CAPITULO III

PROPUESTA DEL PLAN DE CONTINGENCIA

3.1. Introducción

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo, sistemas de información y datos contenidos en los diversos medios de almacenamiento. Con esto se pretende reducir la posibilidad de ocurrencia de riesgos y procedimientos a seguir en caso que se presente algún problema.

En el plan de contingencia se hace énfasis al aspecto físico y lógico, es donde se concentra el mayor número de inconvenientes; pero también es necesario establecer pruebas y verificaciones periódicas para que el plan de contingencia esté operativo y actualizado.

Las acciones que contemplan el plan de contingencia son:

- Antes
- Durante
- Después

De manera que permita reducir:

- Pérdidas financieras directas / indirectas
- Pérdidas de la operatividad de la U.T.C.
- Pérdidas de usuarios finales
- Costos extras para apoyo
- Costo de compensación
- Pérdidas de la infraestructura tecnológica
- Pérdidas de sistemas de información
- Información errónea o incompleta
- Bases pobres para la toma de decisiones

Entre otras, que retardan o paralizan las actividades que normalmente desarrolla la institución, provocando pérdidas económicas, retrazo en el proceso educativo por falta de infraestructura, lo que es más preocupante, la pérdida de información que es muy difícil de recuperar peor aún si son ocasionados por desastres naturales o atentados.

Es necesario enfatizar a los siguientes puntos del plan:

- Controles detectores de las bases para entender la importancia del plan.
- Obtener el consentimiento de los directivos.
- Definir los requerimientos de recuperación.

- Converger apropiadamente en la prevención de desastres.
- Integrar el plan de contingencia dentro de los planes generales de la organización.

3.2. Objetivos

- Concientizar al personal administrativo, docente y estudiantes que están sujetos a cualquier tipo de riesgos y que debemos estar preparados para actuar en forma rápida y oportuna minimizando todo tipo de desastre.
- Proporcionar una guía de contingencia flexible y adaptable a los requerimientos de la universidad.
- Establecer políticas de seguridad que abarquen el aspecto lógico y físico que permitan salvaguarda la integridad de la información e infraestructura.

3.3. Justificación

Esta es una propuesta que la universidad debe tomar en cuenta para desarrollar habilidades y medios de sobrevivir y mantener sus operaciones, en caso de que suceda un evento que afectara y ocasionara una interrupción total o parcial de las actividades informáticas, mediante esta propuesta se pudo prever y corregir dichos eventos.

Esta propuesta se inició por la identificación de los procesos críticos de la universidad, la definición de estos procesos críticos se los realizó de manera compleja mediante una matriz de impacto estratégico.

Es importante reconocer que depende de la magnitud del daño y del tiempo para estimar la recuperación de cualquier tipo de desastre; gracias al avance de la tecnología se solucionó parte de los problemas , políticas, procesos y estrategias corrigiendo situaciones críticas; se generó un ambiente de seguridad en la red de datos de la universidad tomando en cuenta que éste plan a futuro está sujeto a modificaciones según se presentaren cualquier tipo de situación.

3.4. Plan de Riesgos (Seguridad)

En esta parte se consideran todas las posibles eventualidades que puedan darse, para ello se elabora una lista de todos los riesgos conocidos por más obvio que sea, en caso de suceder algún imprevisto, actuar en forma inmediata y dar solución al problema presentado, de manera que no se paralicen las actividades de la institución.

La universidad está propensa a diversos riesgos entre ellos se encuentra el riesgo del Volcán Cotopaxi, pone en peligro la integridad de las personas y es el punto más vulnerable, seguido de los datos de información que pueda perderse; otro riesgo es la falta de seguridad que se encuentra en

los cables de electricidad y datos (UTP); entonces es en esta área donde se realizará una lista detallada del más mínimo riesgo a que está expuesta la universidad, a continuación se muestra en la siguiente Tabla.

Nº	Lista de Riesgos
1	Corto circuito
2	Asfixia por emanación de gas tóxico
3	Mala conexión en el voltaje
4	Falta de protección a los equipos más importantes
5	No son actualizados los extinguidores
6	Mala distribución de los equipos
7	Falta de equipos actualizados para mantenimiento
8	Ingreso de personal no autorizado
9	Poca actualización de personas responsables
10	Personales fijos para las actividades
11	Terremotos, temblores
12	Inundaciones
13	Erupción del Volcán Cotopaxi
14	Desborde de los ríos
15	Humedad
16	Falta de ventilación
17	Falta de protección de los diferentes cables

Tabla 3.1 Lista de Riesgos

3.4.1. Análisis de Riesgos

Los dos elementos esenciales en un análisis de riesgos consiste en identificar y cuantificar estos riesgos. La identificación depende, en gran medida, de la información disponible que tenga el Plan de Riesgos, la evaluación depende de la combinación de las matemáticas con la valoración subjetiva del analista.

El análisis de riesgos supone más el hecho de calcular la posibilidad de que ocurran cosas negativas. Habrá ciertos puntos

donde es necesario la aplicación de probabilidades que permitan dar una idea más clara del riesgo y las soluciones que permita corregirlo.

La evaluación de riesgos y presentación de respuestas se prepara de acuerdo al listado de los riesgos y las alternativas de solución que permitan minimizarlos.

Hay que tener muy en cuenta que, al realizar el análisis de riesgos, es importante identificar todos los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de quebrantarse.

Los recursos a considerar al estimar las amenazas de la seguridad son:

Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges, switchs.

Software: Programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos: Durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

Usuarios: Personas para operar los sistemas.

Infraestructura: La infraestructura se refiere al edificio en sí, a los mobiliarios que se encuentran instalados, sin pasar por alto la documentación, seguridades que se contrata de empresas privadas, etc.

Estudios realizados demuestran que el **80%** de los problemas proceden de los llamados "clientes internos" de la organización (los empleados o elementos que se desempeñan en la organización), y sólo el **20%** restante (diagrama de Pareto), proviene de elementos externos a la organización. Es necesario que la universidad mantenga una política hacia la distribución de actividades del personal involucrado en esta área, de esta manera minimizar la vulnerabilidad que existe internamente en la institución.

En la sección 3.4 se establece el tipo de riesgo y la caracterización del factor de riesgo de los posibles inconvenientes que pueden presentarse; terminando con el desarrollo de la matriz de riesgo.

3.4.2. Análisis de Fallas en la Seguridad

Este análisis contempla tanto en el aspecto físico como lógico que es donde las fallas de seguridad son muy notorias y comunes; de ahí la importancia de realizar una bitácora donde se vaya almacenando y enriqueciendo con los problemas actuales y los futuros con sus respectivas soluciones que permitan eliminar o minimizar estas fallas de seguridad; la bitácora abarca los componentes o elementos que se encuentra actualmente funcionando en la universidad, es responsabilidad de el/los encargado(s) de seguir registrando los nuevos componentes que adquieran, y dar sus posibles riesgos y soluciones, encontrándose en actualización.

Esto conlleva al desarrollo de políticas bien establecidas que permita brindar información completa y detallada de la seguridad de equipos y de sistemas de información.

3.5. Plan de Recuperación de Desastres

Una vez conocidos los riesgos y sus características que pueden envolver a la universidad, es importante y necesario definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre

para poder actuar en forma inmediata, oportuna y suplir este inconveniente.

Además, cuando se presente un desastre, es fundamental el detalle del motivo que lo originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido, para una próxima falla, afectará menos y se sabrá a que enfrentar y la contingencia será inmediata.

Los procedimientos que se desarrollen, para actuar frente a cualquier eventualidad deben ser planeados y probados debidamente en base a los riesgos que fueron enlistados en la Tabla 3.1. A más se requiere verificar para establecer el cumplimiento de dichos procedimientos, que debe ser común para todo el personal que labora en la institución.

3.5.1. Actividades Previas al Desastre

Obviamente debe existir una planificación de actividades previas al desastre de manera que permita actuar frente a dichas eventualidades y permitir recuperarse en el menor tiempo posible y a un costo mínimo.

Algunos desastres son impredecibles (erupción del volcán, terremotos, etc), para mitigar estos riegos es necesario realizar simulacros con las personas involucradas.

Pero antes de tener las actividades previas a un desastre es mejor fomentar una cultura preventiva y de mantenimiento de todos los procesos que normalmente se realizan, para que sólo en casos extremos aplicar dichas actividades para evitar los riesgos.

Estas actividades contemplan un plan de acción que permitan hacer frente a las eventualidades o riesgos que se presentan en la institución en el diario vivir y para ello se considera dos puntos importantes estos son:

- Sistemas de información y datos
- Equipos de cómputo

Naturalmente existen otros recursos que no pueden pasar por alto, pero estos son los que tienen más incidencia y más inmunes son los riesgos informáticos, mereciendo un poco más de nuestra atención, por ejemplo el cuidado de las licencias.

3.5.1.1. Sistemas de Información y Datos

En este caso los datos que se lleva en la universidad son valiosos. Es importante priorizar los sistemas de información, con el objeto de tener un inventario de lo que realmente existe en él, es necesario salvaguardar los manuales y CDs de instalación de todos los sistemas. Si sucede algún tipo de eventualidad, priorizar (ranking), los sistemas de información de manera que permita volver operativamente a la institución con los elementos mencionados anteriormente.

Pero hay que acotar que es necesario respaldar los datos que permiten que los sistemas de información vuelvan a operar normalmente. De ahí la importancia de sacar los respectivos respaldos de dichos sistemas. Pero lamentablemente de acuerdo a las entrevistas y visitas efectuadas a dichas dependencias no se realiza este proceso de respaldo, es un punto negativo, que al suceder algún riesgo el plan de acción no tendría sentido, por no existir la parte medular que son los datos que permitan complementar la contingencia.

3.5.1.2. Equipos de Cómputo

El equipo de cómputo prácticamente comprende, lo que se conoce como centro de procesos de datos o conocido comúnmente como centro de cómputo, que es el conjunto de recursos físicos, lógicos y humanos necesarios para la universidad, realización y control de las actividades informáticas de una institución.

Entre sus actividades operativas se puede señalar:

1. Operar el sistema de computación central y mantener disponible para los usuarios. En este caso no posee sistemas de información como indicamos anteriormente, pero posee otros tipos de servicios entre uno de los principales el acceso a Internet.

2. Revisar los resultados de los procesos e incorporar acciones correctivas. Lastimosamente no se ha puesto ningún tipo de interés en realizar manuales de instrucciones o de procedimientos que permitan encaminar a la consecución de resultados.

3 Garantizar la integridad de la información. Como no se maneja ningún tipo de sistema de información y al no tener una base de datos, la integridad de información se mantiene intacta.

4 Garantizar la conectividad y funcionamiento continuo del hardware y software. Para ello es necesario llevar un registro de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados, pero no se cumple con esta fase, por tal razón es conveniente establecer una matriz con los problemas más comunes y las alternativas de solución, se observa en el (ANEXO VI).

5 Administrar los enlaces de conexión satelital con la empresa proveedora IMPSAT.

6 Configuración, manejo y monitoreo de puntos de red.

7 Administración de claves y usuarios a nivel de administrador.

8 Realizar labores de mantenimiento preventivo, correctivo y limpieza de los equipos (servidores) del

cuarto de telecomunicaciones o laboratorios, con el objeto de mantener operativo los equipos de cómputo.

9 Actualización del software, quizá una de las tareas más tediosas por el número de máquinas existentes, porque esta actividad se realiza por cada máquina, por ello se recomienda explotar todas las ventajas que el servidor ofrece y no solo tomarle para el acceso a Internet.

10 Parte importante que permite resolver en forma rápida los inconvenientes o eventualidades es el etiquetado de las computadoras, servidores, cableado de voz, datos de igual forma el etiquetado de los diferentes dispositivos del rack, sistemas de seguridad (extinguidores, sistemas de detección de humo entre otros). Este etiquetado puede darse de acuerdo a la importancia de su contenido o tipo de objeto, para ser priorizados en caso de evacuación.

11 Un inventario actualizado de los equipos de manejo de información (computadoras, impresoras, y otros tipos de periféricos), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

3.5.2. Actividades Durante el Desastre

Esta etapa es muy importante porque es el momento mismo de ocurrencia de una contingencia o siniestro, es donde debe primar la calma y la inteligencia de saber como actuar frente a estas adversidades debido a que es la fase donde la toma de decisiones es fundamental para aplicar en forma eficiente el plan de emergencias. Cabe recalcar que es esencial que esté una segunda persona informado del plan de contingencia, si fuera el caso de faltar el encargado, esta preparado el segundo para tomar las acciones pertinentes.

3.5.2.1. Plan de Emergencias

El plan de emergencias establece las acciones a realizar cuando se presente un siniestro, así como la difusión de las mismas.

Para ello es necesario prever los posibles escenarios de acción en las que puede ocurrir un siniestro, puede darse en cualquier día a cualquier hora.

Es importante señalar que el plan requiere de la colaboración y participación de todos, se detalla las actividades que cada una de las personas debe realizar al momento de suscitarse un siniestro. A continuación se detallan algunos factores importantes a considerar:

- Es importante señalizar las vías de salida o escape.
- Establecer un plan de evacuación del personal. Es muy importante este plan, especialmente por los fenómenos naturales o accidentes que se esta expuesto y son difíciles de prever, es necesario estar preparados, por ejemplo el caso de la reactivación del volcán Cotopaxi, estar preparados al momento que se presente este fenómeno. Al establecer un plan es importante rodearse de las personas e instituciones con experiencia en planes de evacuación.
- Considerar un plan de resguardo de activos tanto de tipo material como de información, fundamental al momento de ejecutar el plan de recuperación de desastre (claro esta si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos que permitan minimizar el siniestro (extinguidores, alarmas, mangueras de agua y espuma entre otros elementos).

- Indispensable tener a la mano la lista de teléfonos de primeros auxilios, de bomberos, ambulancia, policía, cruz roja, una llamada oportuna permitirá evitar menos pérdidas humanas y materiales.

3.5.3. Actividades Después del Desastre

Las actividades después del desastre, son acciones que se realizan luego de ocurrido el desastre y comprende de evaluación de daños, resultados, ejecución de actividades, y retroalimentación. A continuación se describen cada uno de esos ítems.

3.5.3.1. Evaluación de Daños

Esta evaluación es fundamental, permite determinar la magnitud del siniestro. Donde se evalúa el daño a los distintos objetos como:

- Sistemas de información.
- Equipos de cómputo de las dependencias.
- Centro cómputo y su equipo de telecomunicaciones.
- Información de respaldo, tanto del medio magnético como la documental.
- Cableado eléctrico, voz y datos.
- Infraestructura y demás instalaciones de la institución.

Una vez estimados los daños de cada equipo, materiales que hayan sido afectos por el desastre en la universidad. Esta información permite determinar que elementos no están operativos y la gravedad de los daños, se puede establecer que objetos pueden recuperarse y el tiempo que se tardara.

3.5.3.2. Ejecución de Actividades

La ejecución de actividades contempla la realización de las actividades previamente establecidas en el plan. Durante su ejecución pueden surgir inconvenientes o problemas nuevos que retarden la operatividad de la institución por eso se debe priorizar, dar solución a dichos inconvenientes y posteriormente retroalimentar el plan.

Los trabajos de recuperación empezarán con la restauración del servicio usando los recursos de la institución o local de respaldo, tiene que ser suficientemente rápida y eficiente para no perjudicar el servicio, operatividad e imagen institucional.

3.5.3.3. Evaluación de Resultados

La evaluación de resultados permite medir objetivamente la eficiencia, eficacia y efectividad del proceso de recuperación de desastres y mantener operativa la Institución.

Es necesario elaborar una matriz de problemas presentados y de las alternativas de solución que se dieron a los mismos, de manera que permita evaluar que las soluciones adoptadas no incidieron en los procesos normales de las actividades.

