo más importante, es decir tener la consigna de: máximo impacto, máximo riesgo y obviar lo que es secundario o incluso despreciable.

Es visible entonces que un Análisis de Riesgo constituye una tarea mayor que requiere esfuerzo y coordinación, y que por lo tanto debe ser planificada y justificada.

Un análisis de riesgos es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión. En particular en cualquier entorno donde se realice el proceso electrónico de bienes y servicios, ya sea de carácter público o privado.

De esta manera un proyecto de cableado estructurado no está exento de análisis, es así que en este capítulo se desarrollará el Análisis de Riesgo de forma general para cualquier sistema de información y que se lo aplicará de manera particular para el proyecto realizado por parte del Grupo Jiménez-Andrade en el edificio Mena-Merizalde.

El Análisis de Riesgos es una aproximación metódica que puede determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los activos de importancia para la Organización, su interrelación y el costo que supondría su degradación.

2. Determinar a qué amenazas están expuestos dichos activos.

3. Estimar el impacto, definido como el daño sobre el activo por consecuencia de la materialización de la amenaza.

4. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

5. Determinar qué salvaguardas pueden existir y que tan eficaces son frente al riesgo.

La figura 2.1. muestra como están ligado estos pasos, cuyos detalle se expresará en las siguientes secciones:

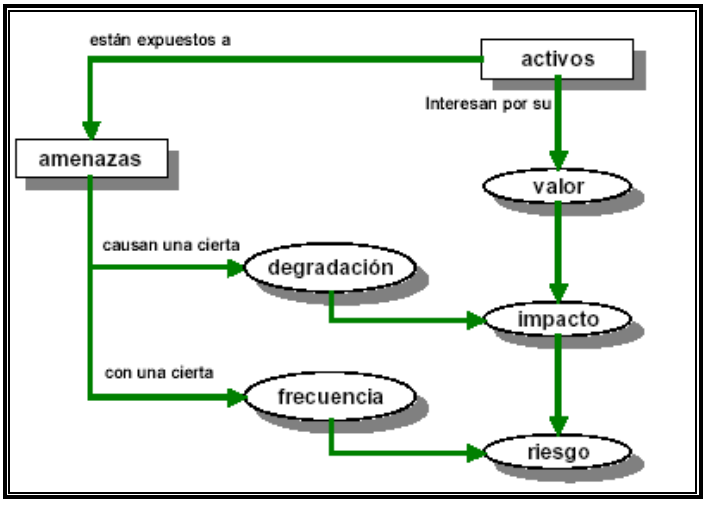


Figura 2.1. Diagrama de bloques de Análisis de Riesgos[21]

[21] Seguridad de la Información INEC

2.2.1. ACTIVOS[22]

Los Activos representan los recursos del sistema de información o que están relacionados con él y que son necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema, es decir los datos, y alrededor de éstos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los que se necesitan para poder gestionarlos.
- Las aplicaciones informáticas, es decir el software que permite manejar los datos.
- Los equipos informáticos, el hardware que permiten hospedar datos, aplicaciones y servicios.
- Los dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las Redes de Comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen los equipos informáticos y de comunicaciones.
- Las personas que operan con todos los elementos anteriormente citados.

De acuerdo al análisis de la situación actual del edificio Mena-Merizalde, se obtuvieron los siguientes datos de los activos pertenecientes a la empresa JH&H, especificado por cada piso de la siguiente manera:

[22] Manual de Seguridad en Redes ArCERT

Subsuelo

DEPENDENCIA	TIPO DE EQUIPO	CANTIDAD
Departamento Técnico	• Computador Desktop • Teléfono Directo • Extensión Telefónica	1 1 1
Servicio Técnico	• Computador Desktop • Teléfono Directo • Extensión telefónica • Impresora local • Fax	4 2 2 1 1
Bodega	• Computador Desktop • Teléfono Directo • Extensión Telefónica • Impresora local • Fax • Consola PBX	1 1 2 1 1
Comedor	• Extensión Telefónica	1

Tabla 2.1. Inventario de Activos del Subsuelo

Planta Baja

DEPENDENCIA	TIPO DE EQUIPO	CANTIDAD
Recepción	• Computador Desktop • Teléfono Directo • Extensión Telefónica	1 1 1
Atención al Cliente	• Computador Desktop • Teléfono Directo • Extensión telefónica • Impresora local • Fax	8 1 8 1 1
Departamento de Ventas	• Computador Desktop • Extensión Telefónica • Impresora local • Teléfono Directo	4 4 1 1
Departamento de Marketing	• Computador Desktop • Teléfono Directo • Extensión Telefónica	2 2 2
Departamento de Importaciones	• Computador Desktop • Teléfono Directo • Extensión Telefónica	1 1 1
Sala de Reuniones	• Extensión Telefónica • Retroproyector • Televisor • Computador Laptop	1 1 1 1

Tabla 2.2. Inventario de Activos de Planta Baja

Planta Alta

DEPENDENCIA	TIPO DE EQUIPO	CANTIDAD
Dirección Administrativa	• Computador Desktop • Teléfono Directo • Extensión Telefónica	1 1 1
Gerencia General	• Computador Desktop • Teléfono Directo • Extensión telefónica • Impresora local • Fax	2 1 2 1 1
Departamento de Contabilidad	• Computador Desktop • Extensión Telefónica • Impresora local • Fax • Teléfono Directo	4 3 2 1 1

Tabla 2.3. Inventario de Activos Planta Alta

TOTALIZACIÓN EQUIPOS DE LA EMPRESA JH&H	
TIPO DE EQUIPO	**CANTIDAD**
Computador Desktop	29
Computador Laptop	1
Televisión	1
Impresoras locales	7
Extensiones telefónicas	29
Líneas Telefónicas Directas	10
Fax	5
Retroproyector	1

Tabla 2.4. Inventario Total de Activos de JH&H

2.2.1.1. TIPOS DE ACTIVOS

Es evidente que no todos los activos son del mismo tipo. Por esta razón es de vital importancia definirlas pues las amenazas y las salvaguardas serán distintas en cada caso.

Por ejemplo, si el sistema maneja datos personales, estos suelen ser importantes por sí mismos y requieren, en su mayor parte, una serie de salvaguardas reguladas por la ley. En estos activos interesa determinar qué tratamiento hay que imponerles. El hecho de que un dato sea de carácter personal impacta sobre todos los activos involucrados en su tratamiento y custodia.

De manera similar ocurre con los datos sometidos a una clasificación de confidencialidad, en éstas, las copias están numeradas y sólo pueden llegar a ciertas personas, no deben salir del recinto y deben ser destruidas en forma prolija.

Para el caso del proyecto el sistema de información en el edificio Mena-Merizalde, se tomará principal atención al cableado estructurado como tal, pues representa el activo de menor rotación y el que sirve de base para todo el sistema de información que maneja la empresa JH&H.

2.2.1.2. DEPENDENCIAS ENTRE ACTIVOS

Los activos más llamativos suelen ser los datos y los servicios; pero estos activos dependen de otros, como pueden ser los equipos, las redes de comunicaciones o las personas que trabajan con dichos equipos. Por esto es importante determinar la dependencia que existe entre activos o la medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior.

Se dice que un activo superior depende de otro activo inferior cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. O, dicho en otras palabras, cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. De manera informal, puede interpretarse que los activos inferiores son los pilares en los que se apoya la seguridad de los activos superiores.

Se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

• **capa 1: El Entorno:** activos que se precisan para garantizar las capas subsecuentes

- Equipamiento y suministros: energía, climatización, etc
- Personal: de dirección, de operación, de desarrollo, etc.
- Otros: edificios, mobiliario, etc.

• **capa 2: El Sistema de Información:** la infraestructura de información**:**

- Equipos informáticos: hardware
- Aplicaciones: software
- Redes de Comunicaciones: cableado estructurado
- Soportes de información: discos, cintas

• **capa 3: La información**

- Datos
- Meta-datos: estructuras, índices, claves de cifra, etc.

• **capa 4: Las funciones de la Organización,**

justifican la existencia del sistema de información y le dan finalidad

- Objetivos y misión
- Bienes y servicios producidos

• **capa 5: Otros activos**

- Credibilidad de la Organización
- Conocimiento acumulado
- Integridad física de las personas

En el caso del la empresa JH&H, las capas estarían dispuestas de la siguiente manera:

Capa 1: Activos descritos en 1.2.1.1.
Capa 2: Activos descritos en 2.2.1.
Capa 3: Información de seguridad para accesos.
Capa 4: Edificio y bienes almacenados en Bodega.
Capa 5: Personal de la empresa, descrito en 1.2.1.1.

2.2.1.3. Valoración de los Activos

Es necesario definir que la razón por la cual interesa un determinado activo, es por su valor, teniendo en cuenta que no se hace referencia a lo que cuestan las cosas, sino a lo que valen. Cuando un activo no vale nada, se puede prescindir de él, de otra manera si no se puede prescindir deliberadamente de este activo, es que tiene cierto valor; es necesario entonces investigar cual es ese valor, puesto que esto es lo que hay que proteger.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un esquema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor de fondo suele estar en la información o datos que el sistema maneja, quedando los demás activos subordinados a las necesidades de explotación y protección de la información. Por otra parte, los sistemas de información explotan los datos para proporcionar servicios internos para la Organización o destinados a terceros, apareciendo una serie de datos necesarios para prestar un servicio.[23]

El conjunto de datos y servicios finales permite caracterizar funcionalmente una organización. Las dependencias entre activos permiten relacionar los demás activos con datos y servicios.

La Organización JH&H, que utilizará las instalaciones del edificio Mena-Merizalde, al ser una empresa dedicada a la comercialización de productos, fundamenta el valor de sus activos en el servicio que presta a sus clientes, siendo para este fin un sistema de información eficiente, sustentado a su vez por una red de cableado estructurado acorde a sus necesidades.

---

[23] Seguridad de la Información INEN

2.2.1.4. Dimensiones de un Activo

Dentro de un activo interesa reconocer diferentes dimensiones:

- **Autenticidad:** conocer el perjuicio que causaría no saber exactamente el responsable de determinada acción.
  Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar)

- **Confidencialidad:** estar al tanto del daño que causaría que lo conociera quien no debe.
  Esta valoración es típica de datos.

- **Integridad:** conocer el perjuicio que causaría que estuviera dañado o descompuesto.
  Esta valoración es típica de los datos, que pueden ser manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

- **Disponibilidad:** conocer el perjuicio que causaría no tenerlo o no poder utilizarlo.
  Esta valoración es típica de los servicios, tal como lo es el servicio de comercialización que presta la Organización arrendataria del Edificio Mena-Merizalde, de ahí que no dimensionar correctamente los archivos repercute directamente en los ingresos de la empresa.,

En sistemas dedicados a la administración electrónica o al e-business, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y dar un seguimiento a las fallas que pudieran darse, sean accidentales o deliberadas, pero que no es el caso de JH&H.

En estos activos, además de la autenticidad, interesa evaluar:

• La trazabilidad del uso del servicio: conocer el daño que causaría no saber a quién se le presta tal servicio. En otras palabras ¿Quién hace qué y cuándo?

• La trazabilidad del acceso a los datos: Conocer el daño que causaría no saber quién accede a qué datos y qué hace con ellos.

Dentro de un árbol de dependencias, donde los activos superiores dependen de los inferiores, es imprescindible valorar los activos superiores, los que son importantes por sí mismos. Automáticamente este valor se acumula en los inferiores, lo que no es impedimento para que también puedan merecer, adicionalmente, su valoración propia.

2.2.1.5. Determinación del Valor de un Activo

Una vez determinadas las dimensiones de seguridad que interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del costo que supondría salir de una incidencia que destrozara el activo.

Hay muchos factores a considerar:

• Costo de reposición: adquisición e instalación.

• Costo de mano de obra especializada invertida en recuperar el valor del activo.

• Lucro cesante: pérdida de ingresos.

• Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.

• Sanciones por incumplimiento de la ley u obligaciones contractuales.

• Daño a otros activos, propios o ajenos.

• Daño a personas.

• Daños al medio ambiente.

Los criterios más importantes a respetar son:

• La homogeneidad: es importante la posibilidad de comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.

• La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos.

Todos estos criterios se satisfacen con valoraciones económicas, de ahí que se vuelve común, el intentar fijarle precio a todo. Esta actividad resulta sencilla si se trata de aspectos tangibles como: equipamiento, horas de trabajo, etc.; pero al entrar en valoraciones más abstractas, intangibles como la credibilidad de la Organización, la valoración económica exacta puede ser difícil de realizar.

2.2.1.5.1. Valoración Cualitativa

Las escalas cualitativas resultan más sencillas de realizar y permiten avanzar con rapidez, pues se posiciona el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como órdenes de magnitud y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.[24]

Las valoraciones cualitativas tienen la limitante de no permitir la comparación de valores más allá de su orden relativo, por ejemplo no se pueden sumar valores dentro de ella.

2.2.1.5.2. Valoración cuantitativa

Las valoraciones numéricas absolutas representan gran complicación definirlas, pero en cambio prescinden de los problemas de las valoraciones cualitativas.

---

[24] Consejos Prácticos de Seguridad Informática

Realizar la suma de valores numéricos no tiene complicaciones y no permite la creación de controversias alrededor de su interpretación.

Además, si la valoración es monetaria, se pueden efectuar estudios económicos, al comparar lo que se arriesga con lo que cuesta la solución y se aclaran interrogantes como:

• ¿Vale la pena invertir tanto dinero en esta salvaguarda?
• ¿Qué conjunto de salvaguardas optimizan la inversión?
• ¿En qué plazo de tiempo se recupera la inversión?

Para el caso de JH&H se realizó una valorización únicamente cuantitativa tal como se demostró en 2.2.1.

2.2.1.5.3. El valor de la interrupción del servicio[25]

Dentro de las dimensiones mencionadas anteriormente, éstas permiten una valoración simple, ya sea cualitativa o cuantitativa, excepto la disponibilidad.

Es necesario tener en cuenta que no es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido supone la terminación de la actividad. Además, hay que considerar que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

De tal forma, para valorar la interrupción de la disponibilidad de un activo se debe utilizar una estructura más compleja, que pueda resumirse gráficamente, como muestra la figura 2.2.

[25] MAGERIT versión 2

2.2.1.5.4. Costo de Interrupción de la disponibilidad[26]

Figura 2.2. Gráfica del costo de las interrupciones

En la figura 2.2. aparece una serie de escalones de interrupción que terminan con la destrucción permanente o total del activo.

Este análisis puede efectuarse para cualquier activo de la Organización, pero para el caso del ejemplo anterior se ha tomado como activo de referencia a la Credibilidad de la Organización JH&H, por encontrarse en la capa superior de dependencias, analizado en 2.1.2.2.

En el ejemplo anterior, paradas menores o iguales a 2 horas se pueden asumir sin consecuencias. A partir de ahí, se disparan las alarmas hasta 6 horas, donde se estabilizan hasta completar 1 día, a partir de ahí se vuelve a disparar las alarmas.

Este crecimiento se estabiliza desde los 2 días, hasta las 2 semanas, donde vuelve a crecer. Y si la parada supera el mes, se puede decir que la Organización ha perdido totalmente su capacidad de operar.

Desde el punto de vista económico del remedio, gráficamente se observa que no es necesario gasto alguno por una parada menor a 2 horas. Vale la pena un cierto gasto por impedir que una parada supere las 6 horas o los 2 días.

---

[26] MAGERIT versión 2

Y cuando se valore lo que cuesta impedir que la parada supere el mes, hay que poner en la balanza todo el valor de la Organización frente al costo de las salvaguardas, pues podría ser inoficioso el enfrentar esa crisis.

2.2.2. AMENAZAS

El siguiente paso dentro del esquema planteado, consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son eventos que ocurren. Y dentro de todo lo que puede ocurrir, interesa lo que probabilísticamente puede pasarle a nuestros activos y causar un daño.

Hay accidentes o desastres naturales: terremotos, inundaciones; y desastres industriales: contaminación, fallas eléctricas, fallas de fábrica de los elementos del sistema de cableado, ante las cuales el sistema es víctima pasiva; pero no por ser pasiva debe permanecer indefenso.

Existen también, amenazas causadas por las personas, ya sean errores en la instalación o el manejo de los equipos de información y comunicación, ataques intencionales, robo, terrorismo, etc.

No todas las amenazas afectan a todos los activos, sino que existe una cierta relación entre el tipo de activo y lo que le podría ocurrir.

