ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE INGENIERÍA

DISEÑO DE UN SISTEMA DE SEGURIDAD FÍSICA PARA LA EPN

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

EDWIN GIOVANNY CÓNDOR GORDÓN

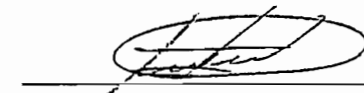
DIRECTOR: ING. NELSON AVILA

Quito, Septiembre 2005

DECLARACIÓN

Yo, Cóndor Gordón Edwin Giovanny, declaro que el trabajo aquí realizado es de mi auditoria; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

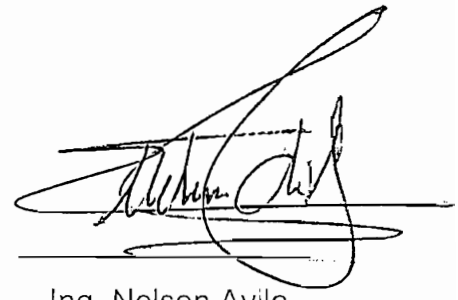
La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la ley de la propiedad intelectual, por su reglamento y por la normativa institucional vigente.



Cóndor Gordón Edwin Giovanny

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Cóndor Gordón Edwin Giovanny, bajo mi supervisión.



Ing. Nelson Avila

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Agradezco a Dios por haberme brindado la oportunidad de cumplir este pequeño sueño.

A todas las personas que pusieron su confianza en mi persona, principalmente a mi familia, amigos, vecinos y conocidos.

A los profesores que me guiaron para ayudarme a descubrir las capacidades que Dios me obsequio para poder alcanzar los sueños que un día tuve.

Al Ing. Nelson Avila, por haber sido un excelente profesor y un amigo, el cual me extendió su mano cuando más lo necesitaba.

A los Ingenieros: Pablo Hidalgo, Soraya Sinche, María Soledad Jiménez, Fernando Flores, Bolivar Ledesma, Iván Bernal, Fabio Gonzáles, Nelson Avila, por haber compartido sus conocimientos de una manera desinteresada.

Mis más sinceros reconocimientos a todas las personas que hicieron que este trabajo pudiera concluirse.

'' Las personas justas caen seis veces y se levantan siete, que clase de persona eres tú''

Edwin Cóndor

DEDICATORIA

A los cuatro pilares de mi vida; mi Madre Mery Gordón, mi Hermano Juan Cóndor, mi Abuelita Josefina Cadena y mi Amiga Juliana Córdova, quienes han llorado mis derrotas y han festejado mis triunfos, July hagamos realidad nuestros sueños se que podemos lograrlo.

'' La piedra que un día despreciaron los constructores es ahora la piedra angular, ésa es la voluntad de Dios''

CONTENIDO

INDICE DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

INDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

RESUMEN

En toda empresa o institución, la seguridad informática tiene una gran importancia, para obtener ventajas competitivas y para mantener la confianza en la misma, para cumplir con dichos objetivos se tienen diferentes mecanismos, tanto físicos como lógicos, el presente proyecto de titulación cubre una pequeña parte de estos mecanismos como es el control de acceso físico a lugares donde se mantienen activos de importancia para las instituciones públicas, privadas o entidades educativas y de investigación, en este caso la Escuela Politécnica Nacional.

Un sistema de control de acceso físico debe permitir el ingreso y salida de personal autorizado, además debe detectar y prevenir la salida de equipos sin autorización, siendo de fácil uso para las personas, ya que de nada serviría el mejor sistema de control de acceso físico si las personas no entienden el funcionamiento del mismo o simplemente lo rechazan. Para evitar estos problemas se debe explicar a las personas los beneficios que se obtienen si se utiliza adecuadamente el sistema implementado.

En el presente proyecto de titulación se ha realizado un análisis sobre los riesgos que actualmente tiene la institución para poder determinar los problemas que deseamos solucionar y definir los objetivos para cumplir con dichos propósitos. Del análisis realizado se ha podido definir, que el principal problema que tiene la Universidad es el acceso no autorizado de las personas hacia cada una de las localidades, lo cual trae como consecuencia una pérdida notable de la credibilidad de la institución.