De la evaluación de resultados y del siniestro en sí, salen dos tipos de recomendaciones: retroalimentación del plan de contingencia y una lista de recomendaciones para minimizar los riesgos y pérdidas que ocasionaron el siniestro.

Anteriormente se realizó una evaluación del plan y de las actividades que la conforman, pero no un análisis del costo de no tener un plan de contingencia para ponerlo en marcha y de lo perjudicial que sería para la institución. He ahí uno de los objetivos principales que se propone con el desarrollo del presente trabajo de investigación, establecer las bases para prever, prevenir y saber que hacer en el momento que suceda una eventualidad.

3.5.3.4. Retroalimentación del Plan

Con la información proporcionada en la evaluación de resultados, el plan necesariamente debe ser flexible y fácil de adaptarse a los cambios, que permita optimizar y mejorar las actividades que tuvieron algún tipo de dificultad.

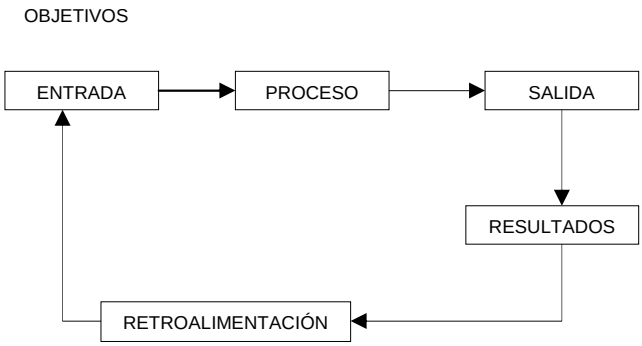


Figura 3.1 Proceso de Retroalimentación

Aspectos importantes a considerar para el cumplimiento del plan:

- Actual
- Entendible
- Factible de realizar
- Ocumentado
- Ser flexible y adaptable a los cambios
- ntener un proceso de mantenimiento

- fatizar la continuidad de la universidad.

3.6. Políticas de Seguridad

Las políticas de seguridad establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la institución.

Cada política de seguridad es consciente y vigilante del personal por el uso y limitaciones de los recursos, servicios informáticos críticos de la institución.

En este caso el Director de Servicios Informáticos es el principal involucrado para establecer medidas, es conveniente que al establecer dichas políticas, sean planteadas ante un grupo de personal capacitados involucrados en el área para que sean discutidas y dar a conocer la necesidad de implantar este tipo de medidas. Las políticas de seguridad a considerarse consta de los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual se aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información que tienen acceso.

Las políticas de seguridad debe ofrecer explicaciones comprensibles acerca del porqué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios, es indispensable mantener el recurso existente de la institución operativo salvo cualquier amenaza o riesgo que pueda ocurrir en la institución. Se considera que las políticas de seguridad son procesos dinámicos, de tal manera que este actuando permanentemente, evitando la desactualización, que cuando se descubran debilidades se pueda subsanar.

3.6.1. Lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se

permita acceder a ellos, las personas autorizadas. Existe un viejo dicho en la seguridad informática que dice "todo lo que no está permitido debe estar prohibido", esto debe propender la seguridad lógica, mediante el uso de herramientas de seguridad.

Existen diversas causas que provocan la inseguridad lógica causando grandes daños a los equipos informáticos y por ende a la información. Lo que repercute notablemente en el desempeño de las actividades en la institución.

Entre las principales causas se señalan:

- La deficiencia en los equipos de soporte.
- La “inteligencia” social.
- El espionaje industrial e institucional.
- La deficiente administración de una red.
- Los virus.
- Fallos en la seguridad de programas.
- Los vándalos informáticos (hacker, cracker).

Quizá esto se deba a la no conceptualización de la institución como una organización de trascendencia nacional, simplemente se cumplen actividades establecidas y no se encamina en la búsqueda

del kaizen (mejoramiento continuo que toda organización debe promulgar).

Debido a las causas señaladas anteriormente se generan huecos de seguridad:

- Física.
- En el software.
    - No confiar en los scripts y/o programas de instalación.
    - Por falta de experiencia.
    - Filosofía de seguridad y forma de mantenerla.

Estos aspectos son notorios debido, que en la institución no existen políticas de seguridad referente a los sistemas de comunicación peor aún para los sistemas de información y la institución no cuenta con ellos dando poca importancia a este tema. Por tanto la universidad debe establecer políticas de seguridad.

Los huecos proporcionan que tanto el equipo de cómputo, sistemas de información y datos sean vulnerables a la intromisión de intrusos y ataques, que normalmente se dan por:

- Intrusiones al Sistema
    - Física

- Por sistema
- Remota

- Técnicas utilizadas

  -Barrido de puertos

  -Escaneo del medio

  -Bugs

  -Backdoors

  - Modificar y controlar el sistema.
  - Explotar un fallo para obtener privilegios.
  - Copia del archivo de password para desencriptarlos.
  - Instalación de sniffers y/o caballos de Troya

3.6.1.1. Políticas de Direccionamiento IP

- Longitud de 32 bits.
- Identifica a las redes y los nodos conectados a ellas.
- Especifica la conexión entre redes.
- Se representan mediante cuatro octetos, escritos en formato decimal, separados por puntos.

Para que en una red de dos computadoras pueda comunicarse entre sí, deben estar identificadas con precisión Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico)

dependiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección Internet o dirección IP, cuya longitud es de 32 bytes. La dirección IP identifica tanto a la red que pertenece una computadora como a ella misma dentro de dicha red.

Clases de Direcciones IP

Clases	Número de Redes	Número de Nodos	Rango de Direcciones IP
A	126	16,777,214	1.0.0.0 a la 126.0.0.0
B	16,384	65,534	128.0.0.0 a la 191.255.0.0
C	2,097,152	254	192.0.0.0 a la 223.255.255.0

Tabla 3.2 Clase de Direccionamiento IP

Existen 5 clases de direccionamiento IP.

Clase A: Sirven para direccionar a hosts que están en subredes muy grandes.

Clase B, C: Subredes

Clase D: Se utilizan como direcciones *multicast*, es decir, para comunicaciones punto a multipunto.

Clase E: Reservada para utilización futura.

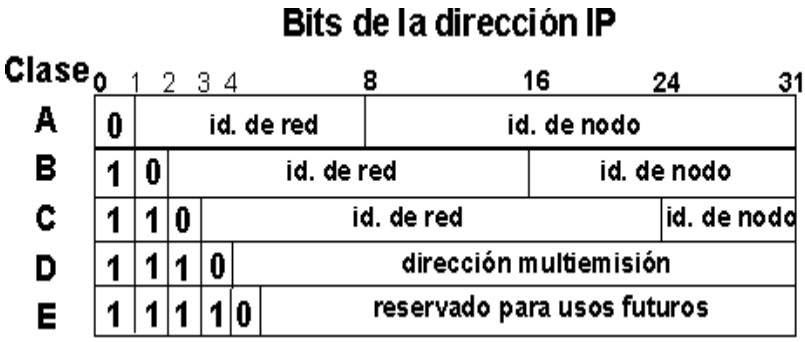


Tabla 3.3 Bit de Direccionamiento IP

Tomando tal cual está definida una dirección IP podría surgir la duda de cómo identificar qué parte de la dirección identifica a la red y qué parte al nodo en dicha red. Lo anterior se resuelve mediante la definición de las "Clases de Direcciones IP". Para clarificar lo anterior, una red con dirección clase A queda precisamente definida con el primer octeto de la dirección, la clase B con los dos primeros y la C con los tres primeros octetos. Los octetos restantes definen los nodos en la red especificada.

3.6.1.1.1. Direccionamiento IP

La **Figura** siguiente muestra el formato de las direcciones tipo A, B, C, D y E Las direcciones que contienen solo 0 ó solo 1 poseen significados especiales, en el primer caso significa “esta red o este host”, y en el segundo caso el valor de 1 es usado como

dirección de broadcast, que significa todos los host en la red indicada.

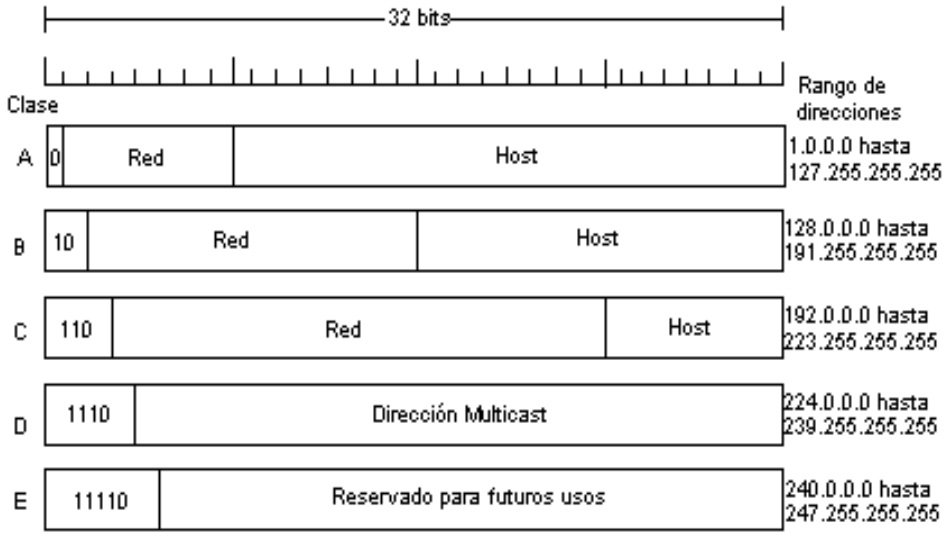


Figura 3.2 Formato de Direcciones IP

A partir de ahora el enfoque a tres tópicos fundamentales cuando se habla de IP: Subredes, Superredes y Fragmentación.

Subred

- Las Subredes son redes físicas distintas que comparten una misma dirección IP.
- Deben identificarse una de otra usando una máscara de subred.
- La máscara de subred es de cuatro bytes y para obtener el número de subred se realiza una

operación AND lógica entre ella y la dirección IP de algún equipo.

- La máscara de subred deberá ser la misma para todos los equipos de la red IP.

Las direcciones IP puede también ser divididas en unidades más pequeñas, llamadas *subredes*. Las subredes proveen una mayor flexibilidad para los administradores de red. Por ejemplo, si a una red le ha sido asignada una dirección clase B, pero dicha red sólo posee 256 nodos entonces el porcentaje neto de utilización de esa red es de 0.39% (256/65535). Con máscaras de subred se puede definir una partición variable de direcciones que permita optimizar la utilización de las direcciones IP.

El direccionamiento IP de la U.T.C., esta configurado el IP para una clase A y utiliza una submascara de clase C, no se respetan los estándares de direccionamiento. En la Tabla 3.4 se muestra como esta configurado el IP de la Universidad.

DIRECCIONAMIENTO IP ACADÉMICA (INTERNET)

Grupo	Nombre Pc	IP	Mascara de Entrada	Area
LAB2	Compaq10	10.10.1.10	255.255.255.0	Laboratorio dos
LAB2	Compaq11	10.10.1.11	255.255.255.0	Laboratorio dos
LAB2	Compaq12	10.10.1.12	255.255.255.0	Laboratorio dos
LAB2	Compaq21	10.10.1.21	255.255.255.0	Laboratorio dos
LAB1	Compaq22	10.10.1.22	255.255.255.0	Laboratorio uno
LAB1	Compaq33	10.10.1.33	255.255.255.0	Laboratorio uno
Administrativo	RelacPublic	10.10.1.80	255.255.255.0	Laboratorio uno
Administrativo	DirecSistem	10.10.1.81	255.255.255.0	Laboratorio uno
Administrativo	Rectorado	10.10.1.82	255.255.255.0	Laboratorio uno
LAB3	PC_56	10.10.1.56	255.255.255.0	Laboratorio tres
LAB3	PC_69	10.10.1.69	255.255.255.0	Laboratorio tres
Administrativo	DirecAdministra	10.10.1.83	255.255.255.0	Laboratorio tres
Administrativo	DirecSistem	10.10.1.84	255.255.255.0	Laboratorio tres
Administrativo	Rectorado	10.10.1.85	255.255.255.0	Laboratorio tres
Internet	Biblioteca	10.10.1.100	255.255.255.0	Biblioteca
Internet	Internet101	10.10.1.101	255.255.255.0	Biblioteca
Internet	Internet102	10.10.1.102	255.255.255.0	Biblioteca
Internet	Internet103	10.10.1.103	255.255.255.0	Biblioteca
Internet	Internet104	10.10.1.104	255.255.255.0	Biblioteca

Servidores	IBM Server	10.10.1.1	255.255.255.0	centro cómputo	interno
		172.30.16.35	255.255.255.240	centro cómputo	externo
Servidores	Compaq Server	10.10.1.2	255.255.255.0	centro cómputo	
	Router - DIU	172.30.16.33		centro cómputo	
	DierecPc	172.30.16.34		centro cómputo	

Tabla 3.4 Direccionamiento IP de la U.T.C.

En la Tabla 3.4 se muestra la configuración correcta de los IP de la universidad clase C con una máscara clase C y sus respectivas subredes. Se eligió la clase C porque ofrece más redes y menos nodos (estaciones de trabajo), además se puede comprobar realizando una operación AND, como se muestra a continuación:

IP: 10.10.1.10

Mascara: 255.255.255.0

	00001010. 00001010.00000001. 00001010
AND	11111111. 11111111.11111111. 00000000
	00001010. 00001010.00000001. 00000000.

Resultado de la operación IP: 10.10.1.0

IP: 192.10.1.10

Mascara: 255.255.255.0

	11000000. 00001010.00000001. 00001010
AND	11111111. 11111111.11111111. 00000000
	11000000. 00001010.00000001. 00000000.

Resultado de la operación IP: 192.10.1.0

El 192 es un número IP de inicio de clase C, entonces la mascara también es de la clase C, se cumple con las normas de seguridad, y permite implementar subredes; en cambio la Clase A tiene menos redes y más nodos el cual no aventaja a la universidad para implementar subredes que es más fácil de monitorear subredes que nodos individualizados., por tal razón se ha optado en utilizar un IP clase C, permite establecer mayor número de subredes.

DIRECCIONAMIENTO IP ACADÉMICA (INTERNET)

Grupo	Nombre Pc	IP	Mascara de Entrada	Area
LAB2	Compaq10	192.10.1.10	255.255.255.0	Laboratorio dos
LAB2	Compaq11	192.10.1.11	255.255.255.0	Laboratorio dos
LAB2	Compaq12	192.10.1.12	255.255.255.0	Laboratorio dos
LAB2	Compaq21	192.10.1.21	255.255.255.0	Laboratorio dos
LAB1	Compaq22	192.10.1.22	255.255.255.0	Laboratorio uno
LAB1	Compaq33	192.10.1.33	255.255.255.0	Laboratorio uno
Administrativo	RelacPublic	192.10.1.80	255.255.255.0	Laboratorio uno
Administrativo	DirecSistem	192.10.1.81	255.255.255.0	Laboratorio uno
Administrativo	Rectorado	192.10.1.82	255.255.255.0	Laboratorio uno
LAB3	PC_56	192.10.1.56	255.255.255.0	Laboratorio tres
LAB3	PC_69	192.10.1.69	255.255.255.0	Laboratorio tres
Administrativo	DirecAdministra	192.10.1.83	255.255.255.0	Laboratorio tres
Administrativo	DirecSistem	192.10.1.84	255.255.255.0	Laboratorio tres
Administrativo	Rectorado	192.10.1.85	255.255.255.0	Laboratorio tres
Internet	Biblioteca	192.10.1.100	255.255.255.0	Biblioteca
Internet	Internet101	192.10.1.101	255.255.255.0	Biblioteca
Internet	Internet102	192.10.1.102	255.255.255.0	Biblioteca
Internet	Internet103	192.10.1.103	255.255.255.0	Biblioteca
Internet	Internet104	192.10.1.104	255.255.255.0	Biblioteca

Servidores	IBM Server	192.10.1.1	255.255.255.0	centro cómputo	interno
		172.30.16.35	255.255.255.240	centro cómputo	externo
Servidores	Compaq Server	192.10.1.2	255.255.255.0	centro cómputo	
	Router – DIU	172.30.16.33		centro cómputo	
	DierecPc	172.30.16.34		centro cómputo	

Direccionamiento IP Administrativa de Datos

Grupo	Nombre Pc	IP	Mascara de Entrada	Área
Administrativo	Compaq Proline	192.10.1.120	255.255.255.0	Financiero
Administrativo	Contadora	192.10.1.121	255.255.255.0	Financiero
Administrativo	AuxiContab	192.10.1.122	255.255.255.0	Financiero
Administrativo	SubDirecFinanc	192.10.1.123	255.255.255.0	Financiero
Administrativo	DirecFinac	192.10.1.124	255.255.255.0	Financiero
Administrativo	SecreDirecFinanc	192.10.1.125	255.255.255.0	Financiero
Administrativo	Guardalmacén	192.10.1.126	255.255.255.0	Financiero
Administrativo	Tesorero	192.10.1.127	255.255.255.0	Financiero
Administrativo	DirecSistem	192.10.1.128	255.255.255.0	Financiero
Administrativo	SecreSistem	192.10.1.129	255.255.255.0	Financiero
Administrativo	EduDistancia	192.10.1.130	255.255.255.0	Financiero
Administrativo	SecreCCAHH	192.10.1.131	255.255.255.0	Financiero
Administrativo	AuxiliarCCAHH	192.10.1.132	255.255.255.0	Financiero

Tabla 3.5 Direccionamiento IP de la U.T.C.