2.2.2.1. VALORACION DE LAS AMENAZAS

En el momento que un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinada la amenaza que puede perjudicar a un activo, se debe estimar lo vulnerable que se encuentra el activo, en dos sentidos:

En la degradación

Se determina el grado en que resultaría perjudicado el activo. La degradación mide el daño causado por un incidente en el supuesto de que ocurriera y se suele

caracterizar como una fracción del valor del activo y así definir que un activo se ha visto parcialmente degradado o totalmente degradado.

Si las amenazas no son intencionales, bastará conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde; de otra forma, si la amenaza es intencional, no se puede pensar en proporcionalidad debido a que el causante, puede realizar un daño de forma selectiva y en mayor medida, de acuerdo a sus intenciones.

En la frecuencia

Se determina los intervalos de tiempo en los que se materializa la amenaza.

La frecuencia pone en perspectiva aquella degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable materialización; mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos:

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

Tabla 2.1. Frecuencia de amenazas[27]

2.2.2.2. ANALISIS DE AMENAZAS AL SISTEMA DE CABLEADO ESTRUCTURADO

Para analizar las amenazas que enfrenta un sistema de cableado estructurado o en general un sistema de información a través de cableado, lo más conveniente es identificar que podrían darse de dos fuentes: interna y externa, además es necesario tomar en cuenta los datos de la situación actual del edificio Mena-Merizalde detallados en 1.2.1.1.

[27] MAGERIT versión 3

2.2.2.2.1. AMENAZAS INTERNAS

Dentro de las amenazas internas se definen aquellas que se producen durante la instalación y uso del cableado estructurado, y condiciones propias de fabricación de los elementos que intervienen en él.

Esto supone estudiar la infraestructura en su totalidad, cables, terminaciones, jacks, ductos, tuberías, localización y utilización, con el objeto de identificar todas las opciones que pudieran suponer una amenaza.

Los cables representan un gran porcentaje dentro de la totalidad de la red, de ahí que se consideran varios parámetros para que éstos puedan ser considerados apropiados para cumplir con los objetivos de las aplicaciones que se le van a dar.

Para que la implementación de cableado estructurado sea óptima, y minimizar en lo posible una amenaza interna, el cable de cobre necesita pasar varias pruebas dispuestas por la norma ANSI/EIA/TIA 568B que en esencia busca garantizar el desempeño de la red.

2.2.2.2.2. ESTÁNDARES DE PRUEBA DE CABLES.[28]

El estándar ANSI/TIA/EIA-568-B especifica diez pruebas que un cable de cobre debe pasar si va a ser utilizado en una LAN Ethernet moderna de alta velocidad, como las que se implementará en la compañía JH&H. Estos parámetros de prueba son:

MAPA DE CABLEADO.

El Mapa de cableado es utilizado para identificar errores físicos en la instalación. Verifica que la totalidad de los 4 pares de cables trenzados estén conectados a los pines correspondientes en ambos extremos del cable, además de revisar la existencia de corto circuitos y circuitos abiertos, pares invertidos o transpuestos.

---

[28] http://www.ghtcable.com/knowledge.asp?id=6

RETARDO DE PROPAGACIÓN

La prueba de retardo de propagación examina el tiempo en que tarda la señal en ser enviada de un extremo a otro.

Al conocer este retardo, se puede medir la longitud del cable por reflexión mediante un TDR (Time Domain Reflectometer).

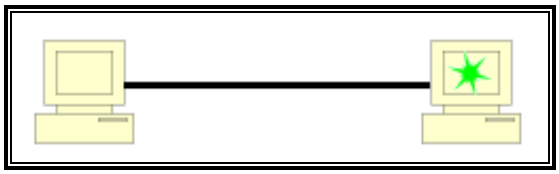


Figura 2.3. Gráfica de simulación de transmisión

DELAY SKEW

La prueba de Delay Skew (Sesgo de Retardo) mide la diferencia entre el tiempo de propagación del par de cables más rápido y el par más lento.

Un retardo ideal se encuentra entre 25 y 50 nanosegundos, medidos en un cable de 100 metros.

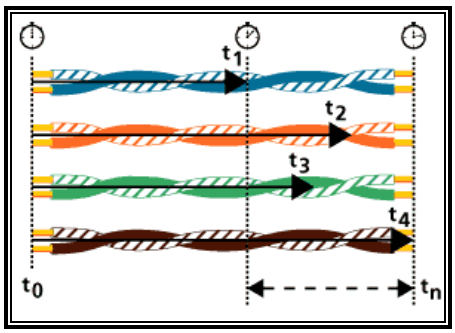


Figura 2.4. Representación de transmisiones por los diferentes pares

PERDIDA POR INSERCION

La pérdida por inserción, se refiere a la pérdida de la potencia de la señal en el extremo final de un cable en comparación con la señal que se introdujo al inicio del mismo.

Esta pérdida se debe a la resistencia eléctrica del cable de cobre, la pérdida de energía a través del aislamiento y el cambio de impedancia presente en los conectores. Por lo tanto, la pérdida por inserción aumenta conforme lo hace la longitud del cable y la frecuencia.

NEXT

El NEXT (Near End Cross Talk) es la relación existente entre la amplitud de la señal de prueba y la amplitud de la señal inducida, medida en el mismo extremo del enlace.

Mientras mayor sea el valor que entregue la medición (en dB), se considerará mejor al cable pues los valores entregados son en realidad negativos.

El NEXT se debe medir de par en par en un enlace UTP, y desde ambos extremos.

PSNEXT

PSNEXT (Power Sum NEXT) mide el efecto acumulado del NEXT de todos los pares de hilos del cable. PSNEXT se computa para cada par de hilos en base a los efectos de NEXT de los otros tres pares (Todos se excitan al mismo tiempo). El efecto combinado de la diafonía proveniente de múltiples fuentes simultáneas de transmisión puede ser muy perjudicial para la señal, especialmente cuando se emplean los cuatro pares, como en 1000BASET.

Para la prueba de PSNEXT se excitan tres pares de hilos y se mide el efecto combinado que tiene el NEXT de cada uno, en el restante. Este efecto combinado de la diafonía proveniente de múltiples fuentes simultáneas de transmisión perjudica a la señal, especialmente cuando se tratan de redes modernas de alta velocidad (1000 BASET) que utilizan los cuatro pares.

FEXT

FEXT (Far End Cross Talk) mide la relación existente entre la amplitud de la señal de prueba y la señal inducida en otro par, pero en el extremo lejano del enlace.

Debido a la atenuación del cable, la diafonía que ocurre a mayor distancia del transmisor genera menor ruido que el NEXT. El ruido causado por FEXT también regresa a la fuente, pero se va atenuando durante la propagación; por lo tanto, FEXT no es un problema tan grave como NEXT.

ELFEXT

ELFEXT (Equal Level FEXT) es la diferencia entre la pérdida FEXT medida y la pérdida de inserción.

PSELFEXT

PSELFEXT (Power Sum ELFEXT) es el efecto combinado de ELFEXT de todos los pares de hilos.

PERDIDA DE RETORNO

Pérdida de retorno es la medición (en dB) de la cantidad de señal que se refleja de nuevo hacia el transmisor. La reflexión de la señal es causada por las variaciones de impedancia en el cable y conectores y suele atribuirse a una mala terminación del cable. Cuanto mayor es la variación en la impedancia, mayor es la pérdida por retorno.

LONGITUD DE CABLE

El test de longitud de de cable verifica que el cable desde el transmisor hasta el receptor no sobrepase la distancia máxima recomendada de 100 metros, en una red 10/100/1000BaseT.

ACR

ACR (Attenuation to Crosstalk Ratio) es la diferencia entre la Atenuación sufrida por la señal y el Next.

El ACR debe ser de al menos varias decenas de decibelios para un correcto desempeño. Si el ACR no es lo suficientemente grande, los errores serán frecuentes. En muchos casos, incluso una pequeña mejora en el ACR puede causar una reducción drástica en la tasa de error de bits. A veces puede ser necesario pasar de un par trenzado no pantallado (UTP) a un par trenzado apantallado (STP), a fin de aumentar el ACR.

PSACR

PSACR (Power Sum ACR) se realiza de la misma manera que el ACR, pero usando el valor de PSNEXT en lugar de NEXT.

Las pruebas detalladas anteriormente fueron realizadas al sistema de cableado estructurado del Edificio Mena-Merizalde por parte de Hendel y en todas ellas, el sistema arrojó datos adecuados para aprobarlas.

2.2.2.2.3. AMENAZAS EXTERNAS[29]

Las amenazas externas a las que está expuesta una Organización son diversas, pues las situaciones y los entornos que lo influyen así lo son. Por ello no se realiza una valoración particularizada de estas amenazas sino que éstas se engloban en una tipología genérica dependiendo del agente causante de la amenaza

Las amenazas externas que afectan a la Organización JH&H, se deben a diversos factores, y éstos pueden ser ambientales, humanos y técnicos.

Factores ambientales

Incendios. Los incendios son causados por el uso inadecuado de combustibles, fallas en instalaciones defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

[29] MAGERIT versión 2

Inundaciones. Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en los sistemas de redes.

Sismos. Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan, o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas.

Humedad. La humedad se produce debido a un mal funcionamiento de las instalaciones hidráulicas que se encuentran alrededor de las paredes y techo de la infraestructura del edificio.

Factores humanos[30]

Robos. Los activos de información tienen el mismo interés para sustraérselas que las piezas de stock e incluso el dinero que pueda tener la Organización.

Actos vandálicos. En las organizaciones existen empleados descontentos que pueden tomar represalias contra los equipos y las instalaciones.

Actos vandálicos contra el sistema de red. Muchos de estos actos van relacionados con el sabotaje.

Fraude. Cada año millones de dólares son sustraídos de varias Organizaciones dedicadas a la misma actividad que JH&H y en muchas ocasiones los centros de información han sido utilizados para dichos fines.

Sabotaje. Es el peligro más temido en los sistemas de información y comunicación. Algunas Organizaciones que han intentado implementar sistemas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, pues el saboteador puede ser un empleado o un sujeto ajeno a la empresa.

---

[30] http://www.sucre.udo.edu.ve/comp_ac/logro2.html

Terrorismo. Años atrás, éste hubiera sido un caso remoto, pero en la situación bélica que enfrenta el mundo en general, las Organizaciones deben de incrementar sus medidas de seguridad, por lo que las de renombre, como JH&H, representan un blanco más llamativo para los terroristas.

Factores Técnicos

Distribución Eléctrica: Todos los dispositivos de una red necesitan corriente eléctrica para su funcionamiento. Los computadores son dispositivos especialmente sensibles a perturbaciones en la corriente eléctrica y cualquier estación de trabajo puede sufrir estas perturbaciones, aunque esta contrariedad perjudique exclusivamente a un único usuario.

Sin embargo, si el problema se produce en un servidor o en los equipos de los cuartos de telecomunicaciones o de equipos, el daño es mucho mayor, ya que está en juego el trabajo de toda o gran parte de una organización. Esta amenaza es de consideración, pues el edificio Mena-Merizalde se encuentra en la zona norte de Quito, en un sector donde se tiene antecedentes de fallas de distribución eléctrica.

2.2.3. DETERMINACIÓN DEL IMPACTO

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos en varias dimensiones y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

2.2.3.1. Impacto Acumulado

El Impacto Acumulado es el calculado sobre un activo teniendo en cuenta:

• Su valor acumulado, el propio más el acumulado de activos que dependen de él.

• Las amenazas a las que está expuesto

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es directamente proporcional al valor propio o acumulado sobre un activo y a la degradación del activo atacado.
El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas que hay que adoptar por los medios de trabajo: protección de los equipos, copias de respaldo, y demás.

2.2.3.2. Impacto Repercutido

Es el calculado sobre un activo teniendo en cuenta

• Su valor propio
• Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.
El impacto es directamente proporcional al valor propio de un activo, a la degradación del activo atacado y a la dependencia que presente el activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información.

Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

2.2.3.3. Agregación de valores de impacto

Hasta este momento, se ha determinado el impacto que tendría una amenaza sobre un activo, en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

• Agregar el impacto repercutido sobre diferentes activos.
• Agregar el impacto acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común.

No se debe agregar el impacto acumulado sobre activos que no sean independientes, pues ello supondría ponderar de forma redundada el impacto al incluir varias veces el valor acumulado de activos superiores.

• Agregar el impacto de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.
• Agregar el impacto de una amenaza en diferentes dimensiones.

2.2.4. DETERMINACIÓN DEL RIESGO

Se denomina riesgo a la medida del daño probable sobre un sistema. Al conocer el impacto de las amenazas sobre los activos, se puede derivar directamente el riesgo teniendo en cuenta solamente la frecuencia con la que puede ocurrir.

Se determina entonces que el riesgo crece con el impacto y con la frecuencia de acción la amenaza.

2.2.4.1. Riesgo acumulado

El riesgo acumulado es aquel calculado sobre un activo teniendo en cuenta:

• El impacto acumulado sobre un activo debido a una amenaza y
• La frecuencia de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la frecuencia de la amenaza.

El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas a adoptar por los medios de trabajo: protección de los equipos, copias de respaldo, etc.

2.2.4.2. Riesgo repercutido

El riesgo repercutido es el calculado sobre un activo teniendo en cuenta:

• El impacto repercutido sobre un activo debido a una amenaza y
• La frecuencia de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la frecuencia de la amenaza.

El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

2.2.4.3. Agregación de riesgos

Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

• Agregar el riesgo repercutido sobre diferentes activos.
• Agregar el riesgo acumulado sobre activos que no sean dependientes entre sí, ni dependan de ningún activo superior común.

No se debe agregar el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores.

• Agregar el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes.

• Agregar el riesgo de una amenaza en diferentes dimensiones.

2.2.5. SALVAGUARDAS[31]

De forma evidente, los pasos anteriores no han tomado en consideración las salvaguardas desplegadas. Por lo tanto se miden los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es común encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos, programas o equipos, otras seguridad física y, por último, política de personal.

Las salvaguardas entran en el cálculo del riesgo de dos formas:

2.2.5.1. Reducción de la frecuencia de las amenazas.

Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

[31] Seguridad de la Información INEC

2.2.5.2. Limitación del daño causado.

Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

En la figura 20 se puede observar como repercute la introducción de las salvaguardas en el esquema presentado anteriormente en el punto 2.2.

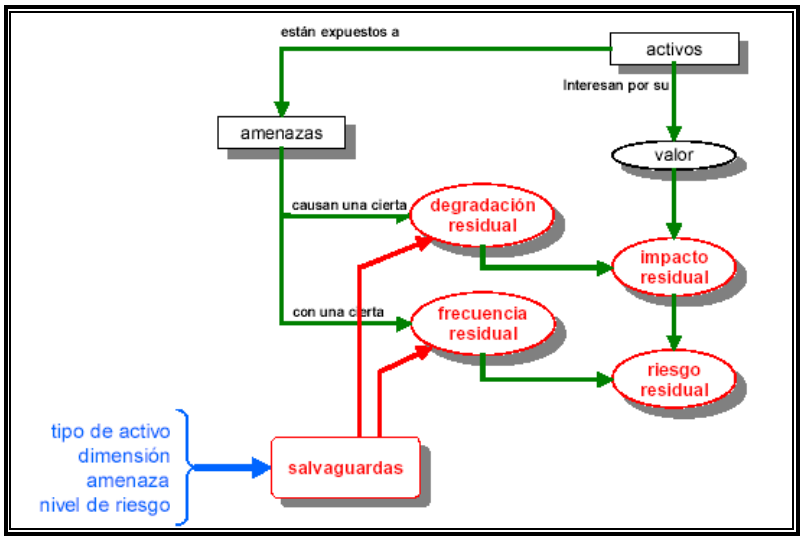


Figura 2.5. Diagrama de bloque análisis de riesgo, incluyendo salvaguardas

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea
- Está perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concienciados
- Existen controles avisan posibles fallos

Entre una eficacia del 0% para aquellas que son inservibles y el 100% para aquellas que son perfectas, se estimará un grado de eficacia real en cada caso concreto.

2.2.5.3. Impacto Residual

Si se ha realizado la Determinación del Impacto a la perfección, el impacto residual será despreciable, en cambio si existen actividades inconclusas, mal realizadas: normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles inoficiosos, entonces se dice que el sistema permanece sometido a un impacto residual.