Para solucionar este problema se propone un sistema de control de acceso físico, dividiendo el requerimiento en dos niveles de seguridad, un nivel de seguridad alto y un nivel de seguridad medio. Para definir el nivel de seguridad a ser implementado en cada una de las localidades se ha tomado en cuenta como criterios de diseño: el valor de los activos existentes y el tipo de información que existe en cada una de ellas.

Se utilizarán lectores de tarjetas de proximidad para autenticar a las personas que deseen ingresar a un área que tenga un nivel de seguridad medio, y se utilizará un lector biométrico basado en la geometría de la mano para autenticar a las personas que deseen ingresar a un área que tenga un nivel de seguridad alto, por ejemplo el centro de cómputo general.

Una vez definidos los mecanismos a ser utilizados para cumplir con el objetivo planteado se realiza un análisis técnico económico de tres diferentes propuestas de sistemas de control de acceso existentes en el país, del análisis realizado se propone la utilización del sistema de control de acceso de la empresa NORTHERN COMPUTERS por presentar la mejor opción. Luego de haber seleccionado los productos existentes en el mercado para cumplir con dicho objetivo se realiza el diseño de: control de acceso vehicular al campus Politécnico, control de acceso al centro de cómputo general y el sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica; además se presenta el diseño del sistema de alimentación eléctrico y de redundancia de energía, el diseño del sistema de puesta a tierra para proteger los equipos a ser utilizados y se presenta una opción de un sistema de respaldo de transmisión de información entre cada una de las diferentes redes de control de acceso locales con el punto de concentración, mediante la utilización de un sistema de acceso inalámbrico.

Uno de los principales problemas que tiene la Universidad, es que muchos de los proyectos que se realizan para solucionar los problemas que afectan a la misma quedan solamente como estudios, por lo que se propone la utilización de un tipo de financiamiento para que el proyecto se pueda ejecutar. En la propuesta realizada se sugiere la realización en una primera etapa del sistema de control de acceso vehicular en conjunto con el sistema de control de acceso del centro de cómputo general, luego de lo cual se puede continuar con la implementación de los sistemas de control de acceso físico de las demás facultades.

Otro problema que se ha visto en el estudio realizado, es que no existe un control adecuado sobre el ingreso y salida de los equipos de cada uno de los laboratorios y en si de toda la Universidad, por lo cual se propone la realización de

forma inmediata de un inventario de todos los equipos que se encuentran en la Universidad por parte del departamento de control de bienes de la Universidad. Posteriormente, el encargado de cada una de las localidades deberá llevar un registro de todos los objetos que ingresan y salen de cada una de las localidades.

Un sistema de control de acceso físico debe estar basado sobre las políticas, procedimientos y estándares adecuados a la realidad de la institución, las mismas que deberán ser conocidas por toda la comunidad politécnica. Dichas políticas deben ser definidas por un organismo, que estará conformado por un grupo pequeño de personas, para agilitar la definición de las mismas, y que representa a toda la comunidad politécnica, y están en la obligación de difundir continuamente las políticas y despejar las inquietudes de las personas que hagan consultas.

Las políticas de seguridad deben seguir un proceso de afinamiento continuo de acuerdo a las necesidades que se vayan presentando.

Este proyecto de titulación propone políticas y procedimientos de seguridad para mejorar el sistema de control de acceso físico propuesto.

PRESENTACIÓN

El principal problema que asecha a la Politécnica, es el ingreso no autorizado de personas hacia localidades que contienen activos de suma importancia para la institución. El presente proyecto de titulación propone la implementación de un sistema de control de acceso físico, basado en la utilización de tarjetas de proximidad y en la utilización de lectores biométricos basados en la geometría de la mano como mecanismos de autenticación, además se proponen políticas para mejorar el sistema de control de acceso físico.

Para cumplir con el objetivo propuesto "DISEÑO DE UN SISTEMA FÍSICO PARA LA EPN" se ha organizado este documento en cinco capítulos con los contenidos que se presentan a continuación:

En el CAPÍTULO 1 se realiza un análisis sobre la situación actual de la politécnica en relación al control de acceso físico en cada uno de los laboratorios del edificio antiguo de la ex facultad de Ingeniería Eléctrica, el centro de cómputo general y el acceso vehicular, además se realiza un análisis de riesgos para determinar los problemas de los cuales nos queremos proteger, los mismos que son utilizados para determinar los objetivos para cumplir con dichos propósitos.