3.6.1.1.2. Configuración de la Red Universitaria

Actualmente la red de la universidad se encuentra configurada con una topología en estrella centralizada por concentradores, tanto switchs como hubs, ver (ANEXO VI). El enlace a Internet se realiza mediante una conexión satelital con la empresa proveedora de Internet IMPSAT, las conexiones internas explicadas anteriormente están enlazadas con los concentradores a los 3 laboratorios del centro de proceso de datos. El área administrativa es una red aparte, de la red académica que tiene Internet, por esta razón no forma una red corporativa, que puedan hacer uso de todos los servicios que brinda dicha red.

3.6.1.2. Seguridad de la Información y Datos

La seguridad de la información es importante, permite mantener la integridad y veracidad de los datos. He ahí que hace necesario contar con elementos que garanticen esta seguridad, pero lamentablemente este tipo de recursos son muy costosos, en este caso no justifica, debido a que la institución no maneja un repositorio de datos únicos, lo que conlleva a la prestación de servicios de red sin la necesidad

de intercambio de información. Pero en los siguientes párrafos se da algunas pautas de cómo manipular esta seguridad de información.

3.6.1.2.1. Control de Acceso a la Información

El control de acceso a la información es muy importante porque permite limitar a los usuarios acceder a cierto tipo de datos. Por tal razón es necesario establecer perfiles de usuarios al momento de crear los mismos.

Una de las ventajas de la plataforma de Linux es sin duda el acceso a información, brinda niveles de seguridad que garantizan la integridad de los datos del usuario, en este caso la universidad, mantiene su nivel de seguridad en los servidores tanto el master como el de respaldo y las estaciones de trabajo están bajo la plataforma de Windows.

Para conseguir dicha seguridad es necesario herramientas de control y seguimiento de accesos, utilizando check-lists para comprobar puntos importantes en la configuración y/o funcionamiento de

los sistemas por medio de procedimientos que hacen frente a las distintas situaciones.

Es muy aconsejable que se disponga de una agenda con las tareas a llevar a cabo regularmente, a fin de que el seguimiento de los datos obtenidos sea efectivo y se puedan realizar comparaciones válidas al contar con datos secuenciales.

Este procedimiento de check-lists puede manejarse mediante eventos que se realicen periódicamente, como a continuación se detalla:

Diariamente:

- Extraer un logístico sobre el volumen de correo transportado.
- Extraer un logístico sobre las conexiones de red levantadas en las últimas 24 horas.

Semanalmente:

- Extraer un logístico sobre los ingresos desde el exterior a la red interna.

- Extraer un logístico con las conexiones externas realizadas desde nuestra red.
- Obtener un logístico sobre los downloads de archivos realizados y quién los realizó.
- Obtener gráficos sobre tráfico en la red.
- Obtener logísticos sobre conexiones realizadas en horarios no normales (desde dónde, a qué hora y con qué destino).

Mensualmente:

- Realizar un seguimiento de todos los archivos logísticos a fin de detectar cambios (realizados con los archivos de back-up del mes anterior).
- Cabe resaltar que en gran parte, este procedimiento puede ser automatizado por medio de programas que realicen las tareas y sólo informen de las desviaciones con respecto a las reglas dadas.

Indudablemente con esto se asegura la información, pero lamentablemente no existe un sistema seguro por más seguridades que a estos se le den, porque siempre

habrán personas o instituciones que accedan a la información.

La universidad posee contados sistemas de información pero no mantiene un repositorio único de información al cual puedan acceder los usuarios. Estos sistemas de información están conectados en red, pero solo con acceso para aquellas personas que se encuentran involucrados con dicha información.

Los sistemas que existen no pueden ser chequeadas más que por las personas autorizadas entre ellos están los sistemas de tesorería, guardalmacén y de contabilidad; el sistema bibliotecario (SIABUC), permite realizar consultas de libros existentes, para estudiantes o usuarios en general se presenta solo de lectura, lo cual no puede ser modificado sea gráficos o programación que es la parte lógica. Entonces de los sistemas que llegara a existir se les da al personal sus privilegios, es decir, si pueden visualizar, imprimir, grabar, o simplemente no tiene el permiso de chequear.

3.6.1.2.2. Tipos de Respaldos

La universidad debe tener respaldos de la información procesada, incluso siendo una entidad sin fines de lucro, pero se trata de una entidad educativa el cual contiene datos de los estudiantes y necesita tenerlos a buen recaudo, sin dejar pasar por alto el área financiera que maneja la economía de la institución siendo muy valiosa.

Los respaldos son elementos que encuentran unidos directamente a la C.P.U., cuya característica fundamental es la de ser capaz de almacenar gran cantidad de datos (información), al momento de necesitar recuperarlos a gran velocidad; los respaldos se pueden almacenar en cualquier soporte físico para poder transportarlos a otro lugar especifico, entre ellos se pueden nombrar los siguientes: Disco duro, disquetes, cinta magnética, Tape Backup, CD, discos magnéticos, hasta el ordenador personal, etc., incluso la documentación que indica los procedimientos de los diferentes respaldos, y transportarlos a un lugar donde se permita el ingreso solo al personal autorizado y quienes se encarguen de los respaldos.

3.6.1.3. Virus Informáticos

Un virus informático es un programa de computadora con la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables", cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador vaya a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere conocimientos del funcionamiento interno de la computadora.

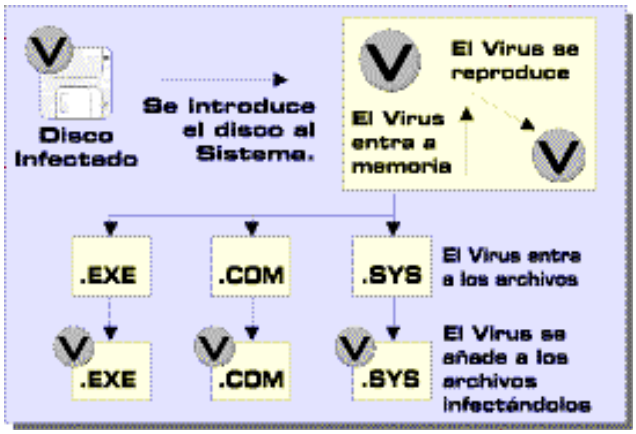


Figura 3.3 Archivos de Ataque de Virus

Los virus atacan exclusivamente a los archivos de sistema y ejecutables observe la Figura 3.3.

Los virus informáticos producen grandes molestias por lo que es necesario conocer los diversos tipos y sus

consecuencias. A continuación se presenta las ventajas y desventajas que pueden existir:

Ventajas

- Básicamente la ventaja de virus es la explotación de la capacidad del ser humano de llenar y acceder a lo imaginable.
- Con el acceso a la información privada pueden ponerla en manos de todo el mundo, pero esto puede ser arma de doble filo porque habrá intereses de por medio especialmente los económicos, que provocan la desigualdad en el mundo.

Desventajas

- Se pierde gran cantidad de información
- Los virus causan daños incontrolables y muy difíciles de detectarles y erradicarles por sus características para la cual fue creada.
- La carga activa puede trastornar o modificar archivos de datos, presentar un determinado mensaje o provocar fallos en el sistema operativo (plataforma).

- No se puede abrir archivos adjuntos porque pudiera existir un virus adjunto.
- Causa fobia por las consecuencias que trae.
- Incrementa el costo en establecer las seguridades de las redes.

3.6.1.3.1. Métodos de Infección

La universidad no es la excepción al momento del ataque o al ser infectada, porque el uso de los equipos informáticos es diario y continuo, con el riesgo de contaminarse en cualquier momento.

Existen diversos modos de infección, sabotaje informático, borrado, suprimido o modificado sin autorización de funciones o datos de computadora para obstaculizar el funcionamiento del sistema.

Normalmente el método de infección se da por falta de protección del sistema, y de la gravedad que tiene al contagiarse con un virus, por información bajada de Internet, introducción de medios magnéticos contagiados por virus, e-mail con archivos adjuntos contaminados, acceso de hacker y crakers.

A continuación los principales virus que ocasionan daños al sistema.

- **Gusanos.-** Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones al sistema informático del departamento de tesorería (JOA), para que transfiera continuamente dinero a una cuenta ilícita.
- **Bomba Lógica o Cronológica.-** Este virus se incuba sin crear ninguna copia de sí mismo hasta reunir las condiciones oportunas. Después de ese período de espera y anonimato el programa se activa y se autorreplica como un virus hasta dañar el sistema, son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las

bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo daño y para que tenga lugar mucho tiempo después de que haya marchado el delincuente. Esta técnica es usada por algunos programadores. Introducen en la aplicación un código que se activa en una fecha determinada, si no ha cobrado por su trabajo ese día, destruya la información del ordenador en el que ha instalado.

- **Backdoors o Puertas Falsas.-** Son programas que permiten la entrada en el sistema de manera que el usuario habitual del mismo no tenga conocimiento de este ataque.
- **Caballos de Troya.-** El objetivo de estos programas no es el mismo para el que aparentemente están diseñados. Se utilizan normalmente para instalar puertas traseras, que provoca pérdidas o robo de datos.
- **Spam.-** Es un programa que se ejecuta una orden repetidas veces. Este código no es dañino, pero es molestoso.
- **Sniffer.-** Estos programas son capaces de monitorear a una persona o a todo lo que se

mueve en la red. Interpretan los datos de la Internet, los copian y los modifican.

- **Ataques a Personal.-** Se suele conocer más como ingeniería social. Consiste realmente en mantener un trato social con las personas que custodian datos. La ingeniería social incluye desde suplantación de identidades confiables hasta la búsqueda en papeleras y basuras de información relevante.
- **Acceso no Autorizado a Sistemas Informáticos.-** Desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
- **Piratas Informáticos o Hackers.-** El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o

contraseñas de mantenimiento que están en el propio sistema.

Los criterios a tomar en cuenta para la seguridad de la información se consideran lo siguiente:

1. **Confidencialidad:** La información disponible sólo para los usuarios autorizados a manejarla. Puede ser accesible a atacantes, pero no sabrán interpretarlas o entenderlas. Este servicio proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.
2. **Integridad:** Este servicio garantiza que los datos recibidos por el receptor de una comunicación coinciden con los enviados por el emisor. Garantiza que la información no sea falsa y que se ha mantenido intacta.
3. **Autenticidad:** Asegurar el origen y destino de la información.
4. **No Repudio:** Quién envía no puede alegar que no envió los datos.
5. **Disponibilidad:** Asegura que el sistema de computación esté disponible a las partes autorizadas siempre que sea requerido, no existan problemas de

caídas, cuelgues o funcionamiento dudoso de la máquina que prestan los servicios.

6. **Control de acceso:** Este servicio se utiliza para evitar el uso no autorizado de recursos.

3.6.1.3.2. Procedimientos y Estrategia de Seguridad ante una Infección.

Actualmente la seguridad informática continua marcando horizontes y justifica las inversiones con la meta de mantener un nivel adecuado de aseguramiento de las arquitecturas de cómputo. Es necesario contar con personal idóneo para adelantar estas labores y mantener un monitoreo permanente del proceso de administración de la seguridad informática, por la razón que la universidad no está protegida en su totalidad es necesario introducir las formas de seguridades referentes a las infecciones de contagio o sabotaje de virus, intrusos no autorizados a la red de datos.

A continuación se muestra alternativas para la prevención:

- Un password no debe ser muy corto, permitiría ser atacado por fuerza bruta.
- Para probar que los passwords son de buena calidad se puede someter a pruebas que garantice su resistencia a un ataque diccionario, la construcción del password debe ser fácil de recordar y tener una longitud de al menos 10 caracteres.
- Ningún sistema de seguridad es 100% seguro. Por tanto los usuarios de computadoras deberían tratar de implementar estrategias de seguridad antivirus. Además no todo lo que afecte el normal funcionamiento de una computadora puede ser un virus.
- **Un disco de Sistema Protegido contra Escritura y libre de Virus:** Disco que contenga el sistema operativo ejecutable con protección contra escritura y que contenga los archivos de inicialización del sistema operativo.
- **Antivirus Actualizado:** Se suele considerar actualizado a un antivirus que no tiene más de tres meses desde su fecha de aparición, se recomienda tener por lo menos dos antivirus, es preferible tener en línea de manera que permita su actualización en forma inmediata.

En la siguiente Tabla se muestra la estadística de los virus activos en los últimos años y su peligrosidad.

Virus	PCs infectados	Peligrosidad	Fecha aparición
1 Bugbear.B	**2,84%**		**05/06/03**
2 Persis.A	**2,03%**		**10/07/03**
3 PSWBugbear.B	**1,75%**		**05/06/03**
4 Klez.I	**1,43%**		**17/04/02**
5 Fortnight.E	**1,42%**		**24/06/03**
6 Mapson	**1,17%**		**07/06/03**
7 Fortnight.D	**1,08%**		**02/06/03**
8 Parite.B	**0,92%**		**02/11/01**
9 Bugbear.Dam	**0,71%**		**12/06/03**
10 Bugbear	**0,69%**		**30/09/02**

1- 10 de **567** Virus Activos

La lista de Virus Activos la forman los virus detectados en tiempo real por la red de censores del Observatorio Mundial de Virus de Panda.

Tabla 3.6 Estadística de los Virus Activos

Además se presenta políticas a tener en cuenta al momento de trabajar en la red.

- Para que su protección antivirus sea efectiva, proteger **todos los puntos de la red** por la que pueda entrar o salir información. Esta protección incluye todos los programas y los servicios que tengan asociados.
- Es imprescindible que todas las tareas de instalación, actualización y configuración del

antivirus en cada punto de la red, estén centralizadas en una sola aplicación que combine agilidad y facilidad de uso.

- Utilice un sistema de filtrado de contenidos. Es imprescindible para rechazar todos los elementos no deseados e incluso pueden evitar la llegada de ciertos tipos de virus.

- **Una Fuente de Información sobre Virus Específicos:** Estar actualizado sobre los diferentes tipos de virus existentes en el medio, sus características, síntomas en si la descripción del virus a propagarse.
- **Un Programa de Respaldo de Áreas Críticas:** Programa que obtenga respaldo (backup) de los sectores de arranque de disquetes y sectores de arranque maestro (MBR, Master Boot Record) de los discos rígidos.
- **Lista de Lugares dónde Acudir:** Elaborar una agenda de direcciones, teléfonos y direcciones electrónicas de las personas y lugares que puedan servir más adelante. Si cuenta con un antivirus comercial, deberán tener los teléfonos de soporte técnico en una parte visible.