El cálculo del impacto residual es sencillo, pues como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.
El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.2.5.4. Riesgo residual

Si se ha realizado la Determinación del Riesgo a la perfección, el riesgo residual será despreciable, en cambio si existen actividades inconclusas o mal realizadas: normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes, o controles que no funcionan, entonces se dice que el sistema permanece sometido a un riesgo residual.

El cálculo del riesgo residual es sencillo, pues como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la frecuencia de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la nueva tasa de ocurrencia.

La magnitud de la degradación se toma en consideración al momento del cálculo del impacto residual.

La magnitud de la frecuencia tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

2.2.5.5. SALVAGUARDAS SUGERIDAS POR LOS FABRICANTES DE LOS ELEMENTOS DE CABLEADO

Las empresas orientadas a la fabricación de los cables utilizados en Cableado Estructurado y la experiencia de las personas que realizan tales implementaciones, coinciden en varios procedimientos durante la instalación y utilización que aseguran el pasar las pruebas mencionadas anteriormente, y por lo tanto disminuir las amenazas al sistema, tanto en su impacto como en su riesgo, y éstas son:

a) No realizar mazos de cables, es decir dejar de lado la estética por el rendimiento del sistema.

b) No juntar, sujetar o amarrar los cables. En caso de no poder cumplir esta demanda se debe utilizar cables con blindaje en lugar de UTP.

c) No efectuar bifurcaciones ni derivaciones, y en lo posible reducir al mínimo la existencia de puntos de consolidación.

d) Al momento del ponchado de cables (terminaciones), hacerlo con herramienta de comprobada eficacia. Procurar siempre que las terminaciones sean exactas y no exista bordes desalineados ni que exista lugares donde el cable se encuentre descubierto.

e) Durante el paso del cable por tuberías, ductos o lugares donde se necesite realizar una tensión de halado al cable, ésta no debe exceder las 25 libras.

f) Se recomienda mantener un radio de curvatura mínimo para las desviaciones del cable, que puede ser de 0.25 pulgadas para patch cords y de cuatro veces su diámetro, en cableado horizontal y vertical.

g) Instalar un sistema a tierra en conformidad con el estándar J – STD 607A. El propósito es impedir que las partes metálicas que posee un equipo se carguen con voltajes peligrosos, resultante de un falla del cableado dentro del dispositivo, o por causas de sobretensiones externas, como las ocasionadas por tormentas eléctricas o problemas ocasionadas por falla de equipos del operador que nos suministra la energía eléctrica primaria.

El detalle del estándar se encuentra en el anexo C del presente proyecto de titulación.

2.2.5.6. SALVAGUARDAS GENERALES PARA EL EDIFICIO MENA-MERIZALDE

Además de cumplir con las salvaguardas sugeridas por los fabricantes, se analizará las amenazas detalladas en 2.2.2. para proceder a determinar las salvaguardas más acordes para el edificio Mena-Merizalde:

2.2.5.6.1. Salvaguardas para afirmar la Seguridad Física

La Seguridad física es primordial dentro de todo el sistema, por ello merece una mención principal dentro de las salvaguardas a implantarse.

Es necesario definir en primer lugar las salvaguardas para el cuarto de equipos, y los cuartos de telecomunicaciones donde se ubican los equipos principales de proceso de datos, aquí debe dotarse de medidas de seguridad acordes con las características del equipo a proteger, su valor y su importancia.

Lo ideal para la selección de la ubicación de los cuartos principales, es buscar la parte más conservadora y clandestina, la cual debe estar lejos del área del tránsito de gran escala, tanto terrestre como aérea; también lejos de equipos eléctricos tales como equipos de microondas. El objetivo es mantenerlos tan lejos como se pueda de cualquier tipo de amenaza.

En la medida de lo posible, el cuarto de equipos (que es el más importante) no debe de contener señal alguna que lo identifique como tal ante la gente externa. Incluso se recomienda de ser posible que el sistema matriz que procese la información sea construido en una sección separada, de forma que facilite el control de acceso y disminuya el riesgo, pero que no es el caso del edificio Mena-Merizalde.

Entre los aspectos que se deben tomar en consideración están la planeación de la distribución física del cuarto de equipos, de los cuartos de telecomunicaciones, y de la trayectoria del cableado, tomando en cuenta los riesgos concernientes a desastres naturales: inundaciones, fuego, fallas eléctricas, polvo, etc, así como la luz solar, si la exposición es muy fuerte; debe evitarse el uso del vidrio; en los casos que no sea posible, pueden utilizarse persianas externas.

Es necesario también considerar que no exista suelos sometidos a vibraciones o la proximidad de maquinaria pesada o de vías de comunicación: ferrocarriles, puentes, etc. Pues pueden ocasionar daños en los equipos de almacenamiento, por el peligro del aterrizaje de los cabezales de lectura y grabación.

Por otro lado, hay que considerar también la resistencia del suelo en instalaciones grandes, para evitar el riesgo de hundimientos de la estructura por sobrecarga.

En los sitios donde la información es altamente sensitiva, como lo es en el cuarto de equipos, se debe tomar en cuenta también el riesgo producido por las emanaciones electromagnéticas o acústicas del hardware, ya que éstas pueden ser interceptadas con relativa facilidad en una distancia menor a los 300 metros. Para ello, la opción es la separación de los dispositivos de los puntos potenciales de interrupción.

Por todas las especificaciones mencionadas anteriormente, se determinó la ubicación de los cuartos de telecomunicaciones y el cuarto de equipos en la forma que se determinó en la sección 1.2.3.3. y 1.2.3.4.

Detalle de los equipos utilizados

Para la selección de todos y cada uno de los equipos que se utilizarán, se ha tenido como base principal su proyección positiva en futuras expansiones del sistema y que

soporten tecnología 10/100/1000 Base Tx., la cual se implementará en este proyecto, de acuerdo al análisis realizado en un principio en el capítulo 1.

Otro aspecto muy importante que se tuvo en cuenta fue la garantía y soporte técnico que el proveedor nos brindará tanto a nivel distribuidor directo local, como a nivel de fábrica, eligiendo así marcas de prestigio, reconocidas y de amplia trayectoria a nivel mundial.

TIPO DE EQUIPO	CANTIDAD	MARCA
Computador Desktop	29	HP EVO D 510 SFF
Computador Laptop	1	HP PAVILON
Impresoras locales	7	XEROX PACER 5500
Switch	4	24 puertos capa 3
Fax	5	SHARP UX-66

Factores inherentes a la infraestructura del Sistema de Información

La construcción del interior de las instalaciones del Sistema de Información tiene gran importancia dentro del proyecto total y por lo tanto estará basado en los antecedentes de la situación actual del edificio, descrito en 1.2.1.1.

Las características de los elementos internos del sistema son:

- **Piso falso**. Se debe tener en cuenta la resistencia para soportar el peso del equipo y el personal. Entre otras consideraciones están:

    - Sellado hermético.
    - Modularidad precisa, que los cuadros ensamblen perfectamente.
    - Nivelado topográfico.
    - Posibilidad de realizar cambios en la situación de unidades.
    - Aterrizado para evitar cargas electrostáticas.
    - Debe cubrir los cables de comunicación entre la unidad central de proceso (CPU) y los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.
    - Deberá proporcionar seguridad al personal.

- Debe permitir que el espacio entre los dos suelos actúe como una cámara plena de aire, que facilite el reparto de cargas.
- La altura recomendable será de 30 cm. si el área de la sala de cómputo es de 100 metros cuadrados o menos, y de 40 a 60 cm. si es mayor de 100 metros cuadrados.
- La altura mínima podrá ser de 18 cm. si la sala es pequeña. Todo lo anterior es con objeto de que el aire acondicionado pueda fluir adecuadamente en la cámara plena.
- Puede ser de acero, aluminio o madera resistente al fuego.
- El mejor piso deberá estar soportado por pedestales o gatos mecánicos.
- Cuando se utilice como cámara plena para el aire acondicionado, tendrá que cubrirse el piso firme con pintura antipolvo.

- **Cableado**. El cableado en el cuarto de equipo y en los de telecomunicaciones, debe procurarse que quede por debajo del piso falso, donde es importante ubicar los cables de forma que se aparten:

  - Los cables de alto voltaje para las computadoras.
  - Los cables de bajo voltaje conectados a las unidades de las computadoras.
  - Los cables de telecomunicaciones.
  - Los cables de señales para dispositivos de monitoreo o detección (fuego, temperatura, humedad, etc.).

  En este sentido cabe señalar que es recomendable utilizar a lo largo de toda la trayectoria, en especial del recorrido vertical, un tipo de cable que además de cumplir con las características señaladas en los capítulos anteriores, cuente también con un recubrimiento que no propague el fuego y por el contrario al consumirse aplaque las llamas.

- **Paredes y techo**[32]

    - Las paredes irán con pintura plástica lavable para poder limpiarlas fácilmente y evitar la erosión.
    - El techo real deberá pintarse, así como las placas del falso techo y los amarres, si éste se emplea como plenum para el retorno del aire acondicionado.
    - Es mejor usar placas metálicas o de madera prensada para el piso falso con soportes y amarres de aluminio.
    - La altura libre entre el piso falso y el techo falso debe estar entre 2.70 y 3.30 metros para permitir la movilidad del aire.

- **Puertas de acceso**

    - Las puertas de ingreso hacia el cuarto de equipo y los de telecomunicaciones, serán de doble hoja y con una anchura total de 1.40 a 1.60 cm.
    - Es necesario una salida de emergencia.
    - Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias.

- **Iluminación**

    - Los reactores deben estar fuera de la sala, ya que generan campos magnéticos, o en su caso deben aislarse.
    - La iluminación no debe alimentarse de la misma acometida que los equipos de cómputo.
    - En el área de máquinas debe mantenerse un promedio mínimo de 450 luxes a 70 cm del suelo.
    - Debe evitarse la luz directa para poder observar la consola y las señales.
    - Del 100% de la iluminación, deberá distribuirse el 25% para la iluminación de emergencia y se conectará al sistema de fuerza ininterrumpible.

---

[32] Manual de Instalación de Cableado Estructurado SIEMON

- **Filtros**

    - Se requieren filtros con una eficiencia del 99% sobre partículas de 3 micrones.
    - Si hay contaminantes, elegir los filtros adecuados.
    - El aire de renovación o ventilación será tratado tanto en temperatura y humedad como en filtrado antes de entrar en la sala.
    - Son recomendables los tipos de humificadores de vapor.

- **Vibración**

    - Si hay vibraciones superiores a las normales, es necesario estudiar antes de colocar los equipos y utilizar los dispositivos anti – vibratorios necesarios, ya que la vibración podría dañar el equipo.

- **Ductos**

    - Serán de material que no desprenda partículas con el paso del aire.
    - No deberán tener revestimientos internos de fibras.

2.2.5.6.2. Salvaguardas para afirmar la Seguridad Física por acción de terceros

CONTROLES DE ACCESO FÍSICO

El principal elemento de control de acceso físico involucra la identificación positiva del personal que entra o sale del área bajo un estricto control. Si una persona no autorizada no tiene acceso, el riesgo se reduce.

Los controles de acceso físico varían según las distintas horas del día. Es importante asegurar que durante la noche sean tan estrictos como durante el día. Los controles durante los descansos y cambios de turno son de especial importancia.

Es determinante definir lo siguientes elementos para diseñar los procedimientos de acceso en una instalación:

Estructura y disposición del área de recepción

En las áreas de alta seguridad donde se necesita considerar también la posibilidad de ataque físico se debe identificar y admitir tanto a los empleados como a los visitantes de uno en uno. También se pueden utilizar dispositivos magnéticos automáticos y otros recursos en el área de recepción.

Acceso de terceras personas

Dentro de las terceras personas se incluye a los de mantenimiento del aire acondicionado y de computación, los visitantes y el personal de limpieza. Éstos y cualquier otro personal ajeno a la instalación deben ser:

- Identificados plenamente.
- Controlados y vigilados en sus actividades durante el acceso.

El personal de mantenimiento y cualquier otra persona ajena a la instalación se debe identificar antes de entrar a ésta. El riesgo que proviene de este personal es tan grande como de cualquier otro visitante.

Identificación del personal[33]

Algunos parámetros asociados típicamente a la identificación del personal son:

- **Algo que se porta:** Consiste en la identificación mediante algún objeto que porta tal como, tarjetas magnéticas, llaves o bolsas. Por ejemplo, las tarjetas pueden incluir un código magnético, estar codificadas de acuerdo al color (rojo para los técnicos, azul para personal administrativo, etc.), e inclusive llevar la foto del propietario.

[33] Seguridad industrial en la administración informática (UPIICSA)

Un problema con esta técnica, sin embargo, es la posibilidad de que el objeto que se porta sea reproducido por individuos no autorizados. Es difícil pero no imposible reproducir una tarjeta con código magnético. Es por esta razón que esta técnica se utiliza en conjunción con otros identificadores para proporcionar una identificación positiva.

Algunos ejemplos de gafetes de identificación son los siguientes:

- Con fotografía. La organización debe proporcionar a todo el personal una credencial con fotografía en la que se debe especificar el nombre del empleado, departamento, área y horario de trabajo.
- Con código óptico.
- Con código en circuito impreso.
- Con código magnético. Son tarjetas que permiten abrir puertas.

Asimismo, los dispositivos de lectura de las tarjetas pueden ser conectados a una computadora que contenga información sobre la identidad del propietario.

- Con código en banda magnética
- Con código electrónico pasivo
- Con código electrónico activo
- Tarjeta Inteligente (“Smart Card”)

- **Algo que se sabe:** Implica el conocimiento de algún dato específico, como:
  - El número de empleado
  - Un password
  - Un código de acceso
  - Respuesta a una pregunta
  - Una fecha de nacimiento
  - Un dato personal

- **Algunas características físicas especiales:** La identificación se realiza en base a una característica física única, es decir por biometría.

La Biometría, se define como, la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.
La identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por sus manos, ojos huellas digitales y voz.

Existen distintas técnicas biométricas, tales como:

- **Reconocimiento de huella digital.** Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital tiene arcos, ángulos, bucles remolinos etc. (llamados minucias).
  Las características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen mas de 8 minucias iguales y cada una posee mas de 30, lo que hace al método sumamente confiable.

- **Geometría de la mano.** Se reconoce la geometría específica que cada ser humano presenta en sus manos, líneas y comisuras.

- **Reconocimiento de la Voz.** La dicción de una o mas frases es grabada y en el acceso se compara la voz (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo, enfermedades de la persona, envejecimiento, etc.

- **Scanner de Patrones Oculares.** Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son considerados los más efectivos por que en 200 millones de personas la probabilidad de coincidencia es casi 0. su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en los mismos enfermedades que en ocasiones se prefiere mantener en secreto.

- **Dinámica de tecleo.** Se identifica la secuencia de teclas correcta asignada por el administrador para cada usuario.

- **Reconocimiento de cara.** Para este permiso tiene que identificarse los rasgos sobresalientes y propios del rostro de cada usuario, estructura ósea, nariz, mentón, cavidad ocular.

- **Impresión labial.** Se realiza de manera análoga a la toma de huellas digitales, combinando en algunos casos con otros métodos que aseguren la verificación de usuario.

- **Patrones de ondas cerebrales.** Se toman muestras de las ondas cerebrales y se realizan extrapolaciones para determinar valoraciones características de cada sujeto.

- **Emisión de calor.** Se mide la emisión de calor del cuerpo (termograma), realizando mapas de valores sobre la forma de cada persona.

- **Dinámica de la firma.** En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadernarse dentro de las verificaciones biométricas. La verificación automática de firmas, usando emisiones acústicas, toma datos del proceso dinámico de firmar o de escribir. La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada. El equipamiento de colección de firmas es inherentemente de bajo costo y robusto. Esencialmente, consta de un bloque de metal (o algún otro material con propiedades acústicas similares) y una computadora barata.

Guardias y escoltas especiales

Éstos pueden estar ubicados en lugares estratégicos donde exista más vulnerabilidad. Es recomendable que todos los visitantes que tengan permisos para recorrer las instalaciones en accesos restringidos sean acompañados por una persona designada como escolta.

Registro de firma de entrada y salida.

Consiste en que todas las personas que entren a las instalaciones firmen un registro que indique la hora de entrada, el motivo por el que entran, la persona a la que visitan y la hora de salida. Se recomienda un formato de registro de visitantes como en la figura 2.7.