En el CAPÍTULO 2 se realiza una breve descripción sobre los métodos utilizados en la actualidad para realizar la autenticación de las personas cómo: passwords, tarjetas magnéticas, tarjetas de proximidad y lectores biométricos, además se realiza una breve descripción sobre los métodos de encripción. Una vez definido el tipo de tecnología a utilizarse se realiza el análisis sobre tres diferentes propuestas, este análisis es utilizado para determinar la mejor opción la misma que se adapta a la mayor cantidad de necesidades de la EPN.

En el CAPÍTULO 3 se realiza la descripción en detalle sobre la solución planteada, la misma que contiene, diseño del sistema de seguridad físico, diseño del sistema de alimentación eléctrico y de redundancia de energía para el sistema

de control de acceso, diseño del sistema de puesta a tierra para proteger los elementos que intervienen en el sistema de seguridad y diseño de un sistema de redundancia de transmisión de datos entre cada uno de las redes de control de acceso local y el punto de concentración. Además éste capítulo contiene un análisis de costos sobre la solución propuesta.

En el CAPÍTULO 4 se presenta una breve descripción sobre la importancia de las políticas de seguridad en todo sistema, y se procede con la descripción de las políticas de seguridad propuestas para mejorar el sistema de control de acceso físico en cada una de las localidades.

Finalmente en el CAPÍTULO 5 se presentan las conclusiones y recomendaciones que han sido fruto del estudio realizado.

Confío que el estudio presentado sirva de alguna manera para incrementar los niveles de seguridad física existentes actualmente en la Universidad, y que este proyecto no quede únicamente en papel cómo han quedado otros estudios.

El autor

1 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EPN

1.1 DESCRIPCIÓN GENERAL

El presente proyecto de titulación se ha realizado pensando en la importancia que tiene en la actualidad la seguridad informática en toda empresa o institución, este proyecto cubre una pequeña parte dentro de este gran conjunto que comprende la seguridad informática como es el control de acceso físico a lugares donde se mantienen activos de suma importancia para las instituciones públicas, privadas o entidades educativas y de investigación, como es el caso de la Escuela Politécnica Nacional.

Muchas veces nos imaginamos que los ataques pueden venir de personas ajenas a la institución, sin tomar en cuenta que los ataques más peligrosos pueden venir de personas que pertenecen a la institución, aunque éstos son los más difíciles de detectar, debido a que las personas que trabajan en la institución tienen acceso a recursos de la misma en una forma casi ilimitada, adicionalmente estas personas pueden servir de conexión a otras en el exterior que buscan ganar acceso a la información o activos de la institución.

En un entorno universitario como el de la E.P.N., los estudiantes, profesores, personal administrativo y en general todas las personas que de una u otra forma interactúan de manera directa o indirecta con la universidad, miran la necesidad de tener una infraestructura de control de acceso robusta con políticas de acceso adecuadas de acuerdo a las necesidades de cada grupo de personas. Por ejemplo, a nadie le gustaría que una persona desconocida ingrese a su casa y hurte algo de su propiedad, así en el caso de la E.P.N. se debe proteger lugares donde se tienen activos críticos, como por ejemplo las bodegas del laboratorio de automatización de la carrera de Ingeniería en Electrónica y Control, o lugares donde se almacena información importante para la universidad como es el caso del centro de cómputo general.

Un sistema de control de acceso debe integrar: personas, procedimientos e infraestructura para poder proteger activos y lo más importante la seguridad física de las personas. Este control se lo realiza para evitar que personas maliciosas traten de hacer daño, permitiendo sólo el ingreso de personas autorizadas a las instalaciones y rechazando a personas no autorizadas. [3]

Entre los principales objetivos de un sistema de control de acceso utilizado para la protección física se pueden mencionar:

- Permitir el ingreso y salida de personal autorizado.
- Detectar y prevenir la entrada o salida de materiales de contrabando [a]
- Proveer información para la seguridad personal.

Además, estos sistemas deben ser de fácil uso para las personas, deben ser seguros y con una probabilidad de fallo muy baja. Estos sistemas deben combinarse con otros como por ejemplo circuitos cerrados de televisión, para poder actuar inmediatamente cuando está ocurriendo una situación no deseada. Cabe recalcar que ningún sistema es 100% seguro, lo que se trata es de disminuir la probabilidad de que una situación no deseada ocurra, para lo cual se debe indicar claramente a las personas que estarán interactuando directamente con el sistema las ventajas que se obtendrán con la correcta utilización del mismo. Como se mencionó anteriormente un sistema de control de acceso integra: personas, procedimientos y equipos, es vital la correcta integración de estos tres componentes para que el sistema funcione adecuadamente, los tres elementos antes mencionados se los considera de igual importancia.