- **Tener Respaldos:** Se deben tener respaldados en disco los archivos de datos más importantes, además, se recomienda respaldar todos los archivos ejecutables, de los archivos más importantes, es bueno tener un respaldo doble, por si uno de los discos de respaldo se daña. Los respaldos también pueden hacerse en cinta (tape backup), aunque para el usuario normal es preferible hacerlo en discos, por el costo que las unidades de cinta representan.
- **Realizar un análisis de qué datos guardar** La planificación del sistema de copias de seguridad pasa primero por evaluar la **importancia de la información** y determinar la **periodicidad** con que se realizan las copias. Seguidamente, elija el **soporte** en el que se van a realizar las copias y protéjalas físicamente en armarios o en sistemas autónomos e ignífugos. Junto con las copias de seguridad. Conserve los **discos de arranque** y de emergencia de todos los sistemas que utilice. Esto le facilitará el inicio de los ordenadores en caso que sea imposible realizarlo de forma normal.
- **Revisar los discos nuevos antes de ser utilizados:** Cualquier disco que no haya sido previamente utilizado debe ser revisado, inclusive los programas

originales y los que se distribuyen junto con revistas de computación.

- **Revisar los discos que se hayan prestado:** Disco que se haya prestado a alguien, aún aquellos que contengan archivos de datos, deben ser revisados antes de usarse nuevamente.
- **Revisar Programas que se Obtengan por Módem o Redes:** Las grandes vías de contagio, constituyen Internet y los BBS, sistemas en los cuales es común la transferencia de archivos
- **Revisar Periódicamente la Computadora:** Se considera que una buena frecuencia de análisis es, por lo menos, mensual.

A continuación se presenta unas recomendaciones el cual debe tener muy en cuenta la universidad, se trata de un tema muy importante:

- Cuando se va a revisar o desinfectar una computadora, es conveniente apagarla por más de 5 segundos y arrancar desde un disco con sistema, libre de virus y protegido contra escritura, para eliminar virus residentes en memoria. No se deberá

ejecutar ningún programa del disco rígido, el antivirus deberá estar en el disquete.

- Cuando un sector de arranque (boot sector) o de arranque maestro (MBR) ha sido infectado, es preferible restaurar el sector desde algún respaldo, puesto que en ocasiones, los sectores de arranque genéricos utilizados por los antivirus no son perfectamente compatibles con el sistema operativo instalado.
- Antes de restaurar los respaldos es importante no olvidar apagar la computadora por más de cinco segundos y arrancar desde el disco libre de virus.
- Cuando se encuentran archivos infectados, es preferible borrarlos y restaurarlos desde respaldos, aún cuando el programa antivirus que usemos pueda desinfectar los archivos.
- Cuando se va a formatear un disco rígido para eliminar algún virus, debe recordarse apagar la máquina por más de cinco segundos y posteriormente arrancar el sistema desde nuestro disquete limpio, donde también debe encontrarse el programa que se utilizará para dar formato al disco.
- Cuando se ha detectado y erradicado un virus es conveniente reportar la infección a algún experto,

grupo de investigadores de virus, soporte técnico de programas antivirus, etc.

3.6.1.4. Formas de Protección

El personal que este al frente del área tiene la responsabilidad de realizar un estudio de los mejores protectores de virus, intrusos no autorizados, existen muchas formas de protección de los sistemas de información y datos, que garantizan en un alto porcentaje la fidelidad de la misma y que proporcione un nivel alto de seguridad a la red institucional o corporativa.

Algunos parámetros fueron señalados anteriormente sobre la protección contra los virus informáticos, a continuación señalaremos otros tipos de protección, muestra lo que ofrece, y sus garantías:

- Firewalls (cortafuegos)
- VPN (red privada virtual)
- Conexiones seguras (SSL)
- Wrappers
- Software de análisis de vulnerabilidad
- Fingerprints para archivos

Cada uno de estas alternativas podrá adaptarse a la red dependiendo de las medidas de seguridad que cada una de ellas necesite y al flujo e importancia de información que mantenga en la red para usuarios externos o propios de la organización o institución.

- **Firewalls (cortafuegos)**

  Un Firewall básicamente es una computadora (Pc) que registra todos los paquetes de información que ingresan en una organización, una vez verificados, derivarlos a otra que tiene conexión interna (conexión a la red) y no recibe archivos que no provengan de aquella.

  Además evita accesos no autorizados desde o hacia una red privada. Pueden estar implementados en hardware o software, o una combinación de ambos, son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de Internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran, pasan a través del Firewall, examina cada mensaje y bloquea aquellos que

no cumplan con determinado criterio de seguridad. Su esquema se representa en la siguiente Figura.

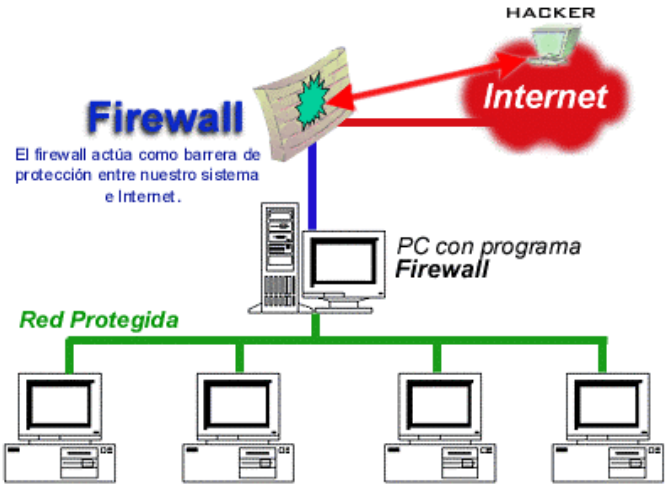


Figura 3.4 Esquema de un Firewall

Al incrementar un Firewall en la universidad se obtendrían grandes beneficios; a continuación las siguientes ventajas y desventajas:

Ventajas

- Protege los documentos o archivos de personal no autorizado.
- La universidad debe estar de acorde a la actualidad con tecnología de punta.
- Determina qué recursos de su equipo están accesibles para los usuarios remotos de la red.

- Un Firewall bien configurado puede aumentar significativamente la seguridad de su sistema.
- Este tipo de programa se basa en el "filtrado de paquetes". Todo dato o información que circule entre nuestro PC y la Red es analizado por el programa, con la misión de permitir o denegar su paso en ambas direcciones (Internet – PC ó PC – Internet).
- El Firewall funciona, en principio, denegando cualquier tráfico que se produzca cerrando todos los puertos de nuestro PC.
- La misión del Firewall es de aceptar o denegar el trafico, pero no el contenido del mismo. En éste caso, la misión de proteger es de un programa Antivirus.
- En el momento que un determinado servicio o programa intente acceder a Internet o al PC, alarmará indicando que existe un intruso.
- Con la instalación de un Firewall en la universidad se consigue hacer el sistema mucho menos vulnerable a intrusos.
- El Firewall actúa como un punto de cierre que monitorea y rechaza el tráfico de red a nivel de aplicación.

- Permite bloquear el material no adecuado, determinado de esta manera que sitios pueden acceder el usuario de la red interna y para completa llevar un registro, este sistema facilita a los responsables de la seguridad, mantener al margen los ataques externos.
- Este sistema permite auditar para justificar el gasto que implica la utilización de Internet, localizando los cuellos de botella potenciales del ancho de banda.
- El programa mantiene alejados a los piratas informáticos de la red, al mismo tiempo permite acceder solo usuarios autorizados.

Desventajas

- Los costos de los Firewalls son altos pero serían de gran beneficio para la Universidad.
- Si no se cuenta con un Firewall, cada uno de los servidores del sistema se exponen al ataque de otros servidores en Internet.
- Los sistemas informáticos cada vez son más complejos, tienen más puntos débiles debido simplemente a su mayor dimensión, pues el número

de posibles atacantes crece debido a la mayor conectividad.

- Al momento de configurar otorgar los permisos necesarios para mayor seguridad porque de ser así no serviría de nada tener un Firewall.
- El Firewall no puede protegerse de los posibles ataques a la red interna por virus informáticos a través de archivos y software.
- El Firewall no puede protegerse de las amenazas a que esta sometido por traidores inconscientes, pertenecientes a la Institución.
- El Firewall no puede proteger contra los ataques de la ingeniería social, en este caso, un craker que quiera ser un supervisor o aquel que persuade a los usuarios menos sofisticados.
- Además no proteger contra los ataques en la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando el ataque.

- **VPN (red privada virtual)**

Una VPN se extiende, mediante un proceso de encapsulación, y en el caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un túnel definido en la red pública. En el Grafico 3.5 se puede ver de mejor forma:

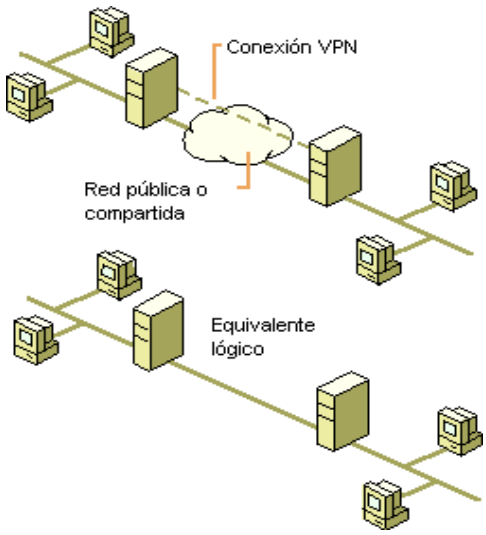


Figura 3.5 Red con Conexión VPN

Una VPN en un acceso remoto permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público. Como en la siguiente Figura.

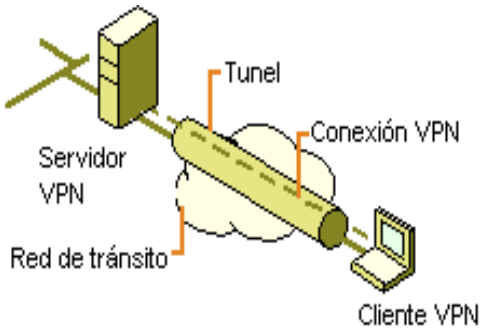


Figura 3.6 Red de VPN

En ocasiones puede ser interesante que la comunicación que viaja por el túnel establecido en la red pública vaya encriptada para permitir una mayor **confidencialidad**.

Ventajas

- Mayor integridad de los datos
- Son transmitidos por la red pública
- Permite acceder a la red corporativa cuando se encuentra en una parte remota.
- Los datos son encriptados
- Autorizan privilegios

Desventajas

- Los datos para la transmisión pasa por la red pública, con el peligro de ser interrumpida por sabotajes.

- Falta de conocimientos puede ser fatal
- Necesita de uso de Internet.

- **Wrappers**

Un Wrapper permite controlar y proteger los servicios de red, limitando el acceso como sea posible, y registrando todos las conexiones para hacer el trabajo de detectar y resolver problemas de forma más fácil.

Esta herramienta ha sido utilizada exitosamente en la protección de sistemas y la detección de actividades ilícitas; es una herramienta de seguridad libre y muy útil.

Los requerimientos de la seguridad varían dependiendo de la complejidad de las tareas o actividades en las cuales se emplea el equipo de cómputo y de la plataforma de equipo que éstas involucren. Las medidas de seguridad necesarias para proteger una Pc no es la misma que las medidas de seguridad necesarias para garantizar el funcionamiento continuo de una red de área local (LAN), y éstas a su vez son menores a las

requeridas cuando se trata de una red área amplia (WAN), que sería el caso de la conexión a Internet.

Ventajas

- Es un software de domino público
- Protege a los sistemas de conexión no deseadas a determinados servicios de la red.
- Permite ejecutar determinados comandos ante determinadas acciones de forma automática.
- Con este paquete podemos monitorear y filtrar peticiones entrantes a distintos servicios TCP-IP, como: SYSTAT, FINGER, FTP, RLOGIN, RSH, REXEC, TFTP, TALK.
- Llega hacer una herramienta simple que sirve para monitorear y controlar el tráfico que llega por la red.

Desventajas

- La seguridad varía de acuerdo a la complejidad de las tareas.
- La mala administración sería desastrosa.
- El desconocimiento de sus funciones y limites, podría dejar huecos, el cual puede crear conflictos.

3.6.2. Física

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información.

La seguridad física abarca componentes como:

- Protección del sistema.
- Planes de contingencia.
- Control de acceso físico.
- Políticas de respaldos.
- Cableado eléctrico.
- Cableado de datos.
- Infraestructura del centro de datos.

Estos puntos se detallan ampliamente en las secciones que a continuación vienen.

3.6.2.1. Instalaciones Físicas del Centro de Datos

La universidad cuenta con un centro de cómputo y es importante considerar la instalación física y la importancia que este tiene para las demás dependencias he ahí que la

ubicación debe ser estratégica de manera que permita brindar de manera eficiente, efectiva y eficaz los servicios.

La administración de recursos informáticos de la U.T.C., es responsabilidad del centro de datos o de la Dirección de Servicios Informáticos. Las funciones de administrar incluyen la administración de los servidores de Internet, bases de datos, supervisión del tráfico de la red, la seguridad de accesos a la red.

Ninguna dependencia podrá instalar nuevos enlaces a Internet, de ningún tipo, sin el consentimiento y supervisión previa del administrador del centro cómputo, a fin de no alterar o interferir con las comunicaciones ya instaladas.

Será responsabilidad del administrador orientar, coordinar proponer y buscar nuevas políticas de acción de manera que permitan fortalecer y eliminar debilidades fomentando el desarrollo tecnológico de la institución.

Se hace necesario antes de dar cualquier paso establecer una ubicación idónea para el centro de datos. Pero se ha encontrado ciertos parámetros que no cumplen, para lo cual

se elaboró una matriz de riesgo como se muestra en la Tabla 3.7.

Actividad	Nivel de Riesgos			
	A	**M**	**B**	**X**
Acceso a máquinas	3			
Acceso de elementos de trabajo		3		
Deslaves				4
Filtraciones de agua			3	
Inundación				4
Espacio físico	2			
Sabotaje			3	
Hundimiento de piso				4
Sismos	2			
Temperatura		3		
Interferencias electromagnéticas		2		
A = Alto **M** = Medio **B** = Bajo **X** = Muy bajo		**1** = Grave **2** = Mediano **3** = Poco **4** = Inexistente		

Tabla 3.7 Riesgos por Ubicación

A más de esto se ha detectado y podido observar otros tipos de riesgos que se dan por no poseer una infraestructura idónea que permitan estar preparados para cualquier eventualidad y cumplir eficientemente los procesos.

Actividad	Nivel de Riesgo			
	A	**M**	**B**	**X**
Líneas telefónicas		2		
Instalación eléctrica		2		
Piso falso	4			
Cableado de datos	2			
Paredes y techos			2	
Puertas de acceso				4
Cuarto de telecomunicaciones	2			
Iluminación			2	
Necesidad de espacio	4			
Distribución departamental		2		
Aire acondicionado				4
Sistemas de conexión a tierra			3	
Generador de energía				4
Seguridad contra incendios				4
A = Alto **M** = Medio **B** = Bajo **X** = Muy bajo		**1** = Eficiente **2** = Bueno **3** = Malo **4** = Deficiente		

Tabla 3.8 Otros Factores de Riesgos

A continuación se indica los parámetros ideales que el centro de cómputo debe tener y mantener las instalaciones.

a. Cableado

Básicamente el cableado comprende el cableado vertical / central / backbone y el cableado horizontal.

Cableado Central /vertical / backbone

El propósito del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de un edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. Consiste de los cables centrales, interconexiones intermedias y principales terminaciones mecánicas y cables de parcheo o puentes, utilizados para interconexiones de central a central.