Fecha	Nombre	Procedencia	Depto. que visita	Persona que busca	Asunto	Hora de entrada	Firma	Hora de salida	Firma

Figura 2.6. Ficha de registro de visitantes

Puertas con chapas de control electrónico.

Estos dispositivos pueden funcionar al teclearse un código para abrirla, disponer de una tarjeta con código magnético, o tener implementado algún dispositivo para el reconocimiento de alguna característica física como las que ya mencionamos.

Entradas de dobles puertas.

De esta forma, la entrada a través de la primera puerta deja un área donde la persona queda atrapada y queda completamente expuesta para ser captada por el sistema de circuito cerrado y fuera del acceso a las instalaciones. Una segunda puerta debe ser abierta para entrar a las instalaciones.

Equipos de monitoreo.

La utilización de dispositivos de circuito cerrado de televisión, tales como monitores, cámaras y sistemas de intercomunicación conectados a un panel de control manejado por guardias de seguridad. Estos dispositivos permiten controlar áreas grandes, concentrando la vigilancia principalmente en los puntos de entrada y salida.

Alarmas contra robos.

Todas las áreas deben estar protegidas contra la introducción física. Las alarmas contra robos, las armaduras y el blindaje se deben usar hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad.
La construcción de puertas y ventanas deben recibir especial atención para garantizar su seguridad.

Las consideraciones anteriores, se implementarán posteriormente por parte de la empresa JH&H, una vez se haya concluido con la etapa de implementación del cableado estructurado.

2.3. GESTIÓN DE RIESGOS[34]

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, sin tomar en cuenta la probabilidad que presente determinada circunstancia. El riesgo, en cambio, pondera la probabilidad de que ocurra.

El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable. Si el impacto y el riesgo residuales son despreciables, el proceso concluye, si no es así, se debe hacer algo.

2.3.1. La interpretación de los valores de impacto y riesgo residuales

Impacto y riesgo residual son una medida del estado actual, entre la inseguridad potencial, es decir sin salvaguarda alguna y las medidas adecuadas que reducen el impacto y el riesgo a valores despreciables. Con estos valores, se puede determinar las carencias que presenta.

[34] MAGERIT versión 3

Si el valor residual es igual al valor potencial, las salvaguardas existentes no sirven, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, significa que los procedimientos han sido cumplidos a cabalidad, pero no se debe prescindir de los cuidados aunque se puede desarrollar las actividades cotidianas con la confianza del saberse preparado.

Mientras el valor residual no sea despreciable, existe cierta exposición. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho.

Los responsables de la toma de decisiones deberán prestar especial atención a esta relación de tareas pendientes, procesarlas y plasmarlas en un informe que será de su exclusiva responsabilidad.

2.3.2. Selección de salvaguardas[35]

Las amenazas, por más pequeñas que sean, hay que conjurarlas, por principio y mientras no se justifique lo contrario.

Es necesario planificar el conjunto de salvaguardas pertinentes para contrarrestar tanto el impacto como el riesgo, reduciendo ya sea la degradación del activo, minimizando el daño, o bien reduciendo la frecuencia de la amenaza, minimizando sus oportunidades para actuar.

Toda amenaza debe ser tratada en forma profesional, de la siguiente manera:

1. Establecer políticas acerca del tema: la Organización debe implantar directrices generales de quién es responsable de cada tarea.

2. Establecer normas: la Organización debe determinar los objetivos a satisfacer para poder decir con propiedad que la amenaza ha sido conjurada.

---

[35] Manual para Certificación PANDUIT

3. Establecer procedimientos, instrucciones detalladas de lo que se debe realizar.

4. Desplegar salvaguardas técnicas que enfrenten las amenazas con capacidad para resolverlas.

5. Desplegar controles que permitan saber que todo lo anterior se encuentre funcionando según lo previsto.

A este conjunto de elementos, habitualmente se los conoce bajo el nombre de Sistema de Gestión de la Seguridad de la Información (SGSI), aunque se está gestionando y actuando en forma paulatina.

Es necesario aclarar que en la práctica no significa que se debe llevar a cabo todos y cada uno de los puntos para cada amenaza, sino desarrollar la política, normas y procedimientos junto con el despliegue de una serie de salvaguardas y controles para verificar que todas y cada una de las amenazas cuenten con una respuesta adecuada.

Al analizar los puntos anteriores, el más impreciso, es el de determinar las salvaguardas apropiadas pues resulta realmente complicado el hacerlo y requiere personal especializado aunque en la práctica las situaciones más habituales cuentan con el respaldo de información estadística que solventa el procedimiento a seguir.

2.3.3. Tipos de salvaguardas

Un sistema debe considerar las salvaguardas de tipo preventivo como prioridad, pues éstas buscan que la amenaza no ocurra o su daño sea despreciable. En la práctica, no todo es previsible, ni todo lo previsible tiene justificación económica para realizarse.

Ya sea para enfrentar lo desconocido como para protegerse de aquello a lo que se permanece expuesto, es necesario disponer de elementos que detecten el inicio de un incidente y permitan reaccionar con presteza al siniestro, impidiendo que se convierta en un desastre.

De cualquier forma, las medidas preventivas o las de emergencia admiten una cierta degradación de los activos por lo que habrá que disponer, en última instancia, de medidas de recuperación que devuelvan el valor perdido por los activos.

El instinto hace que se suela actuar de forma preventiva para que las cosas no ocurran, o no puedan causar mucho daño. No siempre es posible que esto suceda y hay que estar preparados para que acontezcan y de ninguna manera, dejar que un ataque pase inadvertido.

Cuando esto ocurra se debe detectarlo, registrarlo y reaccionar primero con un plan de emergencia, que detenga y limite el incidente y después con un Plan de Recuperación de Desastres, regresar al punto donde se debe estar.

2.3.4. Pérdidas y ganancias

Al invertir en salvaguardas, es de sentido común, no hacerlo más allá del valor de los activos a proteger. En la práctica, algunos análisis arrojan gráficos como el de la figura 23, mostrado a continuación, en el que se puede ver el costo de lo que costaría no estar protegidos y el costo de las salvaguardas.

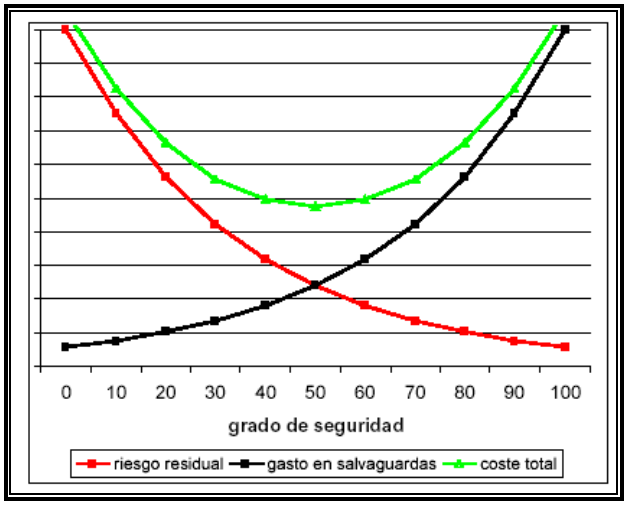


Figura 2.7. Punto de equilibrio del costo de riesgo/salvaguarda

El tipo de gráfica anterior, permite visualizar cómo al avanzar de un grado de seguridad 0 hacia un grado de seguridad del 100%, el costo de la inseguridad o riesgo disminuye, mientras que el costo de la inversión en salvaguardas aumenta. Es

visible el hecho de que el riesgo caiga fuertemente con pequeñas inversiones y que el costo de las inversiones se dispare para alcanzar niveles de seguridad cercanos al 100%.

La curva central suma el costo para la Organización, ya sea derivado del riesgo, que implica baja seguridad, o bien derivado de la inversión para alcanzar la seguridad.

Existe un punto de equilibrio entre lo que se arriesga y lo que se invierte en defensa, y si la única consideración es económica, se debe tender a este punto. Pero llevar el sentido común a la práctica no es evidente, ni por la parte del cálculo del riesgo, ni por la parte del cálculo del costo de las salvaguardas.

En la práctica, cuando hay que protegerse de un riesgo que se considera significativo, aparecen varios escenarios hipotéticos: E0, E1, E2

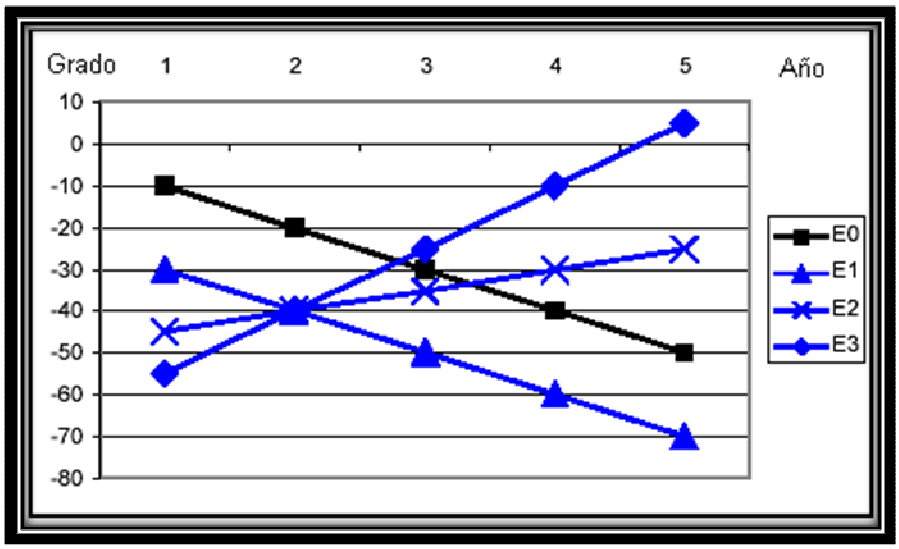


Figura 2.8. Gráfica de diferentes tipos de salvaguardas

E0: si no se hace nada
E1: si se aplica un cierto conjunto de salvaguardas
E2: si se aplica otro conjunto de salvaguardas

Y así N escenarios con diferentes combinaciones de salvaguardas.

El análisis económico tendrá como misión decidir entre estas opciones, siendo E0, no hacer nada, una opción posible que pudiera estar justificada económicamente.

En cada escenario hay que estimar a lo largo del tiempo el costo que va a suponer. Para poder agregar costos, se contabilizan como valores negativos las pérdidas de dinero y como valores positivos las entradas de dinero.
Considerando los siguientes componentes:

- (recurrente) riesgo residual
- (una vez) costo de las salvaguardas
- (recurrente) costo anual de mantenimiento de las salvaguardas
+ (recurrente) mejora en la productividad
+ (recurrente) mejoras en la capacidad de la Organización para prestar nuevos servicios, conseguir mejores condiciones de los proveedores, entrar en asociación con otras organizaciones, etc.

El escenario E0 es muy simple: todos los años se afronta un gasto marcado por el riesgo, que se acumula año tras año.

En los demás escenarios, hay cosas que suman y cosas que restan, pudiendo darse varias situaciones:

En E0 se sabe, en forma estimada lo que cada año se pierde.

El escenario E1 aparece como una mala decisión, pues supone un gasto añadido el primer año; pero este gasto no se recupera en años venideros.

El escenario E2 que, supone un mayor desembolso inicial, pero empieza a ser rentable a partir del cuarto año.

El escenario E3 representa un mayor desembolso inicial, pero se empieza a ahorrar al tercer año, e incluso se llega a obtener beneficios operativos a partir del quinto año. Se puede decir que en el escenario E3 se ha hecho una buena inversión.

2.3.5. La actitud de la Dirección

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. En otras palabras, debe aceptarse la responsabilidad de las insuficiencias.
La decisión que toma la Dirección, no es técnica, puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios.

Estos niveles de aceptación se pueden establecer por activo o por agregación de activos en un determinado departamento, en un determinado servicio, en una determinada dimensión.

Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente la Dirección.

Si el impacto o el riesgo están por encima de lo aceptable, es posible:

1. Eliminar el activo: existen activos que, simplemente, no valen la pena mantener.

2. Introducir nuevas salvaguardas o mejorar la eficacia de las presentes

Algunas salvaguardas, notablemente las de tipo técnico, se traducen en el despliegue de más equipamiento que se convierte a su vez en un activo del sistema. Estos activos soportan parte del valor del sistema y están a su vez sujetos a amenazas que pueden perjudicar a los activos de valor.

Hay pues que repetir el análisis de riesgos, ampliándolo con el nuevo despliegue de medios y, por supuesto, cerciorarse de que el riesgo del sistema ampliado es menor que el del sistema original; es decir, que las salvaguardas efectivamente disminuyen el estado de riesgo de la Organización.

CAPITULO III

3. PLAN DE RECUPERACION DE DESASTRES

Una vez realizado el Análisis de Riesgo[36], es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre, ya sea natural o técnico, considerando todas las áreas de los usuarios que procesan y transmiten información y en todos los activos detallados en el capítulo anterior.

Debido a que este trabajo depende directamente de una decisión de la Organización involucrada, y a que su interés se fijará en el procesamiento de los datos, se efectuará este plan en forma específica para el Sistema de Información del edificio Mena-Merizalde, sustentado en el sistema de cableado que se detalló en el capítulo uno del presente proyecto de titulación..

Al presentarse una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Organización.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Organizacional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

---

[36] Plan de Recuperación ante desastres informáticos BCP Generator

Actividades Previas al Desastre.

Actividades Durante el Desastre.

Actividades Después del Desastre.

3.1. ACTIVIDADES PREVIAS AL DESASTRE

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo del sistema, que aseguren un proceso de Recuperación con el menor costo posible a la Organización.

Es posible detallar las siguientes Actividades Generales:

- Establecimiento del Plan de Acción.
- Formación de Equipos Operativos.
- Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad).

3.1.1. ESTABLECIMIENTO DE PLAN DE ACCIÓN

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a los activos de las capas inferiores, en este caso se establecerá un Plan de acción dirigido a las siguientes capas:

- Entorno del Sistema
- Sistemas de Información.
- La Información. Obtención y almacenamiento de los Respaldos de Información, Backups. Políticas, Normas y Procedimientos de Backups.

3.1.1.1. Entorno del sistema

La Organización deberá mantener:

a) Inventario actualizado de los equipos de manejo de información: computadoras, switches, routers, impresoras, y demás equipos de comunicación.

b) Contenido especificado: software que usa, principales archivos que contiene.

c) Ubicación y nivel de cada dependencia de la Organización.

d) Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Organizacionales, pero haciendo la salvedad en el contrato, que en caso de siniestros, la restitución de los equipos siniestrados se podrá hacer por otros de mejores características, para realizar la actualización tecnológica, siempre y cuando esté dentro de los montos asegurados.

e) Señalización o etiquetado de los Computadores y unidades de almacenamiento, de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar color rojo a los Servidores, color amarillo a los computadores con Información importante o estratégica y color verde a aquellos de contenidos normales.

f) Tener siempre actualizada una relación de computadores, requeridas como mínimo para cada Sistema permanente de la Institución, que por sus funciones constituyen el eje central de los Servicios Informáticos de la Organización, las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

La Organización JH&H, usuaria del edificio Mena-Merizalde deberá comprometerse a cumplir con todos y cada uno de los puntos anteriores para garantizar el emprendimiento correcto de este Plan de Acción.

Para asegurar el correcto desempeño del plan de Acción, es necesario definir un manual de funciones, que establezca la participación de los usuarios del sistema y su compromiso con el desarrollo del procedimiento. Para la conformación de este manual, es necesario definir varios elementos de juicio, y son:

3.1.1.2 Sistemas de Información[37]

La Organización JH&H, deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Organizacional. La relación de Sistemas de Información deberá detallar los siguientes datos:

1. Nombre del Sistema.

2. Lenguaje o Paquete con el que fue creado el Sistema de Información. Programas que lo conforman, tanto programas fuentes como programas objetos, rutinas, macros, etc.

3. La Dirección, Departamento, Gerencia, que genera la información base del Sistema.

4. Las unidades o departamentos internos/externos que usan la información del Sistema.

5. El volumen de los archivos que procesa el Sistema.

6. El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.

7. El equipamiento necesario para un manejo óptimo del Sistema.

8. Las fechas en las que la información es necesitada con carácter de urgencia.

---

[37] Información general acerca de la recuperación ante desastres MICROSOFT

9. El nivel de importancia estratégica que tiene la información de este Sistema para la Organización, medido en horas o días que ésta puede funcionar adecuadamente, sin disponer de la información del Sistema.

10. Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para optimizar recursos).

11. Actividades a realizar para volver a contar con el Sistema de Información, es decir actividades de Restauración.

Con toda esta información se deberá de realizar una lista priorizada de los Sistemas de Información necesarios para que la Organización JH&H, pueda recuperar su operatividad perdida en el desastre.

3.1.1.3. La Información[38]

Obtención y almacenamiento de Respaldos de Información, Backups.

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Organización, para lo cual se debe contar con:

1) Backups del Sistema Operativo: en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos.

2) Backups del Software Base: Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan los Aplicativos Organizacionales.

3) Backups del Software Aplicativo: Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final. Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

---

[38] Información general acerca de la recuperación ante desastres MICROSOFT

4) Backups de los Datos: Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución.

5) Backups del sitio Web: Aplicativo y Bases de Datos, Índices, ficheros de descarga, contraseñas.

6) Backups del Hardware. Se puede implementar bajo dos modalidades:

Modalidad Externa. [39]

Mediante convenio con otra Organización que tenga equipos similares o superiores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido.

Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

Modalidad Interna.

Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados, como equipos de emergencia del otro local, debiéndose poner por escrito, al igual que en el caso anterior, todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas.

En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible

[39] Información general acerca de la recuperación ante desastres MICROSOFT

contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

Políticas, Normas y Procedimientos de Backups

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente, debiéndose incluir:

1. Periodicidad de cada Tipo de Backup.

2. Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).

3. Uso obligatorio de un formulario estándar para el registro y control de los Backups.

Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa, y los backups efectuados.

1. Almacenamiento de los Backups en condiciones óptimas, dependiendo del medio de almacenamiento empleado.

2. Reemplazo de los Backups, en forma periódica, antes que el medio de almacenamiento de soporte se pueda deteriorar.

3. Almacenamiento de los Backups en locales diferentes donde reside la información primaria, evitando de esta manera la pérdida, si el desastre alcanzó todo el edificio.

4. Pruebas periódicas de los Backups, verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

3.1.2. FORMACIÓN DE EQUIPOS OPERATIVOS[40]

[40] Consejos prácticos de seguridad en la Información INEI

En cada unidad operativa de la Organización, que almacene información y sirva para la operatividad Institucional, se deberá designar un responsable de la seguridad de la Información de su unidad. Pudiendo ser el jefe de dicha Área Operativa y sus labores serán:

1. Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.

2. Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.

3. Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.

4. Supervisar procedimientos de respaldo y restauración.

5. Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.

6. Coordinar redes, líneas, terminales, módems, otros aditamentos para comunicaciones.

7. Establecer procedimientos de seguridad en los sitios de recuperación.

8. Organizar la prueba de hardware y software.

9. Ejecutar trabajos de recuperación.

10. Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.

11. Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.

12. Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.

13. Participar en las pruebas y simulacros de desastres.

3.1.3. FORMACIÓN DE EQUIPOS DE EVALUACIÓN [41]

AUDITORIA DE CUMPLIMIENTO DE LOS PROCEDIMIENTOS SOBRE SEGURIDAD

Esta función debe ser realizada de preferencia por personal de Auditoria, de no ser posible, la realizará el personal del área de Informática y Comunicaciones, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

1. Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos, se cumpla.

2. Supervisar la realización periódica de los Backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

3. Revisar la correlación entre la relación de Sistemas de Información necesarios para la buena marcha de la Organización, y los Backups realizados.

4. Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

3.2. ACTIVIDADES DURANTE EL DESASTRE[42]

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- Plan de Emergencias.
- Formación de Equipos.
- Entrenamiento.

---

[41] Consejos prácticos de seguridad en la Información INEI

[42] MAGERIT versión 3

3.2.1 PLAN DE EMERGENCIAS

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

1. Durante el día.

2. Durante la noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

1. Vías de salida o escape.

2. Plan de Evacuación del Personal.

3. Plan de puesta a buen recaudo de los activos, incluyendo los activos de Información de la Organización, siempre y cuando las circunstancias del siniestro lo posibiliten.

4. Ubicación y señalización de los elementos contra el siniestro: extinguidores, cobertores contra agua, herramientas.

5. Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación, lista de teléfonos de Bomberos, Ambulancia, Jefatura de Seguridad y del personal de los equipos de seguridad, nombrados para estos casos.

3.2.2. FORMACIÓN DE EQUIPOS

Establecer en forma clara y con detalle cada equipo: nombres, puestos, ubicación, entre otros, con funciones claramente definidas a ejecutar durante el siniestro, es

decir, un manual de funciones de la organización, la misma que será descrita en la sección 3.3.6.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita por estar en un inicio o estar en una área cercana, deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los activos del sistema de información, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los activos señalados en el literal 3.1.1.

3.2.3. ENTRENAMIENTO

Establecer un programa de prácticas periódicas de todo el personal de JH&H en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, exposiciones de los proveedores, capacitación del manejo del sistema de información, charlas del uso correcto de los equipos de comunicación.

Un aspecto importante es que el personal de la compañía JH&H, tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, daños maliciosos, accidentes a la infraestructura) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos. Para llevar a cabo esto, es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Organizacional.

Una vez conocidos los elementos que deben tomarse en cuenta al momento de un siniestro o emergencia, es posible elaborar un Manual de funciones que facilite el desenvolvimiento de cada uno de los responsables de salvaguardar el sistema de información de la Organización JH&H.

3.3. ACTIVIDAD DESPUÉS DEL DESASTRE

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción elaborado en el punto 3.1.1

- Evaluación de Daños.
- Priorización de Actividades del Plan de Acción.
- Ejecución de Actividades.
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.

3.3.1. EVALUACIÓN DE DAÑOS

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

3.3.2. PRIORIZACIÓN DE ACTIVIDADES DEL PLAN DE ACCIÓN

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las acciones estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las diligencias afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

3.3.3. EJECUCIÓN DE ACTIVIDADES

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción (3.1.1.).

Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

3.3.4. EVALUACIÓN DE RESULTADOS

Una vez concluidas las labores de Recuperación del Sistema que fue afectado por el siniestro, se debe evaluar en forma objetiva, todas las actividades realizadas, la calidad con la que fue hecha, el tiempo utilizado, las circunstancias que aceleraron o entorpecieron las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

3.3.5. RETROALIMENTACIÓN DEL PLAN DE ACCIÓN

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento de juicio es evaluar cual hubiera sido el costo de que nuestra Organización no haya tenido el plan de contingencias que se llevó a cabo.

Una vez que se han tomado en cuenta todas las consideraciones de 3.3., se puede elaborar un manual de funciones acorde a las necesidades de la empresa JH&H y su sistema de información.

3.3.6. MANUAL DE FUNCIONES DE LA EMPRESA JH&H

El presente manual tiene por objeto definir las responsabilidades que tendrá cada departamento, área o funcionario de JH&H, así como las actividades que realizará para su ejecución.

Coordinación General del Plan

Responsable: Director Administrativo.

Actividades:

- Verificar que las actividades de todos los miembros del plan de acción sean cumplidas a cabalidad, como se exprese en este manual de funciones.
- Establecer claves de acceso, llaves de encripción y puertas para cada uno de los departamentos usuarios del sistema de información.
- Realizar un inventario de los equipos de manejo de información.
- Ingresar los equipos del inventario realizado, dentro de un seguro comercial.
- Organizar charlas, conferencias, capacitaciones dirigidas a todo el personal acerca de la importancia de aplicar el plan de acción en la seguridad de la información de la empresa.

Administración de la Información:

Responsable: Jefe Departamento Técnico

Actividades:

- Señalizar y etiquetar los computadores y unidades de almacenamiento, de acuerdo a la importancia de su contenido.

- Actualizar por lo menos una vez al año la relación de los computadores de todo el sistema, funciones que realiza y posible sustituto en caso de presentarse un siniestro.
- Mantener un registro del Sistema de Información, tal como se especifica en la sección 3.1.1.2.
- Recolectar y administrar la información del respaldo que cada dependencia genere, por semana.

Respaldos de la Información

Responsables: Gerencia General. Jefe Administrativo, Jefe de Contabilidad, Jefe de Ventas, Jefe de Marketing, Jefe de Importaciones, Jefe de Bodega.

Actividades:

- Mantener un Backup del Sistema Operativo que utilizan sus computadores.
- Mantener un Backup del software y lenguajes de programación que se usaron para desarrollar las aplicaciones de cada dependencia.
- Mantener un Backup del software aplicativo, así como todos los documentos y archivos que cada departamento haya generado. Este respaldo desde hacerse en forma diaria.

Evaluación

Responsable: Auditor Externo

Actividades:

- Revisar que las normas y procedimientos de seguridad de la información se cumplan a cabalidad como lo señala el manual de funciones.
- Supervisar la realización periódica de los respaldos de cada dependencia.
- Información de los cumplimientos e incumplimientos al Coordinador General de la compañía.
- Realizar una evaluación de daños, inmediatamente después de que se haya producido un siniestro, y conjuntamente con el Coordinador General, elaborar un informe del mismo.

- Evaluar los resultados que se obtuvieron después de haberse presentado el siniestro en cuanto al desempeño de cada uno de los responsables del plan de acción.

Generales:

Responsables: Todo el personal

Actividades:

- Vigilar la infraestructura de todo el edificio Mena-Merizalde, el personal que labora en él y los bienes que se almacenan en la empresa.
- Asistir a las capacitaciones que se realicen acerca de la seguridad de la información de la empresa.
- Después de presentarse un siniestro detallar las actividades que cada uno realizó en pos de salvaguardar el sistema de información del equipo de evaluación para la retroalimentación del plan de acción.
- Colaborar con las actividades que se describen en el manual de funciones para su total ejecución.
- Difundir las actividades expresadas en el manual de funciones para el conocimiento del mismo por parte de todo el personal que trabaja en el edificio.

CAPITULO IV

4. CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

De acuerdo con los objetivos planteados y los resultados obtenidos durante el desarrollo de los capítulos anteriores del presente proyecto de titulación, se pueden establecer las siguientes conclusiones:

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de comportamiento del personal, en relación con los recursos y servicios informáticos de la organización y que en el caso de JH&H se ve reflejado en el manual de funciones implementado.

No se puede considerar que una política de seguridad informática sea una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a la conducta de los empleados; es más bien una descripción de los activos que deseamos proteger y la razón por la que lo hacemos, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, el medio para impulsar el intercambio y desarrollo en el ámbito de sus negocios.

Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos, infraestructura y servicios informáticos.

Un elemento que merece mayor énfasis, es el sistema de cableado estructurado, pues en un sistema de información, tomar decisiones de infraestructura de cableado correctas, puede ser una excelente forma para pulir diversos aspectos como la disminución de amenazas, ya sea en la degradación de los activos o en la frecuencia con la que ocurren y esto desemboca por consecuencia en la mejora de la productividad, la seguridad, la optimización y el desempeño de toda la red.

En la actualidad, los principales problemas a los que se enfrentan la mayor parte de las empresas de la región en su infraestructura de cableado son: el limitado alcance de su diseño inicial, una instalación deficiente, un pobre desempeño, la administración de su infraestructura en forma inadecuada e incorrecta, así como la falta de políticas para los movimientos, adiciones y cambios, lo que recae en la incapacidad de soportar las tecnologías convergentes y las aplicaciones futuras.

La mejor manera de proteger esta inversión es elegir correctamente la solución con el desempeño adecuado, pues se ha logrado determinar que el producto representa un 50% del éxito total de un proyecto y el otro 50% corresponde al diseño, la instalación, el servicio y la consultoría posterior que en conjunto, le pueden proporcionar a un usuario final el mejor servicio acorde a sus necesidades, tal como se ha intentado orientado en el presente proyecto de titulación.

En ocasiones, y debido a la gran presión que ejerce la limitación en el presupuesto, existe la tentación de realizar procedimientos de instalación que no son nada recomendables y que van en contra de lo sugerido tanto por fabricantes como por organismos de estandarización y normalización, como puede ser el cortar camino, ir por trayectorias adversas al sistema, acciones que sin duda puede derivar en más de un problema al ejercicio de toda la red de información de un edificio.

Existen soluciones en el mercado, tanto de fabricantes, distribuidores e integradores, en las que su única propuesta es el precio. Es indispensable que el usuario final conozca la manera tangible que representa elegir el producto adecuado, el diseño correcto, el proceso de instalación acorde a sus requerimientos, excelencia en el servicio, la consultoría y el valor agregado, pues en conjunto suman el más alto beneficio esperado.

Al sugerir los diferentes productos necesarios para la implementación del sistema de cableado estructurado en el edificio Mena-Merizalde, se tomó en cuenta las recomendaciones mencionadas anteriormente, pues son los que más se ajustan a las necesidades propias del caso.

Cabe señalar que del costo total de una Red de Área Local, el cableado estructurado representa únicamente entre el 5% y 8% de la inversión, y dentro de estos porcentajes el tener un cableado estructurado total y correctamente administrado representa menos de un 10% del costo total de esta infraestructura, además el retorno de la inversión se puede considerar prácticamente inmediato debido a que cuando el cliente recibe la infraestructura recién instalada todo está perfectamente ordenado, los cables se encuentran muy bien etiquetados, organizados y su administración por lo tanto, se torna sumamente sencilla para cualquier usuario.

Una vez definida la importancia que tiene el cableado estructurado dentro de un sistema de información, es importante establecer políticas de seguridad que determinen que toda la infraestructura montada alrededor y la información procesada en ella, cuente con un respaldo acorde a las necesidades propias de cada usuario del sistema.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. De igual manera, deberán establecerse las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Al diagnosticar la situación actual del edificio Mena-Merizalde, se identificó la falta de políticas de seguridad para vigilar el acceso a la red y a los sistemas informáticos, en especial de su columna vertebral, que es el sistema de cableado estructurado, lo que genera aplicaciones o usos efectuados de manera indebida.

Fue evidente también la falta de capacitación a los usuarios en cuanto al manejo de la infraestructura y el uso de herramientas de seguridad en el sistema.

No existía tampoco un plan de contingencia para el caso de accidentes naturales, ni un plan de emergencia si se presentaba una caída del sistema por agotamiento de los recursos.

El trabajo de investigación realizado en este proyecto de titulación, permitió confirmar que existen condiciones técnicas, operativas y políticas que facilitan la

implementación de lineamientos que apunten hacia el logro de políticas de seguridad a los fines de alcanzar el mejor aprovechamiento del sistema.

Promocionar una cultura de Seguridad requiere de un liderazgo fuerte con una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planificación y administración de la Seguridad. Los aspectos de Seguridad deberían ser objeto de interés y responsabilidad a todos los niveles de la administración pública y empresa, así como para todos los empleados, y una manera sencilla de lograr este interés sería difundiendo el manual de funciones que se describió en la sección 3.3.6.

Evaluar y controlar permanentemente la seguridad física del edificio es la base para o comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor teniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra incidentes

Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de las áreas que recorren ciertas personas hasta el extremo de evacuar el edificio en caso de accidentes.

Aumentar las medidas para garantizar la disponibilidad de los servicios informáticos genera confianza y acerca a los usuarios a la informática.

La empresa JH&H debe asumir el Plan de Contingencias Informáticas, analizarlo y determinar su idoneidad, con el fin de ponerlo en marcha en un tiempo razonable

Es determinante entender que en un Plan de Contingencias se invierte, para un ahorro futuro y no considerarlo como un gasto del presente.

Además, adoptar el Plan de Contingencias impacta en la organización, en las funciones y en las responsabilidades.

El Plan de Contingencias en el Sistema de Información debe ser un elemento vivo, que se mantenga, pruebe y actualice periódicamente.

4.2. RECOMENDACIONES

Implementar un plan de contingencia para la Seguridad Informática, este será una herramienta imprescindible para la recuperación de información, este plan de contingencia debe contemplar tanto la seguridad física, como la seguridad lógica y estaría complementado con un plan de emergencia y con un plan de recuperación de la información.

Documentar en lo posible las políticas de seguridad a implementar y comunicar a todo el personal involucrado, en el funcionamiento del Edificio Mena-Merizalde sobre las políticas adquiridas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.

Sensibilizar a la Gerencia de la Organización JH&H, arrendataria del edificio Mena-Merizalde en torno al tema de seguridad de la información.

Fortalecer los conocimientos de todo el personal, tanto administrativo como operativo, con cursos de formación y capacitación en el área de seguridad de la información.