El presente proyecto tiene como principal objetivo plantear un sistema de control de acceso físico en el edificio antiguo de la ex Facultad de Ingeniería Eléctrica, los cinco puntos de acceso vehicular al campus politécnico y el centro de cómputo general, los mismos que servirán de guía para que las demás Facultades implementen sistemas similares.

[a] Los materiales de contrabando son considerados como objetos que sirven para producir un ataque potencial como por ejemplo, armas, explosivos, etc. [3].

Para cumplir con el objetivo propuesto, se realiza una exposición en detalle del diseño propuesto, el mismo que incluirá:

- Diseño eléctrico y de respaldo de energía para los diferentes dispositivos de control de acceso.
- Interconexión de los diferentes mecanismos de control de acceso.
- Requerimientos mínimos necesarios para el software de administración del sistema, el mismo que tratará de ajustarse a los problemas detectados.
- Análisis de costos de la solución propuesta.

Adicionalmente se definirán políticas de seguridad referentes al control de acceso físico en los diferentes puntos antes mencionados.

1.2 LEVANTAMIENTO DE LA INFORMACIÓN

1.2.1 INTRODUCCIÓN

La EPN es una universidad pública, motivo por lo cual muchos de los proyectos que se han planteado para la misma sólo han quedado definidos como estudios, debido a la falta de presupuesto existente en la misma.

La Politécnica se encuentra dividida en edificios de Facultades, los mismos que están ubicados en sitios específicos dentro del Campus Politécnico, dichos edificios en su mayoría eran utilizados como aulas de estudio de la Politécnica antigua, y en la actualidad son utilizados como laboratorios sin tener las suficientes seguridades que se requieren para que sean utilizados como tales, quizás el mayor problema sea que la Politécnica es una universidad pública y se debe esperar a que el gobierno central destine fondos para la misma.

Antes de realizar cualquier diseño de seguridad física se deben tomar en cuenta las amenazas de las que nos queremos proteger, medir la probabilidad de ocurrencia de las mismas, y entonces definir la forma de cumplir los objetivos del proyecto. [2]

Como se mencionó anteriormente el objetivo principal es realizar un diseño de seguridad física para la EPN, para lo cual es de vital importancia verificar el estado actual de la institución, para obtener información que será de importancia para poder alcanzar dicho objetivo.

Para definir las amenazas de las cuales nos queremos proteger se ha realizado un levantamiento de información, mediante una encuesta realizada en enero del 2005 a los responsables de cada uno de los laboratorios del edificio antiguo de la ex Facultad de Ingeniería Eléctrica, al encargado del centro de cómputo general y el encargado del control de acceso vehicular. Se puede observar dicha encuesta en el Anexo 1.

A continuación se presenta la información obtenida de la encuesta, ordenada en tres grupos:

- Laboratorios de la ex Facultad de Ingeniería Eléctrica.
- Centro de cómputo general.
- Puntos de acceso vehicular.

En cada uno de los puntos antes mencionados se describe cuales son las vulnerabilidades físicas que actualmente tienen, problemas que han tenido en años anteriores, además de presentar una breve descripción de los activos que se tienen en cada uno de ellos.

1.2.2 LEVANTAMIENTO DE LA INFORMACIÓN DE LOS LABORATORIOS DE LA EX FACULTAD DE INGENIERÍA ELÉCTRICA.

1.2.2.1 Introducción

El edificio de la ex Facultad de Ingeniería Eléctrica se encuentra ubicado en la parte nor-occidental del Campus Politécnico, el mismo que consta de 4 plantas como se muestra en el Anexo 3, Diagrama P1. Dentro de cada planta existen diferentes aulas que han sido adecuadas como laboratorios y oficinas; cabe

recalcar que la mayoría de estos lugares en el pasado fueron aulas de estudio de Ingeniería Eléctrica, motivo por el cual no tienen las seguridades que deberían tener los laboratorios.