Problema:

En la U.T.C., lamentablemente no se ha realizado un estudio para el diseño e implementación de la red de

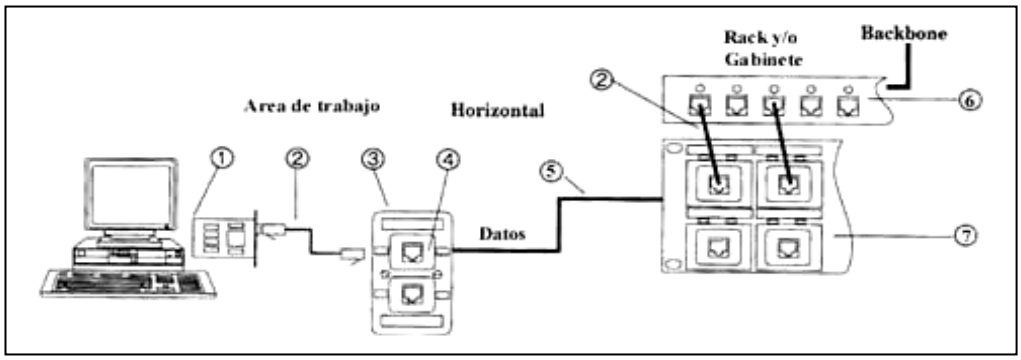
datos, simplemente se estimó la necesidad de implantar una red, sin tomar en cuenta los estándares internacionales que rigen para el diseño de una red de datos. Actualmente el cableado vertical es casi inexistente debido a la infraestructura misma de la institución, que no brinda facilidades para este tipo de diseño.

Pero se puede observar que existe una especie de cableado vertical que une algunas de las dependencias sin ningún diseño lógico, lo que tarde o temprano el medio de transmisión o la información serán preso de los factores del medio ambiente.

Solución:

- El diseño de una red para datos debe basarse en el esquema de la Figura 3.7, donde se señala todos los puntos a ser considerados en el momento de diseño e implementación de la misma.
- Por las inspecciones que se realizaron a la institución, las estaciones de trabajo (work-station) cumplen con este estándar.

- Se sugiere tomar las precauciones del caso al momento de enlazar el face plate con el panel de parcheo, debido, que el medio de transmisión que se utiliza (cable UTP categoría 5e) no utiliza las medidas de protección, causando daños en el medio de transmisión.



1. Tarjeta de Red.
2. Cable de Parcheo RJ45/RJ45.
3. Tapa Face plate.
4. Jack Modular (Hembra RJ45).
5. Cable UTP (FTP) RJ45.
6. Concentrador (HUB).
7. Panel de Parcheo.

Figura 3.7 Esquema de un Cableado para Voz

- En el diseño de nuevo campus existen pisos o plantas donde se necesita diseñar una nueva red de acuerdo a la infraestructura y tecnología, se propone desarrollar un diseño lógico del backbone que establezca, de modo que brinde crecimiento futuro para la institución, sin la necesidad de mayor inversión. En la Figura 3.8 se observa el esquema de un backbone.

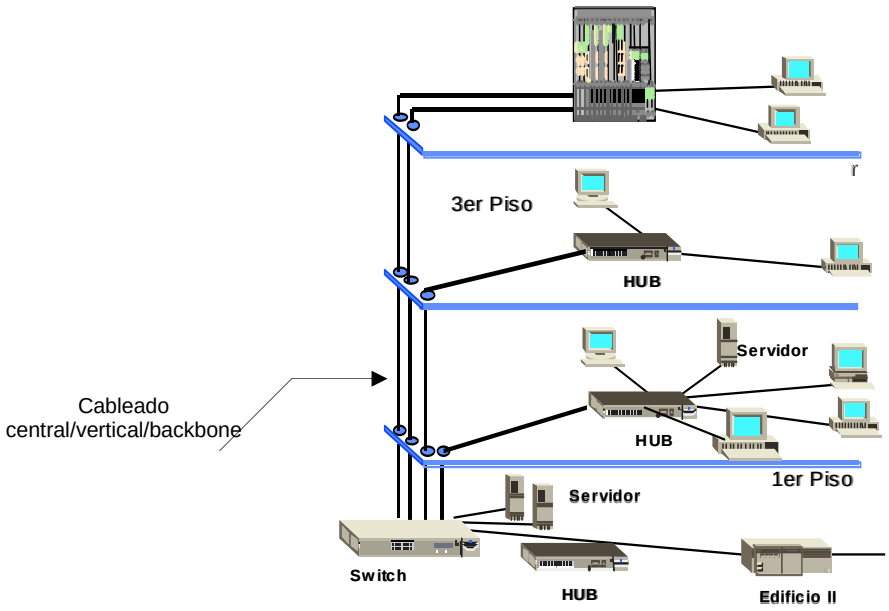


Figura 3.8 Esquema de un Cableado Central/Vertical/Backbone

Cableado horizontal

El cableado horizontal proporciona los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. El cableado horizontal comienza donde el usuario conecta un terminal y termina en un punto localizado centralmente llamado el cuadro de distribución. El cableado horizontal conecta cada área de trabajo a una localización central.

Problema:

- Referente a los estándares de cableado horizontal, la institución cumple en su gran parte, pero existen ciertos inconvenientes al momento de detectar alguna falla o avería en el medio de comunicación, debido a que el equipo no se encuentra distribuido de una manera lógica.
- El problema de la detección de fallas del medio se incrementa aún más a la no-existencia de pisos falsos por los cuales pasa las canaletas.
- También existe una escasa nomenclatura de los cables al momento de salir del face plate a las estaciones de trabajo.

Solución:

- Es necesario el diseño, que generalmente se da con pisos falsos y en otras ocasiones con techos falsos, permitiendo detectar y solucionar fácilmente algún inconveniente que se presente, sustituir un cable resulta más fácil y rápido.
- Pero si no se da este esquema de pisos falsos por la estructura de la U.T.C., es necesario la utilización

de canaletas que se adapten fácilmente a las necesidades de la institución, realizar un estudio de las diferentes canaletas que existan, con la posibilidad de escoger la más conveniente, de acuerdo al medio de desarrollo.

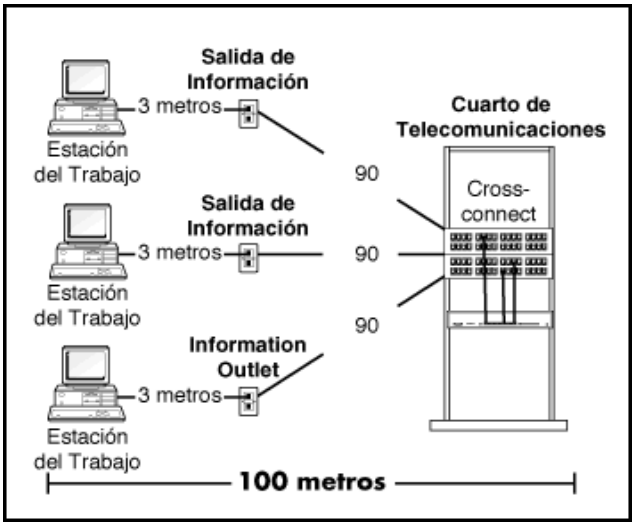


Figura 3.9 Estándares de Distancias del Cableado Horizontal

b. Piso y Techo Falso

Los pisos y techos falsos son aquellos que facilitan la instalación del cableado de voz, datos, video y energía. Obviamente el cable de energía jamás se debe mezclar con el resto de cableado. Deben ser canaletas muy separadas a una determinada distancia.

Problema:

- Como se expuso anteriormente la institución no posee ni pisos ni techos falsos, lo que retraza el mantenimiento e incremento de nuevos puntos de red. Al momento de existir un problema con el medio de transmisión (cable UTP categoría 5e) tendríamos que destruir la pared, de idéntica forma al incrementar un punto de red y colocar el face plate. Con riesgo de destruirse los cables.
- No se respetan los estándares de cableado, nunca deben estar juntos el cableado eléctrico y de voz.
- A más de este existe mucho cableado que sale de las estaciones de trabajo lo que forma una telaraña de cables que puede ocasionar un cortocircuito.

Solución:

- Utilizar canaletas que se adapten a los requerimientos y necesidad institucional.
- El uso de canaletas facilita el crecimiento de la red sin la necesidad de realizar obras de ingeniería.
- De acuerdo a la infraestructura de la institución el uso de las canaletas es el más adecuado, por su

adaptabilidad al medio exterior y en el interior, lo que proporciona seguridad a los medios de transmisión en nuestro caso cable UTP categoría 5e.

- En la Figura 3.10 se observa un esquema de pisos y techos falsos apropiados para un cableado, de idéntica forma como el cableado eléctrico se encuentra en el interior del piso falso, evitando así una telaraña de cables

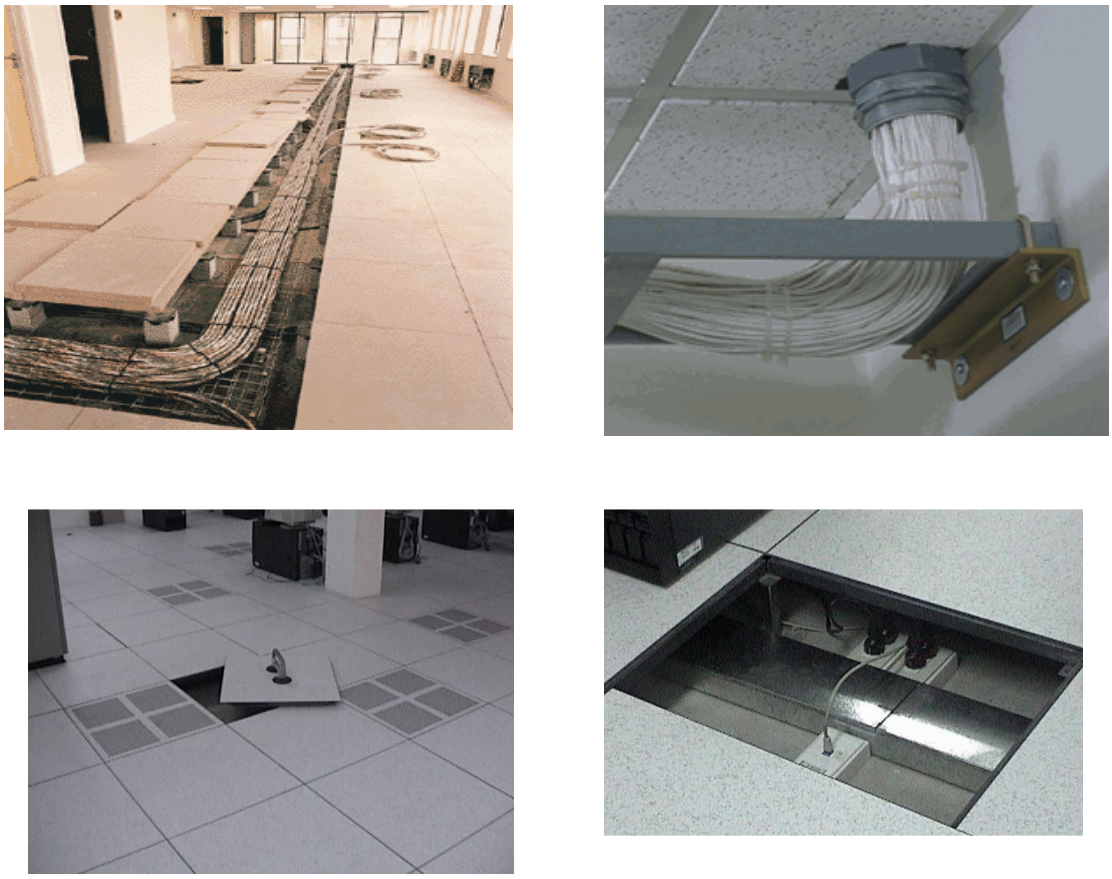


Figura 3.10 Cableado en un Piso y Techo Falso

En las dos últimas Figuras se puede observar la estructura de los pisos falsos y las instalaciones para datos, cableado de energía y aire acondicionado.

c. Closet o Armario de Telecomunicaciones

El armario de telecomunicaciones es el área donde se aloja el equipo del sistema de cableado de telecomunicaciones. Se puede incluir todo el equipo necesario para conectar estaciones de trabajo a la habitación de equipo, como concentradores, repetidores, módems, entre otros.

Además sirve como punto de concentración para el cableado que interconecta dispositivos y sistema de parcheado para añadir y quitar dispositivos de la red.

Dentro de un armario o closet podemos tener elementos como:

- Rack
- Gabinete
- Concentradores
    - Hub

    - Mau
- Repetidores
- Switch
- Path panel
- Regletas
- Patch cord
- Firewall, etc.

Un armario garantiza la seguridad de los dispositivos evitando ser destruido.

Problema:

- En la universidad no existe un armario de telecomunicaciones, el rack se encuentra descubierto como se muestra en la Figura 3.11, visualizándose el modo que se mantiene los cables, con el riesgo de ser manipulado por cualquier intruso, además la falta de identificación de los patch cord que no permiten una identificación apropiada de las máquinas conectadas a la red.

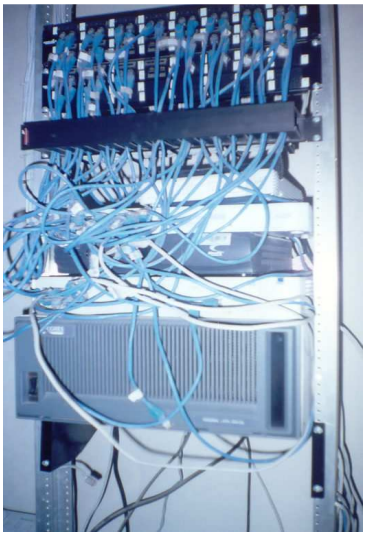


Figura 3.11 Rack U.T.C.

Solución:

- La solución es muy simple, implementar un armario de telecomunicaciones y etiquetar los patch cord, además llevar un registro de que máquinas se encuentran conectadas a la red y subredes si existiese.
- Los servidores deberían estar en un rack de telecomunicaciones como en la Figura 3.12, para que usuarios no autorizados manipulen los servidores.

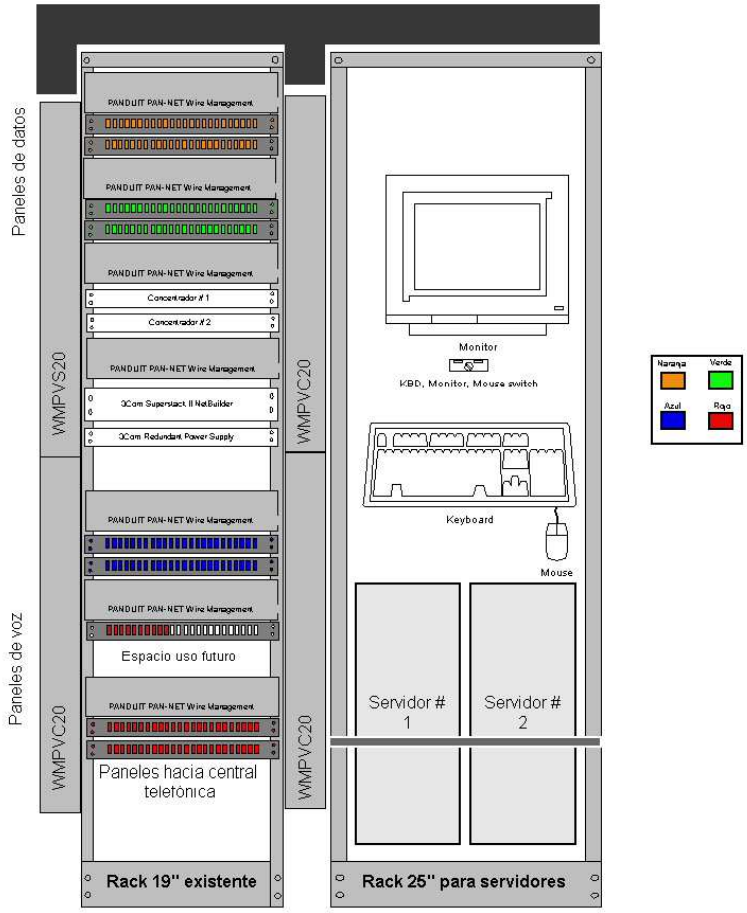


Figura 3.12 Armario de Telecomunicaciones (voz, datos y servidores)

d. Paredes y techos

Es muy importante la infraestructura en la que se desarrolla las actividades del centro de datos y debiendo ser la mejor. Con la construcción del nuevo campus universitario se espera un edificio inteligente, donde albergará todas las seguridades, siendo único en la provincia y en el país, pero la construcción está muy

lejana, entonces tienen que pensar en la mejor edificación de los techos y paredes.