Definir claramente los permisos y accesos de cada funcionario de la Organización y de todos los usuarios del sistema de información de la Organización.

Las Políticas de Seguridad en el edificio Mena-Merizalde, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, rotación de funcionarios, desarrollo de nuevos servicios.

Capacitar a los usuarios en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y a la seguridad física del área de trabajo.

Crear un programa de educación y entrenamiento a los usuarios de la Organización arrendataria del edificio Mena-Merizalde que incluya: prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad, la integridad y el desempeño de las tareas de la información.

Retroalimentar los diferentes Planes diseñados para el Sistema de Información de JH&H en el Edificio Mena-Merizalde, con todos los incidentes de seguridad deben ser registrados, reportados, revisados y escalados apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas, esto significa que por lo menos cada año se deberá examinar las falencias o debilidades del plan para modificarlo o reforzar los puntos más propensos a desastres.

BIBLIOGRAFIA

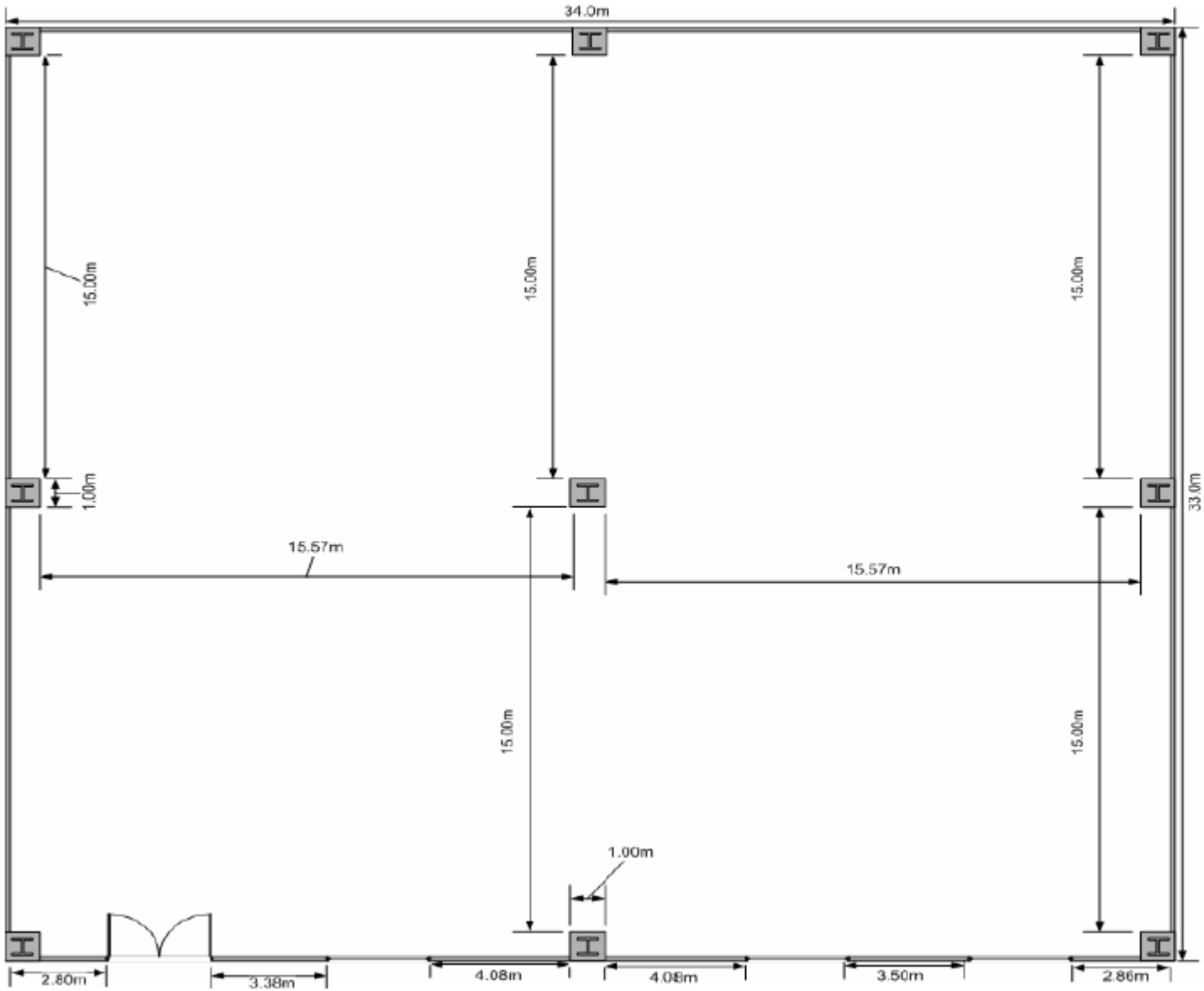
- Manual de Certificación Cableado Estructurado. PANDUIT. 2006
- Manual de Certificación Técnico Instalador. ORTRONICS. Septiembre 2008
- Manual de Certificación
- Application & Practice. IEEE-COMSOC. Noviembre 2007
- Seguridad de la Información. Plan de Contingencia INEN. Diciembre 2006
- MAGERIT versión 1
- MAGERIT versión 2
- MAGERIT versión 3
- Plan de Recuperación ante desastres informáticos BCP Generator. 2005
- Seguridad industrial en la administración informática (UPIICSA). 2006

REFERENCIAS DE INTERNET

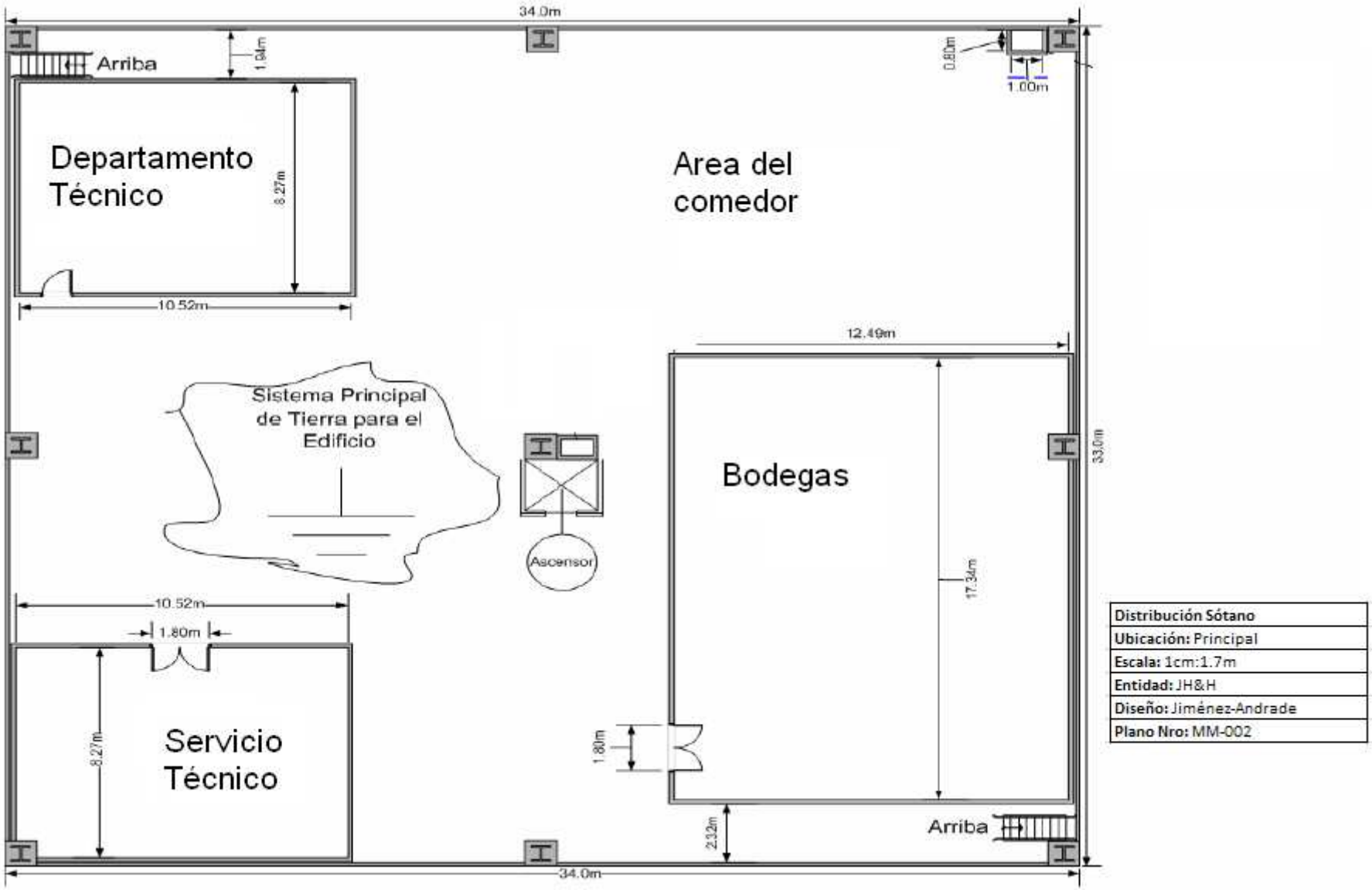
- http://www.arqhys.com/archives.pdf
- http://hermosillovirtual.com/lam/cableado.htm
- http://www.cecsa.net/frame_infocliente.html
- http://www.axioma.co.cr/strucab/scmenu.htm
- http://www.ghtcable.com/knowledge.asp?id=6
- http://www.sucre.udo.edu.ve/comp_ac/logro2.html

ANEXOS

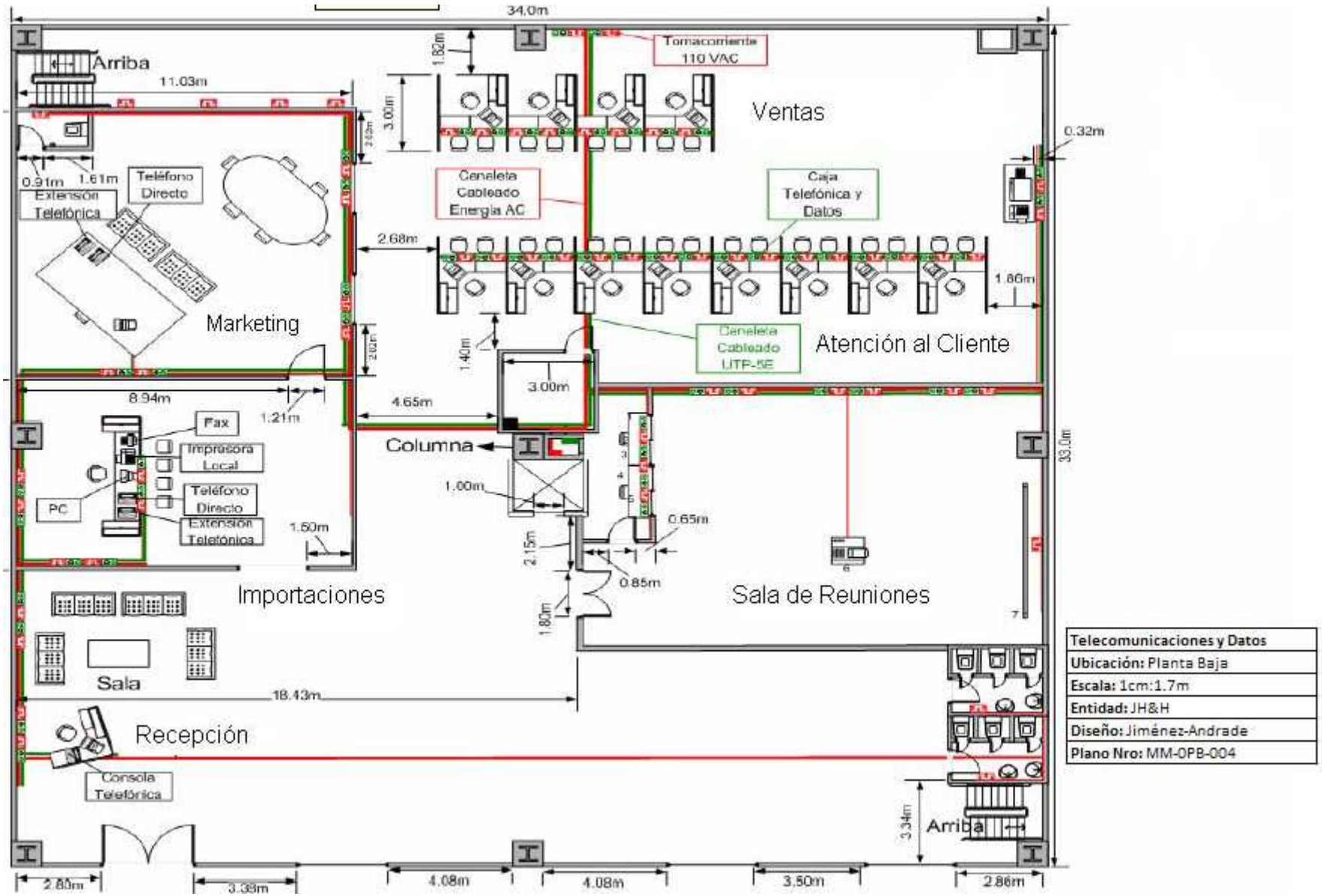
ANEXO A



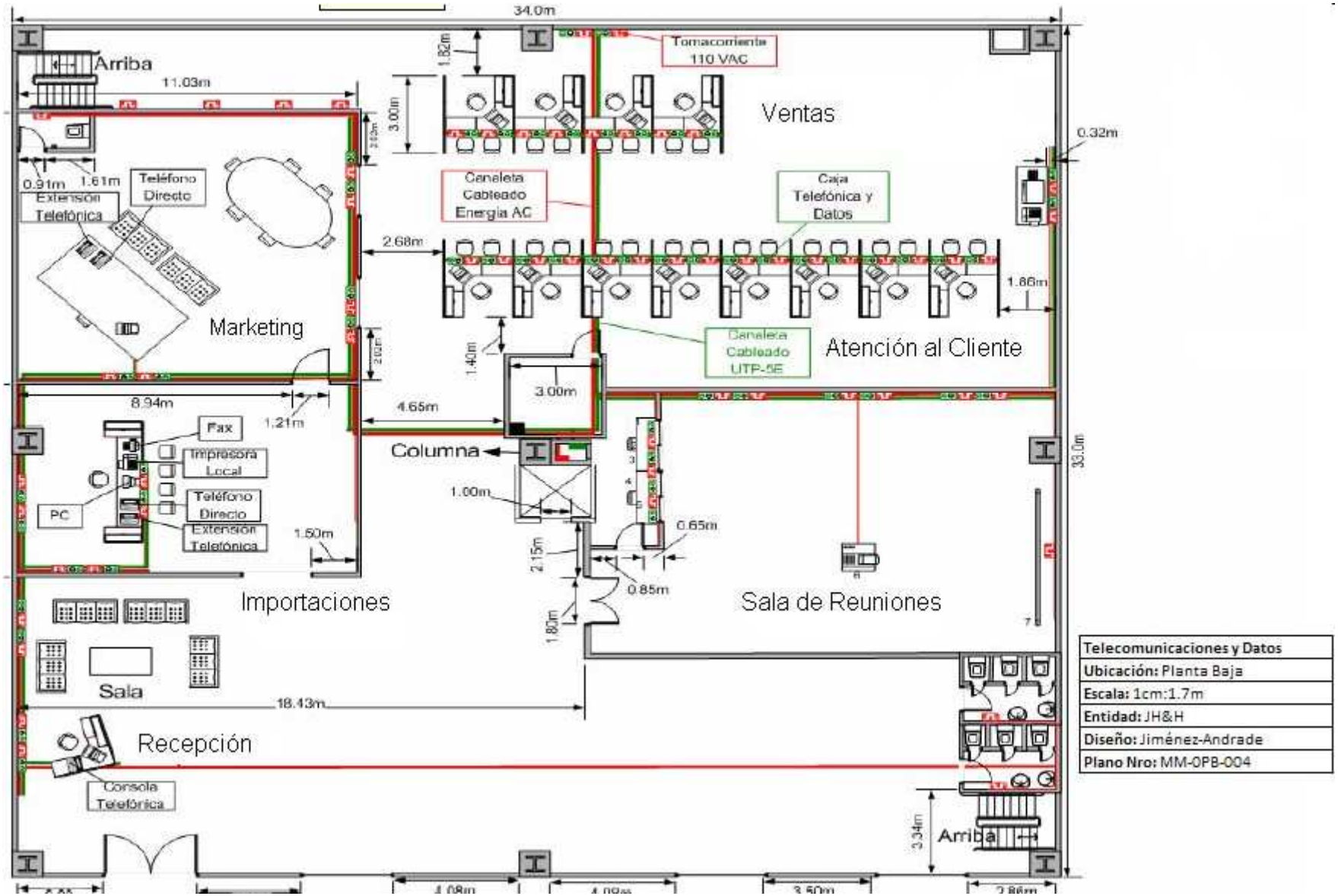
Distribución General Edificio
Ubicación: Principal
Escala: 1cm:1.7m
Entidad: JH&H
Diseño: Jiménez-Andrade
Plano Nro: MM-001



Distribución Sótano
Ubicación: Principal
Escala: 1cm:1.7m
Entidad: JH&H
Diseño: Jiménez-Andrade
Plano Nro: MM-002



Telecomunicaciones y Datos
Ubicación: Planta Baja
Escala: 1cm:1.7m
Entidad: JH&H
Diseño: Jiménez-Andrade
Plano Nro: MM-0PB-004



Telecomunicaciones y Datos
Ubicación: Planta Baja
Escala: 1cm:1.7m
Entidad: JH&H
Diseño: Jiménez-Andrade
Plano Nro: MM-0PB-004

ANEXO B

ESPECIFICACIÓNES DE DISPOSITIVOS UTILIZADOS

Los equipos tendrán componentes y dispositivos que permitan que las operaciones que se realicen sean de una manera mucho más eficiente, además contarán con el sistema operativo WINDOWS XP PROFESIONAL.