En cada una de las ubicaciones definidas como laboratorios, funcionan diferentes asignaturas de laboratorios, cada uno de ellos con diferentes sesiones y además cada sesión con diferente número de alumnos, el número de alumnos en cada sesión depende del número de estudiantes que se tiene en cada semestre; a continuación se presentan la realidad de cada uno de ellos.

1.2.2.2 Laboratorio de Comunicaciones

El laboratorio de comunicaciones se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 205 como se observa en el Anexo 3, Diagrama E1, en esta ubicación funcionan los laboratorios de:

- Comunicación digital
- Teoría de comunicaciones
- Sistemas microprocesados

En el laboratorio de comunicación digital durante el semestre Octubre/2004 Marzo/2005, se tuvieron 12 sesiones por semana, cada sesión tenia 6 estudiantes, aproximadamente 15 estudiantes por día [b].

En el laboratorio de Teoría de Comunicaciones, se tuvieron 3 sesiones por semana, cada sesión tenia 6 estudiantes, aproximadamente 4 estudiantes por día.

b

12 sesiones	6 estudiantes	1 semana	14,4 estud	aproximad	15 estud
semana	1 sesión	5 días	día		día

En el laboratorio de Sistemas microprocesados, se tuvieron 4 sesiones por semana, cada sesión tenia 3 estudiantes, aproximadamente 3 estudiantes por día.

A esta ubicación, aproximadamente estarían ingresando diariamente 22 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

En esta ubicación no existen divisiones interiores, funcionan conjuntamente oficinas y laboratorios.

Este laboratorio permanece abierto desde las 7h00 hasta las 21h00, y queda sin ninguna protección personal durante periodos en las mañanas, la hora del almuerzo y durante la noche.

Cinco personas tienen llaves de acceso a esta ubicación, en su totalidad profesores.

En años anteriores han existido pérdidas de objetos pertenecientes a profesores como laptops, y otros equipos durante la noche, debido a la poca seguridad física existente en el mismo; dichos robos se han producido debido a que en la segunda planta del edificio, existe una conexión directa entre el aula magna y cada una de las oficinas y laboratorios a través del techo falso. Por esta razón en dicha ubicación se ha colocado un sistema de alarma con sensores magnéticos de apertura y sensores de detección de movimientos, tienen acceso a las claves de la consola de control 6 personas, dichas claves no han sido modificadas.

Además se ha colocado una puerta metálica extra, y se ha colocado una malla que bloquea la conexión entre el aula magna y cada una de las oficinas y laboratorios.

En esta ubicación se tienen computadores, además de equipo electrónico entre los que se tiene osciloscopios digitales, osciloscopio analógico, generadores de funciones, fuentes AC/DC, programador de memorias. El software existente es

variado como por ejemplo Windows 2003, Windows XP, y aplicaciones como Microsoft Office, programas de simulación, entre otros. Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas, motivo por lo cual la información almacenada en los computadores es de suma importancia, para cada uno de los profesores que tienen sus oficinas en esta ubicación. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación y los precios referenciales que tienen estos activos en el mercado.

1.2.2.3 Laboratorio de Postgrado

El laboratorio de Postgrado se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 204 como se observa en el Anexo 3, Diagrama E1, en esta ubicación funcionan los laboratorios de la maestría correspondientes a:

- Gestión de Redes
- Redes de Área Local
- Redes de Área extendida

Todos los laboratorios tienen 24 sesiones por semestre, cada uno de ellos con aproximadamente 8 estudiantes por sesión.

A esta ubicación, aproximadamente estarían ingresando diariamente 4 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

Esta ubicación permanece abierta desde las 17h00 hasta las 21h00, y pocas horas durante el día, las mimas que son variables y dependen en gran parte del horario del ayudante del laboratorio, existiendo períodos en las mañanas y durante la noche en los cuales el laboratorio queda sin protección personal.

Una sola persona tiene llaves de acceso a esta ubicación.

Hasta el momento no han existido pérdidas de activos. Como medida de prevención se han colocado protecciones adicionales como una puerta metálica adicional y un sistema de alarma con sensores de apertura de puerta y sensores de movimiento. Las claves de administración del mismo lo tiene una sola persona, no se realizan cambios periódicos de claves.

En esta ubicación se tienen computadores, switches, hubs, routers, etc. El software existente es variado como por ejemplo Windows 2000, Windows XP, y aplicaciones como Microsoft Office, programas de administración de redes como por ejemplo loriot, analizadores de paquetes, entre otros. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación.