Problema:

- Las instalaciones se encuentran pintadas con una pintura de agua, que no permite ser lavadas las paredes.
- Las ventilaciones son apropiadas, pero lamentablemente no existe cortinas o persianas adecuadas, para que no permita el paso de la luz del día, que ocasiona una reflexión de luz con los monitores.
- La infraestructura de los distintos laboratorios no es la apropiada, lamentablemente se debe adaptar a las circunstancias. Otro detalle importante a tomar en cuenta, es lo referente a la cañería de los servicios higiénicos que se encuentran en medio de los tres laboratorios, lo que puede ocasionar una fuga de líquido y dañar el cableado eléctrico o de datos.

Solución:

- Pintura plástica lavable

- Falso (amarres de plafón)
- La altura neta: 2.70 a 3.30 metros
- Reubicación de los servicios higiénicos y su cañería
- Instalación de persianas o cortinas que no permitan el paso de la luz solar.

e. Puertas de Acceso

Las puertas de acceso permiten brindar seguridad al centro de datos, y a los usuarios que se encuentran dentro de sus instalaciones.

Problema:

- No existen puertas adecuadas para la seguridad, aumentando la vulnerabilidad de las instalaciones del centro de datos.
- Las puertas de acceso se han establecido de acuerdo a las necesidades, sin tomar en cuenta la probabilidad de que pueda suceder algún tipo de riesgo.
- No existe una conexión adecuada entre los tres laboratorios y próximamente con el cuarto, lo que

produce incomodidad en los usuarios del centro de datos.

Solución:

- Las puertas de seguridad para acceder al centro de datos debería ser mínima de doble hoja de 1.50 cm.
- Además el centro de datos debería poseer salidas de emergencia que facilite la evacuación inmediata de las personas que se encuentran en su interior, y equipos que se puedan salvar.
- Es importante al momento de optar por una puerta de acceso a laboratorio u otras dependencias, primero teniendo en cuenta las dimensiones máximas del equipo, evitando los inconvenientes al ubicar equipos en el interior del centro de datos.

f. Iluminación

Una buena iluminación crea un ambiente agradable de trabajo, a más de proporcionar el funcionamiento de los equipos y brindar seguridad a las instalaciones.

Problema:

- La iluminación al ingreso de las instalaciones de la institución no es la adecuada.
- No existe un generador, que proporcione alimentación de energía a las instalaciones en el momento de que estas llegue a suspenderse.
- En caso de un corte de energía no existe ningún tipo de iluminación conectado al UPS.

Solución:

- Es momento de adquirir un generador para resguardar la integridad de los equipos que puedan afectar al momento de un apagón. Además debe ser instalado fuera del centro de datos
- La alimentación de la iluminación debe ser diferente a la instalada para los equipos
- Considerar que el 25% de la iluminación debe ser de emergencia conectado al UPS.

Recursos y prioridades de los usuarios.- En la siguiente Tabla se identifica los recursos y las prioridades de acceso que tienen cada uno de los usuarios, que son determinadas por el centro de procesamiento de datos.

RECURSO DEL SISTEMA		IDENTIFICACIÓN USUARIO	TIPO DE ACCESO	PERMISOS OTORGADOS
NUMERO	NOMBRE			
1	• Base de datos financiero	Grupo de contadores y financieros	Local	Lectura y escritura
2	• Base de datos biblioteca	Grupo bibliotecario	Local	Lectura y escritura
3	• Módem satelital (DIU) • Router • Switch • Servidores • Cableado para datos	Grupo de Administración de comunicaciones	Local y remota	Lectura, escritura y ejecución
4	• Servidor • Estaciones de trabajo • Impresoras • Unidades de almacenamiento externo	Grupo de Administración de usuarios y mantenimiento de periféricos	Local	Lectura, escritura y ejecución
5	• Estaciones de trabajo • Impresoras • Unidades de almacenamiento externo	Grupo de usuarios finales	Local y remota	Lectura y escritura

Tabla 3.9 Determinación de Recursos

En el análisis de los riesgos, es necesario determinar los siguientes factores como se indico en uno de los capítulos anteriores:

- Estimación del riesgo de pérdida del recurso (**R**i)
- Estimación de la importancia del recurso (**W**i)

La evaluación general del riesgo se maneja con la fórmula que a continuación se indica:

$$\mathbf{WR_i = R_i * W_i}$$

Al tomar como ejemplo el primer recurso del sistema la evaluación del riesgo sería:

Recurso:	Servidor
Riesgo:	**R1** = 10.0
Importancia:	**W1** = 1.0
	WR = 10 * 1 **= 10**

En la Tabla 3.10 se establece la matriz de riesgo de los recursos más importantes que están susceptibles a amenazas de riesgo, aplicando la fórmula y el procedimiento anterior.

RECURSO DEL SISTEMA		RIESGO (Ri)	IMPORTANCIA (Wi)	RIESGO EVALUADO (Ri * Wi)
Nº	NOMBRE			
HARDWARE				
1	Servidor	10,00	1,00	10,00
2	Módem satelital (DIU)	9,00	0,85	7,65
3	Router	8,00	0,85	6,80
4	Switch	7,00	0,85	5,95
5	HUB	7,00	0,60	4,20
6	UPS	8,00	0,80	6,40
7	Estaciones de trabajo	6,50	0,80	5,20
8	Computadoras portátiles	5,00	0,50	2,50
9	Cableado de red de datos	6,70	0,80	5,36
10	Procesadores	4,00	0,60	2,40
11	Tarjetas principales (mainboard)	5,00	0,60	3,00
12	Impresoras	8,00	0,80	6,40
13	Líneas de comunicación	9,00	0,90	8,10
14	Unidades de almacenamiento externo	4,00	0,40	1,60
SOFTWARE				
15	Sistema operativo servidor Linux	10,00	1,00	10,00
16	Sistema operativo estaciones de trabajo Windows x	8,00	0,80	6,40
17	Utilerías	5,00	0,50	2,50
18	Programas de diagnóstico	8,00	0,80	6,40
19	Programas de comunicaciones	8,00	0,85	6,80
20	Programas de control de virus	7,00	0,80	5,60
DATOS				
21	Datos fuera de línea	4,00	0,50	2,00
22	Respaldos (back-up)	7,00	0,75	5,25
23	Base de datos locales	7,00	0,75	5,25
GENTE				
24	Usuarios	7,00	0,70	4,90
25	Personas que operan los sistemas	7,00	0,60	4,20
26	Administradores de servidores	7,00	0,80	5,60
DOCUMENTACIÓN				
27	Programas/aplicaciones desarrolladas	7,00	0,70	4,90
28	Hardware	7,00	0,90	6,30
29	Software	6,00	0,80	4,80
30	Procedimientos administrativos locales	7,00	0,80	5,60
31	Sistema de comunicación satelital	9,00	0,90	8,10
ACCESORIOS				
32	Información grabada	8,00	0,80	6,40
33	Repuestos para equipos de cómputo	8,00	0,90	7,20
34	Medios magnéticos para respaldos	7,00	0,70	4,90

Tabla 3.10 Niveles de Riesgo de los Recursos de la U.T.C.

En la Tabla 3.11 se determina los rangos tanto para el riesgo como para la importancia del recurso con los cuales se determinaron el riesgo evaluado.

TIPO	RANGO MÍNIMO	RANGO MÁXIMO
Riesgo (Ri)	1	10
Importancia del recurso (Wi)	1	10

Tabla 3.11 Niveles de Riesgo de los Recursos

En el siguiente gráfico se muestra el triángulo de debilidades luego de haber realizado el análisis de la seguridad física y lógica de la red de datos de la U.T.C.

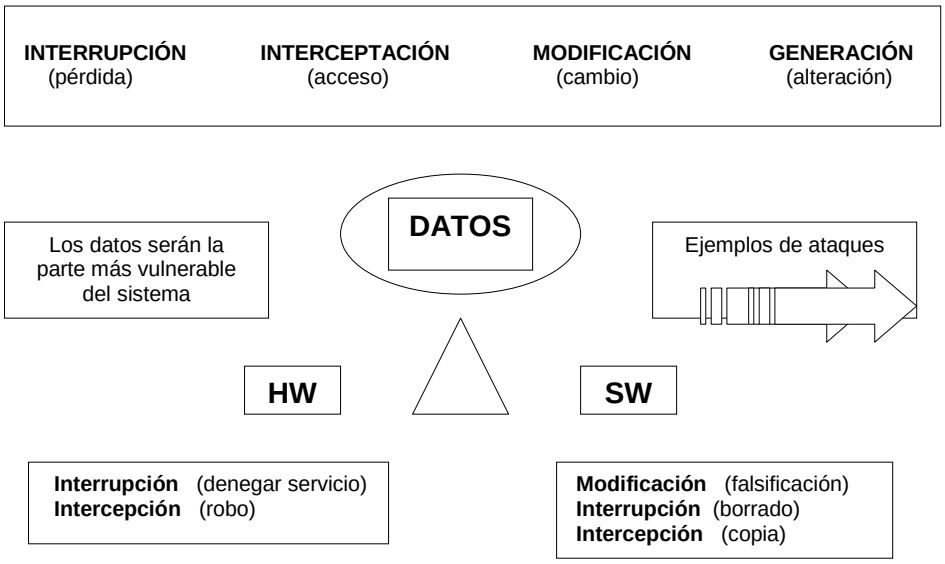


Figura 3.13 Triángulo de Debilidades

3.6.2.2. El Fuego

El fuego es consecuencia del calor y la luz que se producen durante las reacciones químicas, denominadas combustión. En la mayoría de los fuegos, la reacción de combustión se basa en el oxígeno del aire, al reaccionar este con un material inflamable, tal como la madera, ropa, papel, petróleo, o los solventes, los cuales entran en la clasificación química general de compuestos orgánicos.

El fuego, es un riesgo constante en el trabajo, hogar y en las actividades de ocio. La mayoría de las personas que mueren en incendios, es a consecuencia del efecto tóxico del humo y de los gases calientes, y no como consecuencia directa de las quemaduras.

Triángulo del Fuego

En el siguiente gráfico están representados los tres elementos del fuego:

Figura 3.14 Componentes del Fuego

Si en este triángulo faltare cualquiera de estos tres elementos no podrá producirse fuego. La base sobre lo que se apoya la prevención del fuego y la lucha contra el mismo, consiste en romper el triángulo del fuego. La reacción de la combustión, reside en el oxigeno del aire para que este apoye a la combustión, esta no es la única fuente de oxígeno en su estructura, solamente requiere calor para quemarse sin que el aire ayude.

A continuación, algunos factores que ayudan a la combustión:

Combustible

Puede ser cualquier material combustible, sólido, líquido o gas. La mayoría de los sólidos y líquidos se convierten en vapores o gases antes de entrar en combustión.

Oxígeno

Es un carburante, es decir activa la combustión. El aire constituye un factor vital para la supervivencia de los seres vivos, está compuesto de 21% de oxigeno, por lo tanto el fuego requiere una atmósfera de por lo menos 16% de oxigeno para que entre en acción.

Calor

Es la energía requerida para elevar la temperatura del combustible hasta el punto en que se despiden suficientes vapores que permiten que ocurra la ignición

Reacción Química

Una reacción en cadena puede ocurrir cuando los otros tres elementos antes mencionados están presentes en las condiciones y proporciones apropiadas considerando como incendio a todo tipo de fuego no controlado que cause o no daños directos.

Tipos de Fuegos

En el siguiente cuadro se establece los tipos de fuego que pueden presentar un incendio, y dependiendo del tipo de material con que se produzcan.

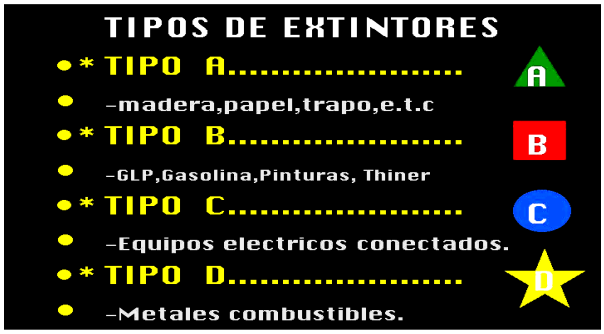


Figura 3.15 Los Diferentes Tipos de Fuego

Clase A

Están involucrados los materiales orgánicos sólidos, en los que pueden dar origen las brasas, por ejemplo; madera, papel, goma, plásticos y tejidos.

Figura 3.16 Tipos de Fuego Clase A

Clase B

Involucran a los líquidos y sólidos fácilmente fundibles, por ejemplo, el etano, metano, la gasolina, parafina y la cera de parafina que son agentes activos que ayudan a la combustión.

Figura 3.17 Tipos de Fuego Clase B

Clase C

Involucran a los equipos eléctricos energizados, tales como electrodomésticos, interruptores, cajas de fusibles y las herramientas eléctricas.

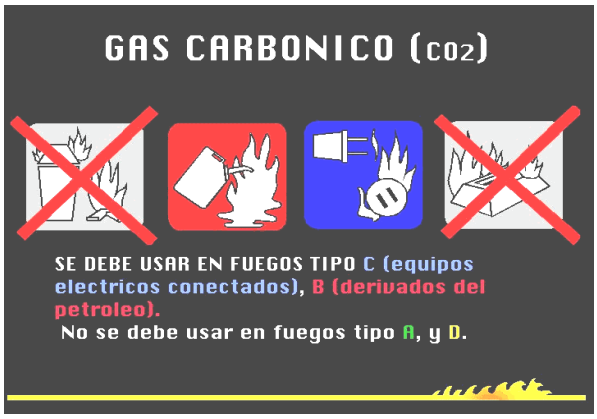


Figura 3.18 Tipos de Fuego Clase C

Clase D

Están involucrados ciertos metales combustibles, como el magnesio, el titanio, potasio y el sodio. Estos metales

exhalan suficiente oxigeno como para mantener la combustión.

3.6.2.2.1. Sistemas Automáticos Antifuego

Actualmente existen detectores para el humo y otros para el calor. De acuerdo a las normativas de seguridad obligan instalar determinados sistemas de detección en los diferentes edificios.

La universidad no posee sistemas para controlar el fuego, es necesario implementar un sistema inteligente de antifuego, para proteger diversos equipos existentes en la universidad, caso contrario de ocurrir un incendio las pérdidas serían cuantiosas.

3.6.2.2.2. Extinguidores Manuales

Los extinguidores son aparatos diseñados especialmente para que permita la descarga de una determinada cantidad de agente extinguidor, almacenado en su interior de acuerdo con las necesidades de su operador.

Los extinguidores son equipos de primeros auxilios contra incendios, destinados a ser usados contra fuegos pequeños e incipientes. A más de esto si no son usados es un elemento que también se caduca, en un determinado tiempo y la actualización es indispensable.