Las CPU HP EVO D 510 SFF serán utilizadas en el edificio principal y las EVO D 530 SFF serán utilizadas en las sucursales.

PCs

HP EVO D 510 SFF
Ordenador con procesador Pentium 4-540 a 3.2GHz, 512MB de memoria, 80GB de disco duro, unidad Combo, LAN y Windows XP Professional

ESPECIFICACIONES:

- Procesador: Pentium 4 Intel 540 con tecnología HT
- Velocidad del procesador: 3,20 GHz
- Caché: 1MB
- Bus del sistema: 800MHz
- Chipset: Intel 915GV Express
- Memoria: 512MB DDR2-Synch DRAM PC3200
- Ranuras de memoria: 4DIMM
- Memoria máxima: 4GB
- Disco Duro: 80GB 7200rpm
- Compartimentos para unidades externas:
- 1 externa de 5,25" y 1 externa de 3,5"
- Compartimentos para unidades internas:
- 1 interna de 3,5"
- Unidad de discos flexibles: Sin unidad de disquetes
- Controladora de disco: SMART III ATA serie de 1,5 GB/s
- Microsoft Windows XP Professional
- controlador integrado VGA, RAMDAC integrado (400 MHz)
- Memoria de la tarjeta de vídeo del subsistema de gráficos: Memoria de gráficos compartida con la memoria del sistema. El uso de la memoria de gráficos puede variar entre 8 y 128 MB, dependiendo de la cantidad de memoria del sistema que haya instalada y de la carga del sistema.

HP EVO D530 SFF P4HT-3G

40GB 512MB DVD WXPP LAN SP

ESPECIFICACIONES:

- Dimensiones (Ancho x Profundidad x Altura) 33.8 cm. x 38.3 cm. x 10 cm.
- Procesador 1 x Intel Pentium 4/ 3 GHz
- Disco duro 1 x 40 GB - estándar - ATA-100
- Conexión de redes Adaptador de red - PCI - Ethernet, Fast Ethernet, Gigabit Ethernet
- Alimentación CA 110/230 V (50/60 Hz)
- Memoria RAM 512 MB - DDR SDRAM - 400 MHz - PC3200
- Controlador de almacenamiento Serial ATA (Serial ATA-150)
- Audio salida Tarjeta de sonido - estéreo
- Tipo Ordenador personal
- Memoria caché 512 KB L2
- Almacenamiento óptico DVD-ROM
- Microsoft Windows XP Professional
- Caché por procesador 512 KB
- Controlador gráfico AGP 8x - Intel 865G
- Unidad de disquete de 3,5 de 1,44 MB

SWITCH CAPA 2 POR 48 PUERTOS

Especificaciones técnicas:

Factor de forma Externo - 1 U
Dimensiones (Ancho x Profundidad x Altura) 44 cm x 41.5 cm x 4.5 cm
Peso 5 kg
Procesador Motorola MPC8245 466 MHz
Cantidad de puertos 48 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos 1 Gbps
Protocolo de interconexión de datos Ethernet, Fast Ethernet, Gigabit Ethernet
Puertos auxiliares de red 4x10/100/1000Base-T/SFP (mini-GBIC)
Protocolo de gestión remota SNMP 1, SNMP 2, RMON 1, Telnet, HTTP
Características Control de flujo, capacidad duplex, soporte de DHCP, negociación automática, soporte VLAN, enlace ascendente automático, soporte DiffServ, apilable
Cumplimiento de normas IEEE 802.3, IEEE 802.3z, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x
Alimentación CA 110/230 V (50/60 Hz)
Cuatro ranuras de uso dual soportan SFPs que pueden conectarse a cableado de fibra para conexiones flexibles Gigabit Ethernet a backbone y servidores.
*Garantía del fabricante: limitada de por vida

SWITCH INTELIGENTE CAPA 3 POR 24 PUERTOS

24-Port 10/100/1000 Gigabit Switch with WebView Gigabit Switching with Fiber Expansion and Browser Configurability

ESPECIFICACIONES:

- WebView remote monitoring and configuration via web browser
- 64 VLANs, 8 port trunking groups, console port, 802.1p CoS support

• 24 10/100/1000 Gigabit Ethernet ports
• 2 MiniGBIC slots for Fiber and Copper Gigabit Ethernet expansion (Shared)
• Supports half duplex and full duplex modes and auto-negotiation for all 10/100/1000 Copper ports
• Auto MDI/MDI-X supports cable detection on all 10/100/1000 Copper ports
• Provides flow control mechanism to ensure zero packet loss. Uses backpressure for half-duplex operation and IEEE802.3x for full duplex operation.

• Supports 8K MAC address table entries • Supports 2Mbit packet memory
• Supports Jumbo Frames sizes up to 9KB
• Provides Store-and-Forward switching mechanism
• Provides non-blocking switching performance
• Provides Multicasting, Broadcasting and Flooding Control
• Four egress queues on all switch ports. Support for strict priority and weighted round-robin (WRR) CoS policies
• Traffic classification based on Port#, VLAN priority in VLAN tagging packet
• Supports 802.1q Tagged based VLAN for support of up to 64 VLANs
• Supports up to 8 trunking groups
• Load sharing among trunk ports based on MAC address
• Port Mirroring to monitor the traffic of Mirrored ports
• ACL to limit the interface and IP domain to manage the switch
• Web-based configuration makes installation and setup easy

Model SRW2024 - 24-Port 10/100/1000 Gigabit Switch with WebView
Standards IEEE 802.3, 802.3u, 802.3ab, 802.3x, 802.1p, 802.1q
Ports 24 10/100/1000 RJ-45 ports and 2 shared MiniGBIC slots
Cabling Type Cat5e or better
LEDs System, Link/Activity, Gigabit
Security Features ACL, 802.1x
Environmental
Dimensions 16.93" x 1.75" x 13.78"
(W x H x D) (430 mm x 44.45 mm x 350 mm)
Unit Weight 7.35 lbs. (3.33 kg)
Power Input 100-240V 0.5A
Certifications UL (UL 1950), CSA (CSA 22.2), CE, EN60950 (2001)
Operating Temp. 0ºC to 50ºC (32ºF to 122ºF)
Storage Temp. -40ºC to 70ºC (-40ºF to 158ºF)
Operating Humidity 20% to 95% Relative Humidity, Non-Condensing
Storage Humidity 5% to 90% Non-Condensing

ROUTERS

Router Cisco 2800 versión 12.3 de dos puertos seriales, 2 puertos FastEthernet, uno auxiliar y otro para consola IOS.

Cisco 2800 soporta la "Cisco Self-Defending Network" con funciones de gestión y servicios avanzados de seguridad como el acelerador de encriptación por hardware, VPN IPSec (AES, 3DES, DES), cortafuegos, prevención de intrusos (IPS), control de acceso a la red (NAC)y funciones de filtraje por URL. La intuitiva gestión basada en Web del router está preinstalada en todos los productos de la serie Cisco 2800 para ayudar a simplificar la gestión y configuración.

FIREWALL

Cajas Nokia y el software es Check_point:
Las especificaciones de estas cajas son:

FIREWALL

Gabinete Porta-FireWall

Marca	: Checkpoint Next Generation with Application Intelligent
Proveedor Software	: Checkpoint (Firewall)
Proveedor Hardware	: Nokia (Cajas en donde se montó el firewall)
Tipo de hardware	: IP – 380
Sistema Operativo	: IPSO v. 3.7.1 Built 23
Número de Interfaces	: Ocho (8)
Alta Disponibilidad	: Si
Módulos de Firewall	: Módulos de CheckPoint NG en cada una de las máquinas Nokia.
Administración	: Consola SmartCenter de administración centralizada y ubicada en la ciudad de Medellín.

GUI (Graphic Unit Interfase): Administración desde una estación de trabajo.

ANEXO C

ESTANDAR ANSI/EIA/TIA 606A

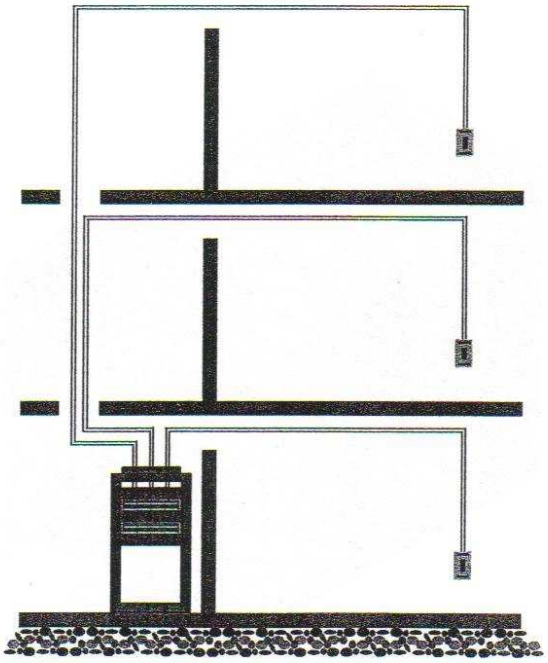
VERSIONES ANTERIORES

La versión anterior, ANSI/TIA/EIA 606, ya no está vigente. El nuevo estándar para la administración del sistema de cableado es el ANSI/TIA/EIA 606A. Algunos puntos importantes que han sido variados con respecto a la versión anterior son los siguientes:

- El estándar 606A establece 4 clases de sistemas de administración, según el tamaño y las características de la infraestructura de telecomunicaciones que será administrada.
- Permite una implementación modular de las diferentes partes del sistema de administración.
- Especifica formatos para las etiquetas.
- La definición de términos es armonizada con los demás estándares que se aplican a la infraestructura de telecomunicaciones.

SISTEMAS CLASE 1

Los sistemas clase 1 operan utilizando un único cuarto de telecomunicaciones



SISTEMAS CLASE 1

IDENTIFICADORES PARA SISTEMAS CLASE 1

Los identificadores requeridos para un sistema clase 1 son los siguientes:

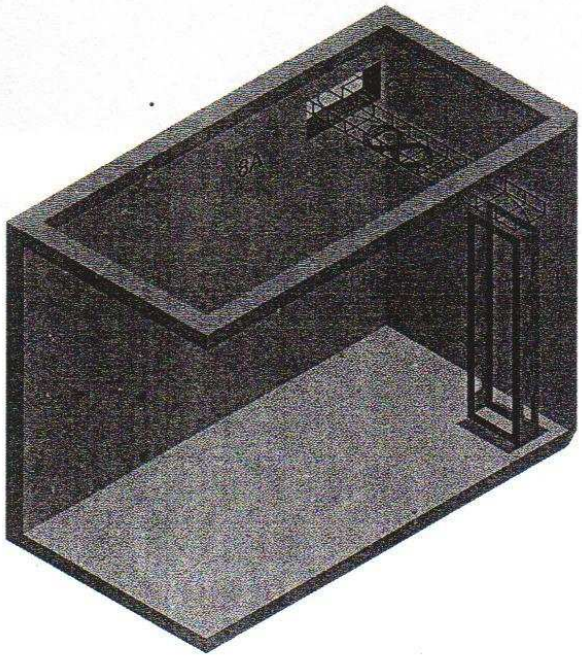
- Identificador para espacio de telecomunicaciones.
- Identificador para enlace horizontal.
- Identificador para TMGB.
- Identificador para TGB.

IDENTIFICADOR PARA ESPACIO DE TELECOMUNICACIONES

Debe asignarse un identificador único a cada espacio de telecomunicaciones en el edificio. Este identificador deberá tener el formato: fs, en donde:

- f = caracter numérico identificando el piso del edificio ocupado por el espacio de telecomunicaciones.

- s = caracter alfanumérico identificando en forma única el espacio de telecomunicaciones en el piso f, o el área del edificio en que el espacio está localizado.

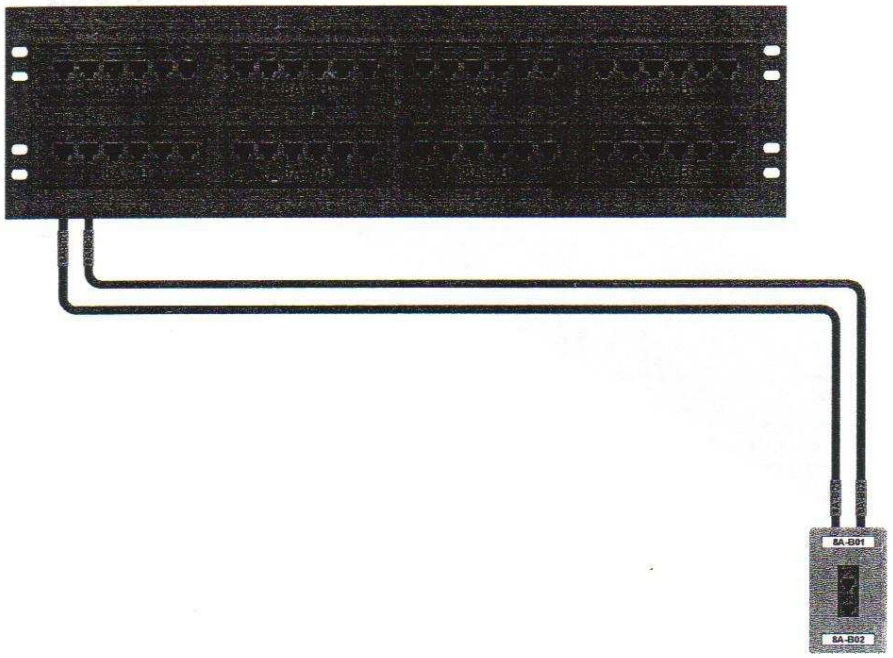


IDENTIFICADOR DE ESPACIO

IDENTIFICADOR PARA ENLACE HORIZONTAL

Debe asignarse un identificador único a cada enlace horizontal. Este identificador debe tener el formato: fs-an, en donde:

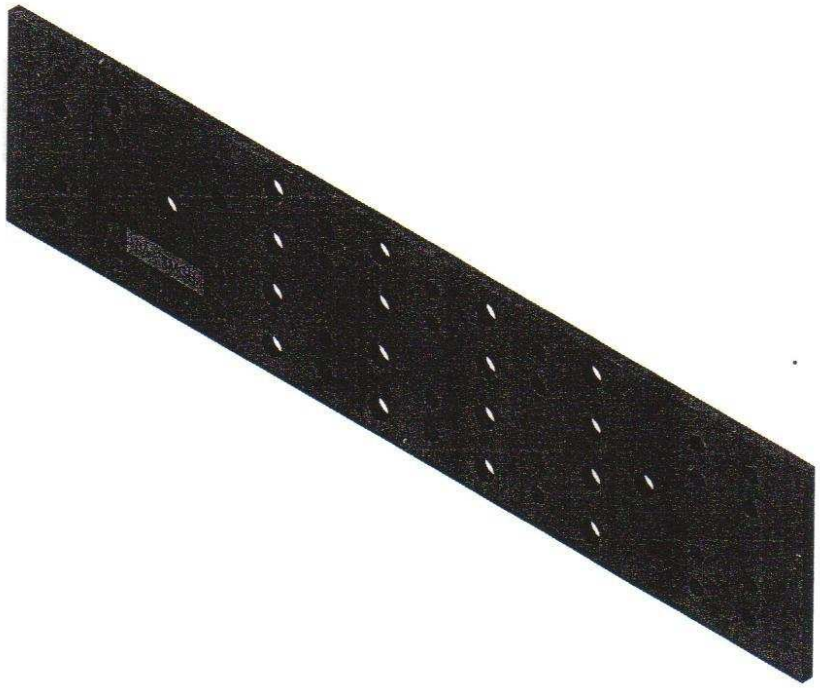
- fs = identificador del espacio de telecomunicaciones.
- a = uno o dos caracteres alfanuméricos identificando en forma única un panel de conexión, grupo de páneles de conexión con puertos numerados secuencialmente, un conector IDC, o grupo de conectores IDC, que forman parte de la conexión cruzada horizontal.
- n = dos a cuatro caracteres designando el puerto en un patch panel, o la sección de un conector IDC, en la cual está terminado un cable horizontal de 4 pares.