1.2.2.4 Laboratorio de Redes

El laboratorio de redes se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 203 como se observa en el Anexo 3, Diagrama E1, esta ubicación funciona como laboratorio y aula de clase de las siguientes asignaturas:

- Programación
- Programación Orientada a Objetos
- Sistemas Operativos
- Programación con herramientas visuales
- Aplicaciones distribuidas
- Bases de datos

- Introducción a la multimedia

- Diferentes seminarios.

Aproximadamente el laboratorio se encuentra abierto por 6 horas diarias, ingresando al mismo 30 estudiantes cada 2 horas, en total estarían ingresando 90 estudiantes diariamente, además de profesores y personal de limpieza, existen horarios laborables durante los cuales el laboratorio queda sin ninguna persona en su interior.

En esta ubicación no existen divisiones interiores, además funciona sólo como laboratorio y aula de clases, no existen oficinas en la misma.

Sólo dos personas tienen llaves de acceso al laboratorio, en su totalidad profesores, no han existido cambios de chapas durante los dos últimos años. En dicha ubicación no han existido robos, pero como medida de precaución se ha implementado un sistema de alarma con sensores de apertura de puerta y detección de movimiento, la consola de este sistema es la misma que controla el laboratorio de comunicaciones.

En esta ubicación se tienen 18 computadores, 1 Switch Cisco de 24 puertos, 2 Routers Cisco. El software existente es variado como por ejemplo Windows 2003, Windows XP, Linux Red Hat, y aplicaciones como Microsoft Office, programas de simulación, aplicaciones de programación como por ejemplo, Visual Estudio punto net, programas de diseño gráfico como flash.

Como se mencionó anteriormente esta ubicación funcionan laboratorios y aula de clases. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, cabe recalcar que el equipo existente en este laboratorio no pertenece a la Politécnica, pertenece a los estudiantes de la carrera de Ingeniería en Electrónica y Redes de Información.

1.2.2.5 Laboratorio de Sistemas Digitales

El laboratorio de sistemas digitales se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 202 como se observa en el Anexo 3, Diagrama E1, en esta ubicación funcionan los laboratorios de:

- Sistemas Digitales.
- Sistemas analógico - digitales.

En el laboratorio de sistemas digitales, durante el periodo Octubre2004/Marzo 2005 se tuvieron 11 sesiones por semana, cada sesión tenía 12 estudiantes, aproximadamente 27 estudiantes por día.

En el laboratorio de sistemas analógico - digitales, durante el periodo Octubre2004/Marzo 2005 se tuvieron 10 sesiones por semana, cada sesión tenía 12 estudiantes, aproximadamente 24 estudiantes por día.

A esta ubicación, aproximadamente estarían ingresando diariamente 51 estudiantes, además de los profesores, personal de limpieza, entre otros.

En esta ubicación no existen divisiones interiores, y no existen oficinas.

Esta ubicación permanece abierta desde las 9h00 hasta las 18h00, cabe recalcar que existen periodos en las mañanas durante los cuales esta ubicación queda sin protección personal, y durante la noche.

Cuatro personas tienen llaves de acceso a esta ubicación, entre profesores y ayudantes.

Hasta el momento no han existido pérdidas materiales, durante las noches o ausencias de personal en el laboratorio, tampoco se ha perdido equipo de laboratorio durante cada una de las sesiones de laboratorio.

Además en esta ubicación no se tiene ninguna seguridad extra, los encargados tienen mucha confianza de los profesores y estudiantes.

En esta ubicación se tiene computadores, además de equipo electrónico como fuentes de poder, generadores de funciones, lámpara ultravioleta, multímetros, osciloscopios, programador universal de memorias, circuitos integrados, protoboard, regletas tomacorriente. El software existente es Windows XP, y aplicaciones como Microsoft Office. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.6 Laboratorio de Control y Computación

El laboratorio de control y computación se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 217 como se observa en el Anexo 3, Diagrama E1, en esta ubicación funcionan los laboratorios de:

- Sistemas de control discreto
- Sistemas de control automático
- Control con micros
- Microprocesados

En el laboratorio de sistemas de control discreto, durante el periodo Octubre2004/Marzo 2005, se tuvieron 4 sesiones por semana, cada sesión tenía 10 estudiantes, aproximadamente 8 estudiantes por día.