Figura 3.19 Tipos de Extintores

A continuación se presenta una tabla con los diferentes extintores:

EQUIPOS	CANTIDAD
Extinguidores de 150 psi c/u Polvo Químico seco 3	3
Extinguidores de 30 psi c/u Polvo Químico seco	10
Equipo completo de comunicación	2
Material absorbente	>100 Lts.
Manga de Viento	1
Red contra incendio	1 ó más
Estuche completo de herramientas para ruptura de cañerías	Mínimo
Tejos, grapas, llaves y otros	Varios

Tabla 3.12 Tipos de Detectores de Humo

3.6.2.3. El Agua

El agua es un nombre común que se aplica al estado líquido del compuesto de hidrógeno y oxígeno H_2O. El

agua no es un elemento sino un compuesto de oxígeno e hidrógeno.[1]

Es importante que la institución posea depósitos de agua adicionales, que permitan suplir las necesidades al momento de presentarse un incidente.

Es necesario que la institución cuente con sistemas contra incendios, así como detectores de humo, entre otros. Lamentablemente la infraestructura del U.T.C., no presta las facilidades, dependiendo de la ubicación de los equipos de computación y por la falta de acondicionamiento de las instalaciones.

3.6.2.4. Infraestructura Eléctrica

La infraestructura eléctrica es un punto importante a tomar muy en cuenta, utilizar equipos electrónicos implica trabajar con electricidad, por tanto es una de las principales áreas a considerar en la seguridad física.

A medida que los sistemas se vuelvan más complejos, hace necesario la presencia de un especialista para evaluar los

---

[1]"Agua," *Enciclopedia Microsoft® Encarta® 2000.* © 1993-1999. Reservados todos los derechos.

riesgos particulares y buscar soluciones que estén de acuerdo con norma de seguridad industrial. La infraestructura eléctrica de la U.T.C., debe enmarcarse en parámetros de calidad sobre la base de estabilidad, valores mínimos, nivel de ruido eléctrico porque se maneja datos y voz por el cableado.

A continuación se muestran parámetros que permitan garantizar un buen suministro de energía eléctrica, a los diferentes circuitos eléctricos y electrónicos.

3.6.2.4.1. Instalaciones Eléctricas

Las inspecciones deben realizarse periódicamente, con el fin de comprobar la resistencia y las conexiones. Pero antes de la revisión del sistema eléctrico, debe realizarse una inspección visual del sistema, a veces los problemas se suelen detectar a simple vista, de no ser así hace necesario la revisión del sistema eléctrico.

Polaridad de Tomacorrientes

Todo objeto que necesite de energía eléctrica debe acceder a un tomacorriente que cumpla:

- Tres ranuras (fase, neutro, tierra).
- Correctamente polarizadas (lámpara de neón solo enciende entre fase/tierra y fase/neutro) ver Figura 3.19.

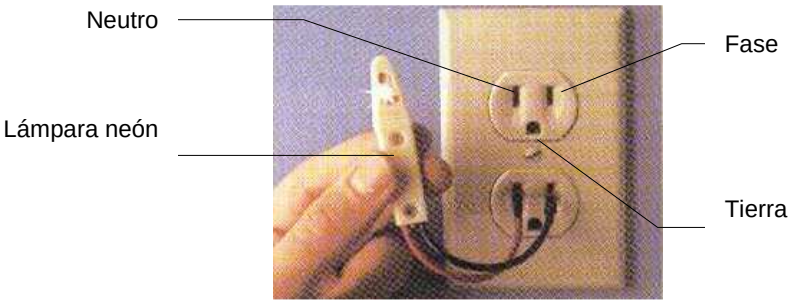


Figura 3.20 Polaridad en Terminales Tomacorriente

Medición de Voltajes

Para la medición de voltajes hay que cumplir con los siguientes parámetros :

- Multímetro digital/analógico o voltímetro de AC (corriente alterna).
- Lectura voltaje entre neutro y tierra debe ser menor a 5 VAC.
- Lectura voltaje entre fase y neutro debe ser menor a 117 VAC.
- Lectura voltaje entre fase y tierra debe ser menor a 114 VAC.

La forma como se realiza estos tipos de mediciones de voltaje se puede observar en la Figura 3.21.

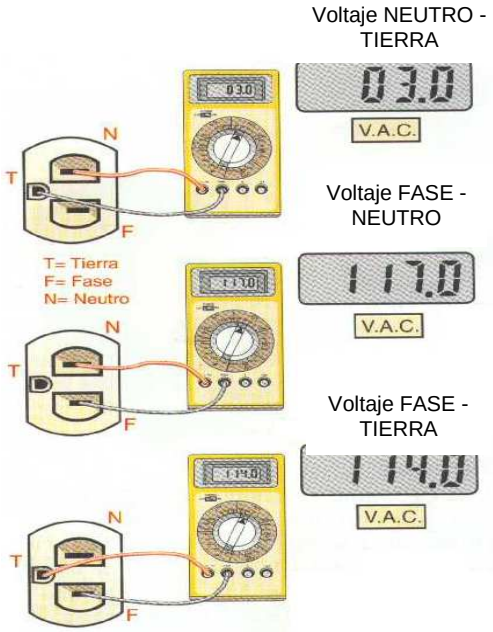


Figura 3.21 Medición de Voltajes

3.6.2.4.1.1. Caídas y Subidas de Tensión

Sin una buena línea de alimentación y los dispositivos adecuados; los sobrevoltajes o caídas de tensión de línea pueden ocasionar daños irreparables en nuestros equipos y la información que en ellos se procesan y almacenan.

En la Figura 3.21 se puede ver como el sistema de cómputo accede al sistema de red eléctrico.

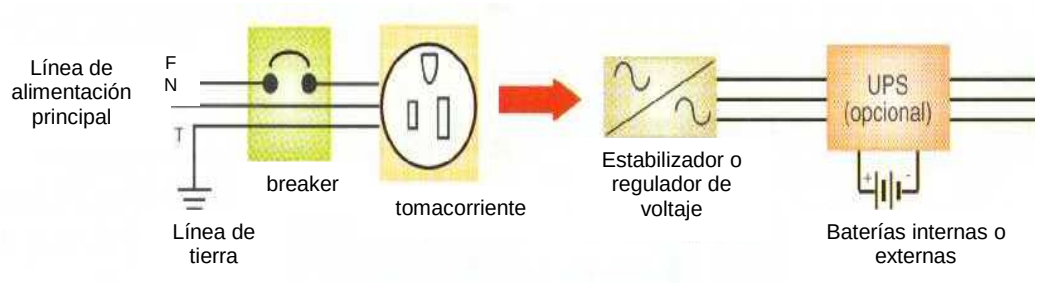


Figura 3.22 Diagrama de Conexión del Sistema

En la Figura 3.22 se puede observar la forma correcta de conexión de los diferentes elementos de protección de un sistema de cómputo o de un objeto electrónico cualquiera:

a. Línea de alimentación principal
b. Línea de tierra
c. Estas tienen que estar conectadas al breaker
d. Tomacorriente
e. Estabilizador o regulador de voltaje
f. Opcionalmente puede utilizarse un UPS si desea proteger la información.

He ahí la importancia de asegurar nuestros equipos de computación con los respectivos dispositivos de protección, que aseguren la

estabilidad de los equipos existentes en la universidad, por tal razón depende de la elección de tener una buena instalación y protegerlos.

3.6.2.4.2. Instalación a Tierra

Conocida también como toma de tierra, denominando a la comunicación entre un circuito eléctrico y el suelo natural para dar seguridad a las personas, equipos protegiendo de los posibles peligros, procedentes de una rotura del aislamiento eléctrico.

La instalación a tierra juega un papel importante, mantiene protegido los equipos asegurando la estabilidad de los procesos que normalmente se realizan.

En este caso, los materiales que se utilizan para la instalación de línea a tierra son:

- Una varilla de cobre sólido
- Un conector de cobre

- Alambre AWG 10 ó 12 o superior dependiendo de la cantidad de elementos que se conecte al sistema.
- Limadura de hierro
- Carbón mineral
- Sal
- Agua, dependiendo de la humedad del terreno.

En la siguiente Figura se indica el esquema de una instalación a tierra como se muestra:

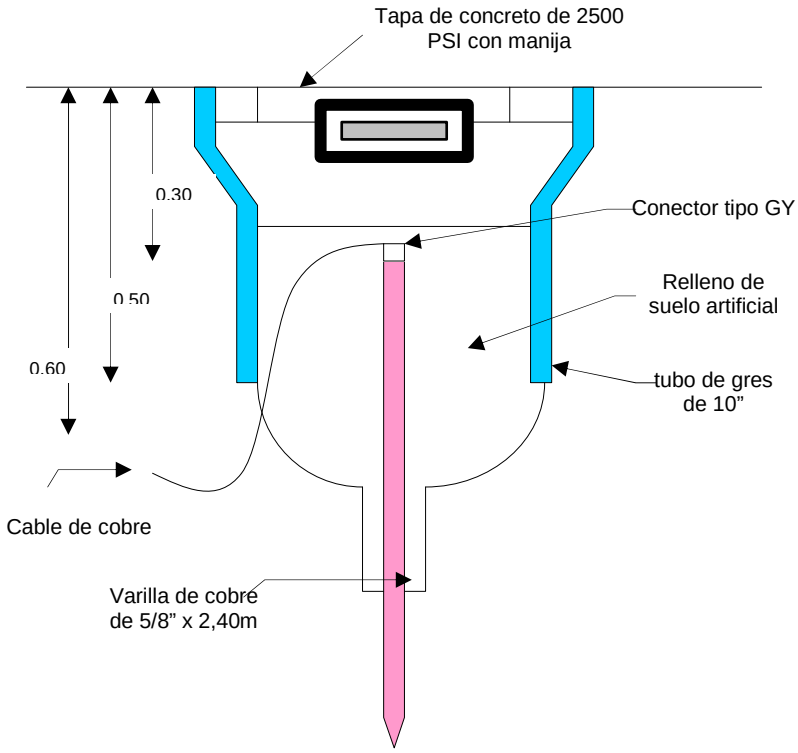


Figura 3.23 Diagrama de Conexión a Tierra

Funciones.- La toma a tierra cumplirá las siguientes funciones:

- Proteger a las personas, neutralizando la tensión, respecto a tierra que puedan alcanzar las masas metálicas.
- Para salvaguardar a personas, equipos y materiales con alcance de descargas eléctricas. Asegurando la actuación de los dispositivos de protección tales como, pararrayos, descargadores eléctricos, líneas de energía eléctrica o similares, así como interruptores diferenciales.
- Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.
- Aterrizaje de las interferencias y el ruido.
- Aterrizaje de la carga estática.
- Alta capacidad de conducción y disipación de corriente.
- Permitir a los equipos de protección eliminar rápidamente las fallas.

Las nuevas tecnologías reemplazan los materiales que se utilizan para mejorar la resistividad del terreno con

componentes llamados suelos artificiales optimizando la línea a tierra.

En el país lamentablemente no existe una cultura de seguridad, debido al alto costo que esto representa, es así que al momento de diseñar el/los planos arquitectónicos e instalaciones eléctricas se hace caso omiso, solo se realiza el cableado de la fase y neutro dejando a un lado la tierra, sin saber la importancia que tiene.

Otra situación que comúnmente se da al momento de adquirir algún equipo electrónico, este viene con sus tres patillas y necesita de un tomacorriente con conectores hembra para conectar el equipo electrónico ver Figura 3.24.

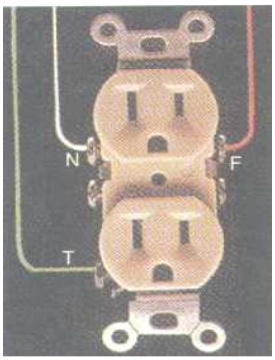


Figura 3.24 Conexión Correcta de Terminales

Existen ciertas costumbres que no son las adecuadas al momento de utilizar la energía eléctrica, entre ellas.

- Se corta el terminal a tierra, solo funciona el terminal neutro y fase.
- Se utiliza adaptadores que permitan introducir el conector al tomacorriente.
- En otras situaciones se liman dichos conectores, por las consecuencias anómalas de los conectores hembra del tomacorriente que no son los adecuados.

En la Figura 3.25 se muestra lo que no se aconseja realizar.

Figura 3.25 Lo que no se Debe Realizar

El equipo al conectar de esta forma funciona pero tarde o temprano será preso de las altas o bajas de tensiones, peor aún si no se dispone de un estabilizador de energía.

En la siguiente Figura se muestra la forma correcta que se debería tener el cableado eléctrico y los toma corrientes.

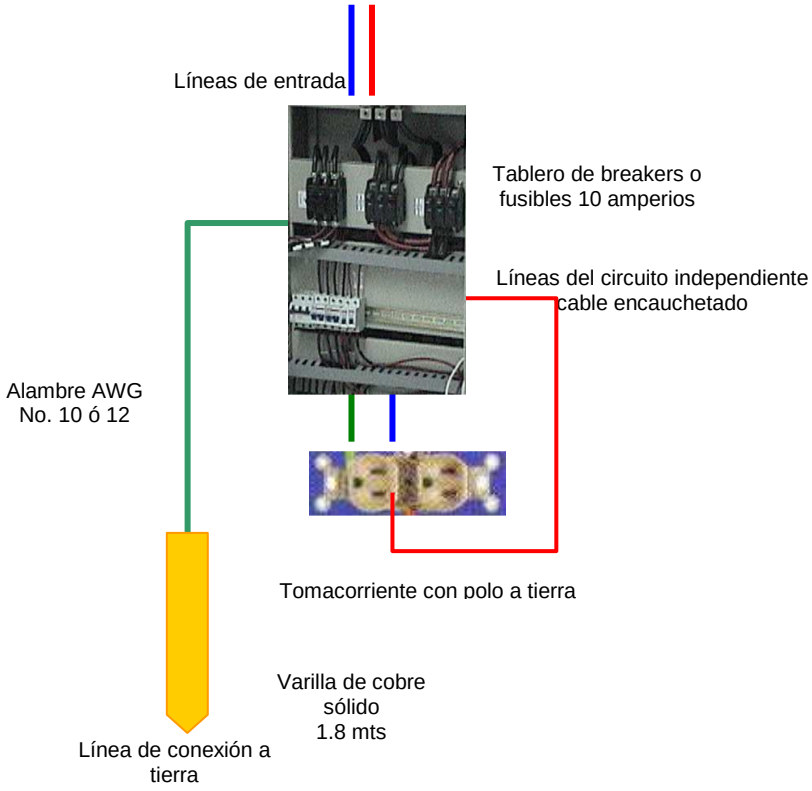


Figura 3.26 Forma Correcta de un Cableado Eléctrico

Hay situaciones en la que una línea a tierra no se puede realizar, este es el caso de un edificio ya construido, incluido la universidad que la aventaja, estar situados los laboratorios en la planta baja donde se puede realizar una instalación a tierra, en cambio las secretarias de carreras se encuentra en la plata alta, para realizar la instalación a tierra de los equipos que se

encuentran en dicha planta, pero no se puede realizar lo siguiente:

- Buscar una columna y perforar hasta encontrar la estructura metálica o una varilla, estas van directamente al suelo. Y realizar la conexión del cable de cobre a dicha varilla, de esta forma quedará aterrada el sistema.
- Otra solución es realizar la conexión de tierra a la cañería de abastecimiento de agua de la infraestructura sanitaria del edificio, de esta forma quedaría aterrada el sistema.
- Buscar el camino más cercano y hacer la conexión a tierra a fin de encontrar un mejor servicio para que los equipos funcionen de mejor manera en toda su capacidad.
- Pudiéndose verificar la instalación a tierra, con la utilización de un voltímetro o un amperímetro.

Fusibles

Al sufrir un incremento de la intensidad eléctrica puede dañarse el circuito del equipo, pero gracias a los

fusibles o diferenciales esto no sucede en la mayoría de los casos, estos dispositivos están diseñados para interrumpir un circuito si se sobrecargan.