IDENTIFICADOR PARA TMGB

Debe asignarse un identificador único a la barra principal de puesta a tierra para telecomunicaciones. Este identificador debe tener el formato: fs-TMGB, en donde:

- fs = identificador del espacio de telecomunicaciones.
- TMGB = porción del identificador que designa la Barra Principal de Puesta a Tierra para Telecomunicaciones.



IDENTIFICADOR PARA TGB

Debe asignarse un identificador único a cada barra de puesta a tierra para telecomunicaciones. Este identificador debe tener el formato: fs-TGB, en donde:

- fs = identificador del espacio de telecomunicaciones.
- TGB = porción del identificador que designa una Barra de Puesta a Tierra para Telecomunicaciones.

IDENTIFICADOR PARA TGB

ESTANDAR J - STD 607A

VERSIONES ANTERIORES

La versión anterior, ANSI/TIA/EIA 607, ya no está vigente. El nuevo estándar para la administración del sistema de cableado es el J - STD 607A. Algunos puntos importantes que han sido variados con respecto a la versión anterior son los siguientes:

- El estándar 607A contiene una especificación más detallada para las barras de puesta a tierra
- El estándar 607A incluye un método para el cálculo del calibre de los conductores de puesta a tierra
- El término "Conductor de Unión para la Interconexión de los Sistemas Medulares de Puesta a Tierra para Telecomunicaciones / TBBIBC" ha sido sustituido por el término "Equalizador de Tierra / GE"

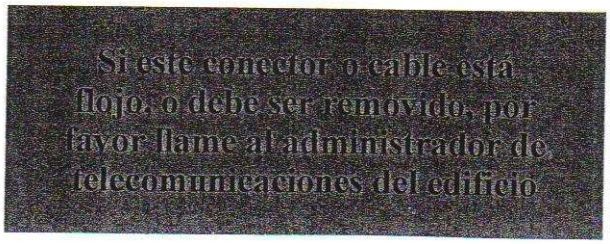
CONDUCTOR DE UNION PARA TELECOMUNICACIONES / BC

El conductor de unión para telecomunicaciones es un conductor utilizado para unir la barra principal de puesta a tierra para telecomunicaciones (TMGB) con el sistema de puesta a tierra del sistema de potencia eléctrica.

El conductor de unión para telecomunicaciones debe tener, como mínimo, el mismo calibre que el sistema medular de puesta a tierra para telecomunicaciones (TBB)

El conductor de unión para telecomunicaciones, al igual que los demás conductores de puesta a tierra, no deberían ser instalados en conduits metálicos ferrosos. De ser necesario instalar conductores de puesta a tierra en conduits metálicos ferrosos que excedan 1 metro (3 pies) de longitud, los conductores deben ser conectados al conduit en cada extremo usando un accesorio para puesta a tierra, o un conductor # 6 AWG como mínimo.

Cada Conductor de Puesta a Tierra para Telecomunicaciones debe ser etiquetado. Las etiquetas deben ser ubicadas en los conductores, tan cercanas al punto de terminación como sea práctico y en una posición de fácil lectura. Las etiquetas deberán ser no-metálicas y deberán incluir la siguiente información:



El Conductor de Unión para Telecomunicaciones, cada Sistema Medular de puesta a Tierra para Telecomunicaciones (TBB), y cada Equalizador de Tierra (GE), deben ser verdes o estar marcados con un distintivo de color verde.

BARRA PRINCIPAL DE PUESTA A TIERRA PARA TELECOMUNICACIONES / TMGB

La Barra Principal de Puesta a Tierra para Telecomunicaciones (TMGB) sirve como una extensión dedicada del sistema de electrodos de puesta a tierra del edificio, para servir a la infraestructura de telecomunicaciones. La TMGB sirve también como el punto central de conexión para los Sistemas Medulares de Puesta a Tierra para Telecomunicaciones (TBB), y equipos instalados en el mismo espacio de telecomunicaciones.

Típicamente, debería existir solamente una TMGB por edificio.

La ubicación ideal para la TMGB se encuentra en las instalaciones de entrada (EF)

Características de la TMGB:

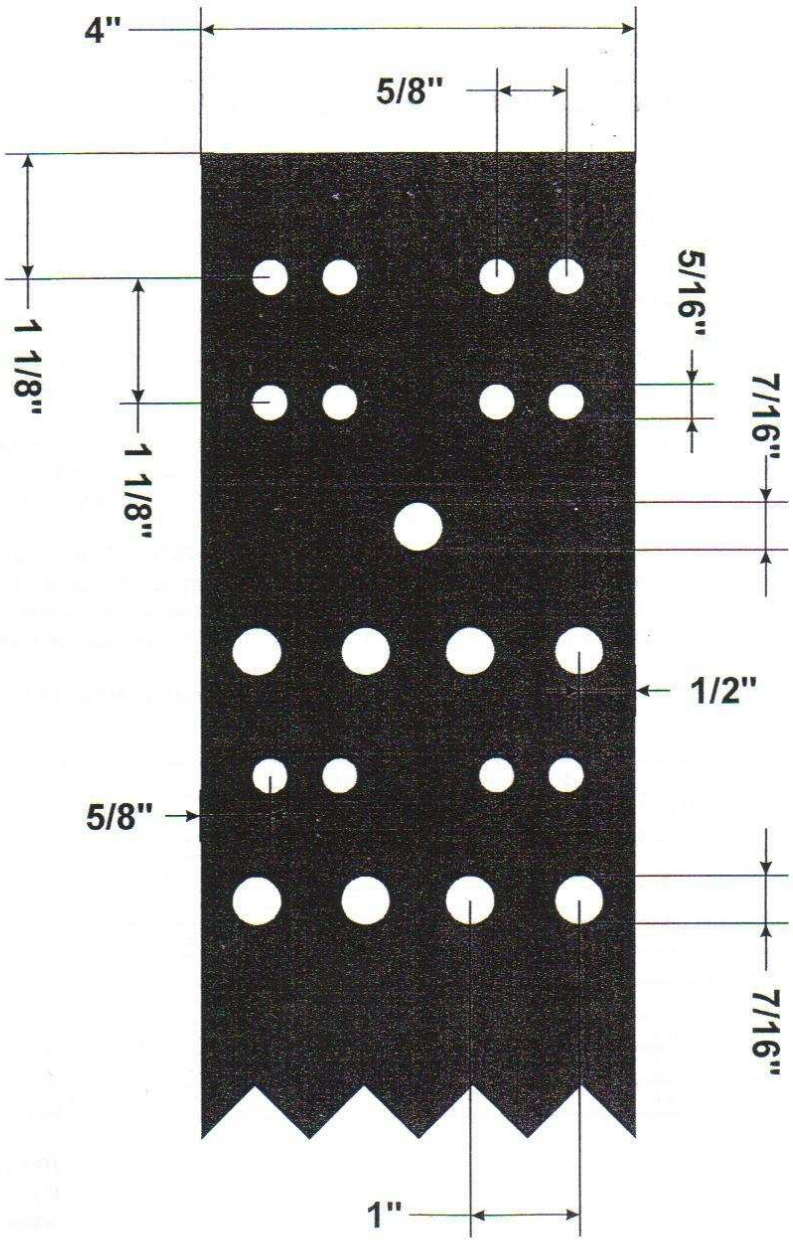
- Debe ser una barra de cobre pre-taladrada provista con orificios que permitan utilizar conectores de tamaños estandarizados;
- Debe ser dimensionada de acuerdo con los requisitos inmediatos de la aplicación y considerando crecimiento en el futuro;
- Debe tener dimensiones mínimas de 6 mm (0.25 pulgadas) de grosor, 100 mm (4 pulgadas) de ancho, y de longitud variable;
- Debe estar listada por un laboratorio de pruebas reconocido.

Es deseable que la barra de puesta a tierra sea estañada eléctricamente para una resistencia de contacto reducida. Si la barra no es estañada, debe ser limpiada antes de instalar los conductores, y debería aplicarse un antioxidante en el área de contacto para controlar la corrosión y reducir la resistencia de contacto.

Las conexiones del BC y el TBB a la TMGB, deberán utilizar soldaduras exotérmicas, conectores de compresión de doble ojo listados, u otro tipo de conector de compresión irreversible. Los conectores de doble ojo son preferidos. La puesta a tierra de equipos de telecomunicaciones y de canalizaciones, deberían utilizar el mismo tipo de conectores mencionados en el párrafo anterior

Todas las canalizaciones metálicas para cableados de telecomunicaciones localizadas en el mismo cuarto o espacio que la TMGB, deberán ser conectados a la TMGB.

La TMGB debe estar aislada de su soporte. Se recomienda una separación mínima con la pared de 50 mm (2 pulgadas) para permitir el acceso a la parte trasera de la barra.



TMGB

SISTEMA MEDULAR DE PUESTA A TIERRA PARA TELECOMUNICACIONES / TBB

El sistema medular de puesta a tierra para telecomunicaciones (TBB) es un conductor que interconecta todas las barras de puesta a tierra para telecomunicaciones (TGBs), con la barra principal de puesta a tierra para telecomunicaciones (TMGB)

La función planeada para el TBB es la de reducir o equalizar diferencias de potencial entre sistemas de telecomunicaciones. A pesar de que el TBB conducirá alguna corriente alterna bajo condiciones de falla a tierra, este conductor no está previsto para ser el único camino de retorno para una falla a tierra.

El TBB se origina en la TMGB, se extiende a lo largo del edificio usando las canalizaciones del sistema medular de telecomunicaciones, y se conecta a todas las TGBs en todos los cuartos de telecomunicaciones y todos los cuartos de equipos. El sistema interior de tuberías para agua del edificio, no debe ser usado como un TBB. El blindaje metálico de un cable, no debe ser usado como un TBB.

El TBB debe ser un conductor de cobre. El tamaño mínimo del conductor usado para el TBB debe ser #6 AWG. El TBB debe ser dimensionado a razón de 2 Kcmil por cada pie lineal de longitud del conductor hasta un máximo de #3/0 AWG. El TBB puede ser un conductor aislado.

Los conductores de los TBBs deberían ser instalados sin empalmes. En donde sean necesarios empalmes, el número de empalmes debería ser mínimo y deberían ser accesibles y localizados en espacios de telecomunicaciones. Segmentos empalmados de TBB, deben ser conectados usando soldaduras exotérmicas, conectores de compresión irreversibles, o equivalente.

La siguiente tabla ilustra las recomendaciones para el dimensionamiento del TBB.

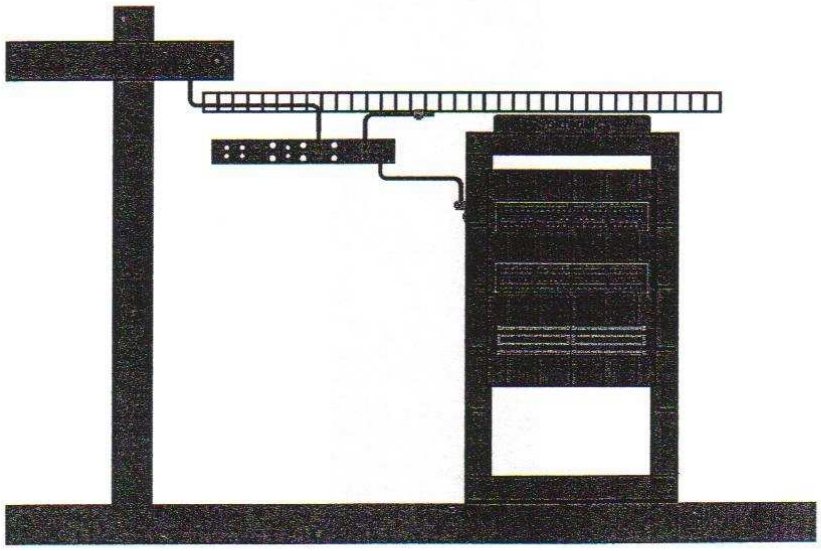
DIMENSIONAMIENTO DEL TBB	
LONGITUD DEL TBB - metros (pies) -	TAMAÑO DEL TBB AWG
Menor de 4 (13)	6
4 - 6 (14 - 20)	4
6 - 8 (21 - 26)	3
8 - 10 (27 - 33)	2
10 – 13 (34 - 41)	1
13 – 16 (42 - 52)	1/0
16 – 20 (53 - 66)	2/0
Mayor de 20 (66)	3/0

BARRA DE PUESTA A TIERRA PARA TELECOMUNICACIONES / TGB

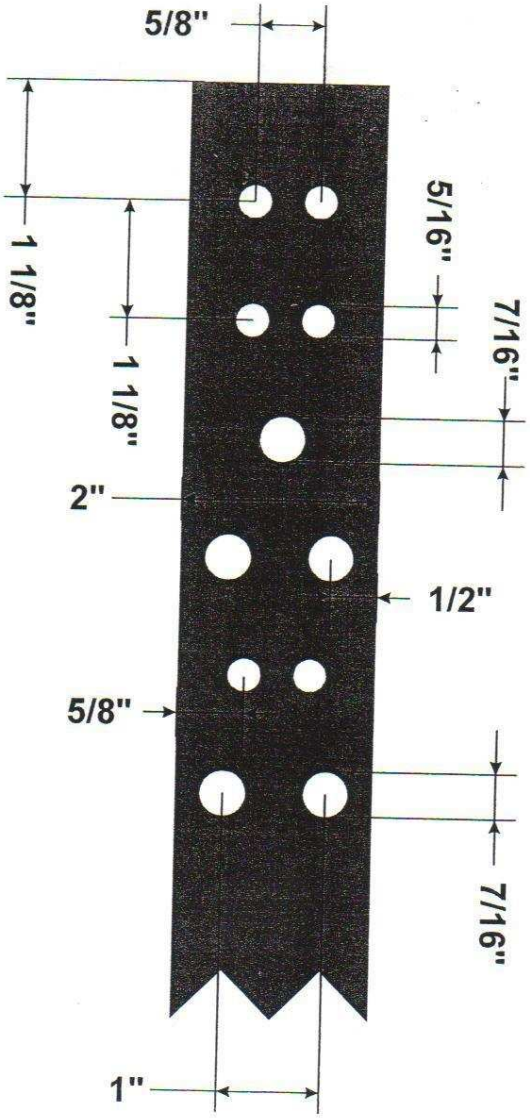
La barra de puesta a tierra para telecomunicaciones (TGB) es el punto de conexión para la puesta a tierra de los sistemas y equipos de telecomunicaciones en el área servida por el cuarto de telecomunicaciones, o cuarto de equipos, en el que está instalada.

Características de la TGB:

- Debe ser una barra de cobre pre-taladrada provista con orificios que permitan utilizar conectores de tamaños estandarizados;
- Debe tener dimensiones mínimas de 6 mm (0.25 pulgadas) de grosor, 50 mm (2 pulgadas) de ancho, y de longitud variable para cumplir con los requisitos de la aplicación, y considerando crecimiento en el futuro;
- Debe estar listada por un laboratorio de pruebas reconocido.



CONEXIONES A LA TGB



TGB