En el laboratorio de Control automático, se tuvieron 15 sesiones por semana, cada sesión tenia 10 estudiantes, aproximadamente 30 estudiantes por día.

En el laboratorio de Control con micros, se tuvieron 8 sesiones por semana, cada sesión consta de 8 estudiantes, aproximadamente 13 estudiantes por día.

En el laboratorio de Microprocesados, se tuvieron 8 sesiones por semana, cada sesión tenia 8 estudiantes, aproximadamente 13 estudiantes por día.

A esta ubicación, aproximadamente estarían ingresando diariamente 64 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

En esta ubicación existen tres divisiones interiores, además funcionan conjuntamente oficinas y laboratorios.

Esta ubicación permanece abierta desde las 7h00 hasta las 19h00, no existen periodos durante los cuales el laboratorio queda si ninguna persona durante el horario que permanece abierto, se turna el personal para ir al almuerzo.

Siete personas tienen llaves de acceso a esta ubicación, cuatro profesores y tres ayudantes.

Se han extraviado objetos pequeños, como cables, durante las sesiones de laboratorio, en esta ubicación se ha colocado como medida de protección una puerta metálica en la entrada principal.

En esta ubicación se tienen computadores, conectores, data switch, además de equipo electrónico como décadas capacitivas, décadas resistivas, fuentes de poder, generadores de funciones, grafizadores, osciloscopios, multímetros, probadores lógicos, taladros, etc. El software existente es variado como por ejemplo Windows 98, Windows 2000, Windows XP y aplicaciones como Microsoft Office, programas de simulación, entre otros.

Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas, motivo por lo cual la información almacenada en los computadores es de suma importancia, para cada uno de los profesores que tienen sus oficinas en esta ubicación, además de los equipos que son utilizados para realizar las prácticas de los estudiantes.

En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían éstos en el mercado.

1.2.2.7 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 218 como se observa en el Anexo 3, Diagrama E1, aquí se encuentra una pequeña red formada por los siguientes servidores:

- Servidor WEB (PIII de 450 MHz)
- Servidor E-Mail (PIII de 670 MHz)
- Servidor de servicios múltiples TELEFIE (PII de 300 MHz)
- Servidor Proxy IBM.
- Servidor RAS (SOHO ROUTER).

Además aquí se tiene el siguiente equipo activo que sirve para realizar la interconexión de las diferentes computadoras con el centro de cómputo general:

- Hub Ethernet 10 Base T, 3 Com 12 puertos.
- Switch Ethernet 10 BaseT/ 100 Base TX Autosensig, IBM, 24 Puertos.
- Switch Ethernet con 24 puertos 10 Base T y un puerto 100 Base TX, IBM, 25 Puertos.

A esta ubicación tienen acceso únicamente profesores encargados de administrar el cuarto de Telecomunicaciones. Cabe recalcar que este cuarto de telecomunicaciones no tiene ningún sistema de protección, como por ejemplo sistemas de detección de incendios, aire acondicionado, etc.

En esta ubicación se ha colocado una puerta metálica adicional, la misma que ha sido forzada el año pasado pero no hubieron pérdidas.

1.2.2.8 Laboratorio de Circuitos Eléctricos

El laboratorio de Circuitos Eléctricos se encuentra ubicado en la primera planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL 101 y 107, como se observa en el Anexo 3, Diagrama E2, en esta ubicación funcionan los laboratorios de:

- Circuitos eléctricos I
- Circuitos eléctricos II
- Tecnología Eléctrica
- Electrotecnia
- Electricidad I
- Electricidad II

Para cada uno de los laboratorios se tiene dos sesiones por día y aproximadamente se tendrían 20 estudiantes por sesión, este número es variable y depende del número de estudiantes que se tiene por semestre.

A esta ubicación, aproximadamente estarían ingresando diariamente 120 estudiantes, además de los profesores, personal de limpieza, ayudantes, estudiantes que se acercan a realizar consultas, entre otros.

En esta ubicación existe una división interior, funcionan conjuntamente oficinas y laboratorios.

Esta ubicación permanece abierta desde las 7h00 hasta las 20h00, en forma continua, no existen horarios en los cuales el laboratorio queda sin ningún responsable del mismo en su interior.

Dos personas tienen llaves de acceso a esta ubicación, en su totalidad profesores.