El fusible al fundirse será sustituido, mientras que un diferencial debe ser restaurarado tras saltar. Para que no suceda esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme.

Cuando se sustituya cualquiera de estos dispositivos del equipo, se debe realizar con mucho cuidado y tomar todas las precauciones y medidas del caso, a continuación se detalla:

- Verificar que estén apagados y desconectados los equipos y cables de poder.
- Tener cuidado con las descargas electroestáticas.
- Tener precaución con las piezas que se retiren del equipo.
- Al momento de cambiar algún elemento del monitor, tomar la medidas correspondientes, porque posee un alto voltaje incluso, después de haberse apagado.

- Antes de volver a encender el equipo verificar que los elementos cambiados esté en el lugar respectivo y que no exista ningún tipo de material, que podría provocar un corto circuito.

Extensiones Eléctricas y Capacidades

Las computadoras personales a veces ocupan todas las tomas de corrientes. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar, algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado por los responsables de las oficinas. No sólo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. Aparte del daño físico que puede provocar engancharse repentinamente con el cable, se trata de una forma rápida y poco agradable de desconectar un sistema completo. El la Figura 3.27 se muestra un ejemplo que la universidad mantiene al momento una telaraña de cables.

Figura 3.27 Extensiones Eléctricas

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

- Utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
- Las canaletas sirven como aislante, es decir no polariza al conductor, sea cual sea la red o instalación.
- No encadenar sucesivos múltiples, esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Utilice los enchufes de pared siempre que sea posible.
- Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas

- Compruebe siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esta cifra el amperaje total de todos los aparatos conectados a ellas.
- Adquiera toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndricas.

3.6.2.4.3. Aire Acondicionado

Un sistema de aire acondicionado consiste teóricamente en un conjunto de equipos que proporcionan aire y mantienen el control de su temperatura, humedad y pureza en todo momento y con independencia de las condiciones climáticas.[2]

El aire acondicionado se emplea para impedir que el aire de un edificio se caliente o humedezca demasiado. Se consideran que son sistemas bastante complejos, por lo que suelen instalarse durante la construcción del edificio. En el gráfico siguiente se muestra un aire acondicionado.

---

[2]"Calefacción, ventilación y aire acondicionado," *Enciclopedia Microsoft® Encarta® 2000.*

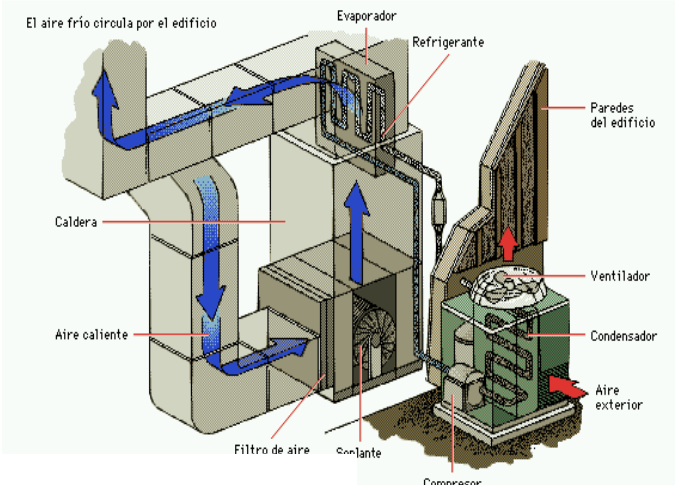


Figura 3.28 Esquema de un Aire Acondicionado

Problema:

- Lamentablemente la institución no cuenta con un aire acondicionado que permita mantener una temperatura idónea para los equipos de cómputo.
- Pero aún si se pudiera adquirir un aire acondicionado para el centro de datos se tendría que realizar mucha obra de ingeniería civil, teniendo en cuenta que la infraestructura no es la idónea para instalar un aire acondicionado.
- Todo esto conlleva a un alto costo tanto en la adquisición de aire acondicionado y su instalación así como en la obra de ingeniería

civil. Sin olvidar el beneficio que tendría el aire acondicionado frente al costo que representa si los equipos del centro de datos llegan a sufrir daños por cambios de temperatura.

Solución:

- La solución es la adquisición del un aire acondicionado que permita regular la temperatura y mantener la estabilidad de los equipos.
- Del análisis costo – beneficio sin duda sobresale el beneficio, es necesario realizar la obra de ingeniería, no sería correcto cambiar de lugar el centro de datos, debido que esta contemplado en las nuevas edificaciones de la U.T.C.
- De darse la adquisición del equipo, no existiría el espacio físico para su instalación por lo que se tendría que construir nuevas instalaciones para colocar el aire. El equipo debe tener proyecciones con las nuevas edificaciones, de manera que este recurso no se desperdicie.

- Buscar el equipo que pueda sustituirle al aire acondicionado, de esta manera dar más años de vida a los equipos existentes.

3.6.2.4.4. UPS (Sistema de Energía Ininterrumpible)

Un UPS, es un dispositivo de protección que sirve para sostener la energía eléctrica por un determinado tiempo cuando esta deja de fluir. En el momento que el voltaje de la red eléctrica falta, el UPS hace el cambio casi en forma instantánea para seguir suministrando a partir del juego de baterías. El tiempo de suministro de la tensión desde un UPS debe ser lo suficiente que permita salvar la información que se estaba procesando y apagar el equipo en forma correcta.

Problema:

- Uno de los principales problemas que tiene el centro de datos es la falta de capacidad para cubrir los laboratorios de computación y de los periféricos que necesitan de alimentación eléctrica en el momento que se produzca un corte de energía.

- Otra problema. es la falta de conocimiento de las características técnicas del UPS, lo que ha llevado a la sobrecarga del sistema de energía ininterrumpible.
- Además el UPS se encuentra junto a los breaks que no se encuentra protegido con su respectiva tapa, lo que podría conllevar a producir chispa ocasionando un incendio o un corte del cableado eléctrico que afectaría al UPS.
- Es importante señalar que al poseer un UPS parte de la iluminación del centro de datos debe estar conectada al UPS para que proporcione iluminación cuando se produzca un corte de energía eléctrica.
- En el siguiente gráfico se muestra el UPS de la U.T.C. y la sobre utilización del mismo.

Figura 3.29 UPS de la U.T.C.

Solución:

Es importante seleccionar un UPS que cumpla con ciertos factores que a continuación se señala:

- El UPS existente en la universidad, tiene que estar separado de esa instalación eléctrica y tener una conexión a tierra. Comprobando la capacidad de KVA que soporta el UPS, para ello recordemos que un CPU, monitor e impresora aproximadamente ocupan 0.4 KVA, si se tratan de impresoras de trabajo pesado se debe ver el detalle técnico de cuantos voltios ocupa y ver si el UPS soporta su conexión. Por lo general las impresoras de trabajo pesado, escáner no se conectan al UPS, necesitan de un regular individualizado .
- Requerimiento de frecuencia
- Tiempo de respaldo requerido
- Futuras Expansiones
- Picos por corriente de arranque
- Servicio de Mantenimiento
- Soporte Técnico (antes, durante y después de la instalación)

- Instalar una línea de tierra a la fuente de alimentación.
- Se considera que una parte de la iluminación debe estar conectada al UPS, por lo que sus requerimientos de potencia aumentarán.
- La tecnología del UPS tendrá que ser la apropiada para que cubra los requerimientos y necesidades de la institución. Y para ello se tiene:

  - OFF-LINE, STAND BY (fuera de línea)
  - LÍNEA INTERACTIVA
  - TRUE ON-LINE (en verdadera línea)

  Siendo uno de los más apropiados el UPS on-línea que brinda todas las características necesarias para la institución.

3.6.3. Otros Tipos de Desastres

Antes de comenzar a hablar de otros tipos de desastres que pueden suceder, se establece una lista de las amenazas endógenas y exógenas que a continuación se muestra en la siguiente Tabla 3.13.

AMENAZA	ACTIVIDAD	
	TIPO	OCURRENCIA
Endógenas	Fuga de producto	X
	Incendio o explosiones	X
	Derrumbes	X
Exógenas	Sismos	X
	Inundaciones	X
	Tormentas	X
	Deslizamientos	X
	Atentados	X

Tabla 3.13 Escenarios de Emergencia

Luego de definir esta lista de sucesos se toma en cuenta las probabilidades de ocurrencia de los mismos.

PROBABILIDAD	DEFINICIÓN	OCURRENCIA DE EVENTO	PUNTAJE
Frecuente	Posibilidad de ocurrencia alta. Sucede en forma reiterada	1 al mes	6
Moderado	Posibilidad de ocurrencia mediana. Sucede algunas veces	1 entre 6 y 12 meses	5
Ocasional	Posibilidad de ocurrencia limitada. Sucede pocas veces	1 entre 1 a 5 años	4
Remoto	Posibilidad de ocurrencia baja. Sucede en forma esporádica	1 entre 6 a 10 años	3
Improbable	Posibilidad de ocurrencia muy baja. Sucede en forma excepcional	1 entre 11 a 19 años	2
Imposible	De difícil posibilidad de ocurrencia. No a sucedido hasta ahora.	1 en 20 años o más	1

Tabla 3.14 Probabilidad de los Siniestros

Fuga de Material / Producto.

Es la salida incontrolada de producto desde la infraestructura empleada para su transporte. Las fugas se presentan por procedimientos operacionales inadecuados, errores humanos o accidentes, daños, deterioro, o acción de terceros que provoquen la

rotura total o parcial de los componentes empleados para el transporte del producto.

La probabilidad de que ocurra una emergencia en este escenario es remota, pero no hay que menospreciarlo debido a que la tubería del oleoducto pasa por ese sector.

Incendios o Explosiones

Un incendio se define como un fuego incontrolado o un proceso de combustión sobre el cual se ha perdido el control. Pero la ocurrencia de un incendio durante el desarrollo de las actividades normales es consecuencia de una fuga incontrolada del producto; algún incidente o atentado, la probabilidad de este tipo de evento es ocasional, y de ocurrir es únicamente responsable el encargado quien vigila o la manera de actuar frente ha esta situación.

Derrumbes

Puede provocar derrumbes por la inestabilidad de laderas naturales y taludes de corte. La probabilidad para que este escenario suceda, es improbable debido a que la institución no se encuentra rodeado por laderas cercadas que amerite este evento. Dejando claro que

esta posibilidad queda descartada, sin dejar olvidado una mínima posibilidad que se produzca y que hacer en esta situación

Sismos

Son movimientos de la corteza terrestre causados por fenómenos naturales como las fallas geológicas activas, la acomodación de placas tectónicas, y, la acumulación de energía por el movimiento relativo de las mismas.

La probabilidad para que éste fenómeno natural se dé, es porque se encuentra en una zona con alto nivel sísmico. La probabilidad de este tipo de evento es moderado.

Inundaciones

Son el cubrimiento de un terreno con cantidades anormales de agua producto de una precipitación abundante (crecidas o torrentadas) o el desbordamiento de un cuerpo de agua cercano.

La probabilidad de este escenario es muy probable debido a que el sistema de alcantarillado del sector es muy deficiente, por lo que las características de torrencialidad infieren una probabilidad

moderada, la universidad es vulnerable y la precaución es la alternativa para no tener que lamentar.

Tormentas Eléctricas

Una tormenta eléctrica es el resultado de una combinación de fenómenos atmosféricos los cuales generan descargas eléctricas inesperadas.

La universidad no es la excepción por características climáticas del área que nos rodea, la probabilidad de ocurrencia de una emergencia por una tormenta eléctrica es remota.

Deslizamientos

Para efectos de este análisis se asumirán como deslizamientos los movimientos del terreno causados por factores exógenos, tales como las altas precipitaciones que favorecen la reactivación de flujos de tierra.

Los deslizamientos por causas naturales pueden darse por precipitaciones fuertes y por el tipo de terreno en el que se encuentra la universidad. Afortunadamente no se encuentra rodeado por edificaciones o elevaciones que causen este tipo de

riesgo, se puede decir, que se tiene una probabilidad de ocurrencia remota.

Atentados

Son actos irregulares, efectuados por personas o grupos que actúan al margen de la ley.

El Alma Mater es un centro de alto nivel educativo, que está al servició de la sociedad, ningún atentado es factible. Salvo el caso de aquellas personas con mentalidad distorsionada que procuran hacer daño al prójimo. Se considera una probabilidad de ocurrencia improbable.

TIPO	TIPO	PROBABILIDAD
Fuga de material / producto	Remota	3
Incendio o explosiones	Ocasional	4
Derrumbes	Improbable	2
Sismos	Moderado	5
Inundaciones	Moderado	5
Tormentas eléctricas	Remota	3
Deslizamientos	Remota	3
Atentados	Improbable	2

Tabla 3.15 Probabilidad de los Siniestros de La UTC

3.6.3.1. Factores de Vulnerabilidad

Los factores de vulnerabilidad dentro de un análisis de riesgos, permite determinar cuales son los efectos negativos,

que sobre un escenario y sus zonas de posible impacto pueden tener los eventos que se presenten.

Para efectos del análisis de riesgo de las instalaciones que manejan la institución, se consideran los siguientes factores de vulnerabilidad:

Víctimas: Se refiere al número y clase de afectados (empleados, personal de emergencia y la comunidad); considera también el tipo y la gravedad de las lesiones.

Daño Ambiental: Incluye los impactos sobre cuerpos de agua, fauna, flora, aire, suelos y comunidad a consecuencia de la emergencia.

Pérdidas Materiales o Económicas: Representadas en instalaciones, equipos, valor de las operaciones de emergencia, multas, indemnizaciones, y atención médica entre otros.

Imagen Empresarial: Califica el nivel de deterioro de la imagen corporativa de la empresa a consecuencia de la emergencia, en este caso de la universidad.

Suspensiones: Determina los efectos de la emergencia sobre el desarrollo normal de las actividades de la institución en términos de días perdidos.

FACTOR DE VULNERABILIDAD	CALIFICACIÓN DE GRAVEDAD			
	INSIGNIFICANTE	**MARGINAL**	**CRÍTICA**	**CATASTRÓFICA**
	1	**2**	**3**	**4**
Victimas	No hay lesiones o no se requiere atención hospitalaria	Lesiones leves que requieren atención	Lesiones con necesidad de hospitalización	Muerte
Daño ambiental	No hay impactos ambientales significativos	Impactos ambiental dentro del área de escenario de emergencia	Impacto en las áreas aledañas al escenario	Impactos con consecuencia sobre la comunidad
Perdidas materiales o económicas			No se puede determinar	No se puede determinar
Imagen empresarial	Conocimiento interno	Conocimiento local	Conocimiento nacional	Conocimiento internacional
Suspensiones			No operatividad	No operatividad

Tabla 3.16 Factores de Vulnerabilidad y sus Consecuencias

Por esta razón es muy importante realizar un listado de las dependencias e instituciones que pueden brindar su apoyo de inmediato y ayudar a mitigar las eventualidades que se presente.

Pero al acudir a estas instituciones en caso de emergencias en ciertos períodos del año es necesario realizar simulacros, para estar en condiciones en caso de suceder alguna eventualidad.

INSTITUCIÓN/EMPRESA	LUGAR	TELÉFONO OFICINA
Cruz Roja	Av. Amazonas s/n	811 / 400
Defensa Civil	Gral. Maldonado 507	810 /148
Policía	Latacunga (San Martín)	812 / 666
Bomberos	Sánchez de Orellana s/n	813 / 520
Hospital General	Hnas. Páez entre la 2 de mayo y Av. Amazonas.	800 / 331
Clínica Latacunga	Sánchez de Orellana 66107	811/ 5 85
Clínica Continental	Conti Clínica SA. R. Romero y Cordero y A. Silva	804 / 805 804 / 807
Clínica Santa Cecilia	Amazonas 7915 Av. Amazonas s/n	811 / 564
Clínica los Andes	Av. 5 de Junio 662 y Amazonas	807 / 130

Tabla 3.17 Lugares donde Acudir en una Emergencia