No han existido actividades que comprometan la seguridad física del mismo durante los dos últimos años. Como medida preventiva se ha colocado una puerta de hierro en la entrada.

En esta ubicación se tiene 1 computador, además de equipo electrónico y eléctrico como amperímetros, analizadores de onda, analizadores de redes, auto transformador, bobinas, décadas capacitivas, décadas inductivas, décadas resistivas, década de condensador, frecuencímetros, fuentes de poder, galvanómetros, generadores de funciones, grafizador de campo, inductores, medidores, microamperímetros, miliamperímetros, mili voltímetros, multímetros, osciladores, osciloscopios, vatímetros, etc. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.9 Laboratorio de Diseño Electrónico

El laboratorio de Diseño electrónico se encuentra ubicado en la primera planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL 113, 114, 115 como se observa en el Anexo 3, Diagrama E2, en esta ubicación funciona únicamente el laboratorio de alta frecuencia

En este laboratorio, se tienen 7 sesiones por semana, cada sesión consta de 6 estudiantes, aproximadamente a esta ubicación estarían ingresando 9 estudiantes diariamente.

En esta ubicación funcionan conjuntamente oficinas y laboratorios.
Esta ubicación permanece abierta desde las 7h00 hasta las 18h00, existiendo periodos durante los cuales el laboratorio queda sin ninguna persona responsable del mismo.

Cuatro personas tienen llaves de acceso a esta ubicación, dos profesores y dos ayudantes.

No han existido eventos que hayan comprometido la seguridad del laboratorio.

Como medida de precaución existe un sistema de alarmas con sensores de apertura de puerta y de movimiento, las claves del sistema sólo tienen dos profesores. Además como funcionan conjuntamente oficinas y laboratorios, existen dos computadores, pertenecientes a los profesores.

En esta ubicación se tienen computadores, además de equipo electrónico como estabilizadores de voltaje, fuente de poder, generadores de señales, impresoras, medidores de intensidad de luz, medidores de intensidad de sonido, medidor de potencia, micro amperímetro, miliamperímetro, osciladores, osciloscopios, etc.

El software existente es Windows Windows XP, y aplicaciones como Microsoft Office, programas de simulación, entre otros. Los computadores son utilizados únicamente por los profesores, en los mismos se almacenan notas de estudiantes, trabajos, proyectos, etc.

En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían éstos en el mercado.

1.2.2.10 Laboratorio de Electrónica

El laboratorio de electrónica se encuentra ubicado en la primera planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL 105, 106, 116, 117 como se observa en el Anexo 3, Diagrama E2, en esta ubicación funcionan los laboratorios de:

- Dispositivos electrónicos
- Circuitos electrónicos
- Comunicación analógica

En el laboratorio de dispositivos electrónicos, se tienen 21 sesiones por semana, cada sesión consta de 10 estudiantes, aproximadamente 42 estudiantes por día.

En el laboratorio de circuitos electrónicos, se tienen 19 sesiones por semana, cada sesión consta de 6 estudiantes, aproximadamente 23 estudiantes por día.

En el laboratorio de comunicación analógica, se tienen 3 sesiones por semana, cada sesión consta de 12 estudiantes, aproximadamente 8 estudiantes por día.

A esta ubicación, aproximadamente estarían ingresando diariamente 77 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

En esta ubicación existen tres divisiones interiores y funcionan conjuntamente oficinas y laboratorios.

Esta ubicación permanece abierta desde las 7h00 hasta las 18h00, cabe recalcar que durante la hora del almuerzo, esta ubicación queda sin protección personal.

Dos personas tienen llaves de acceso a esta ubicación, en su totalidad profesores, los mismos que tienen sus oficinas junto al laboratorio.

En años anteriores han existido pérdidas de objetos, pertenecientes al laboratorio como multímetros, calculadoras y otros objetos, durante la noche, debido a la poca seguridad física existente en el mismo, dichos robos se han producido a través de la puerta principal. Estos han sido motivos para que en dicha ubicación se coloque un sistema de alarma con sensores de apertura de puerta y movimiento de cuatro sectores, las claves de dicho sistema tienen cuatro personas, las claves no han sido modificadas, además se ha colocado una puerta metálica extra con una cerradura Eléctrica.

En esta ubicación se tienen computadores, además de equipos electrónicos como osciloscopios, analizador de espectros, fuentes de poder, generadores, generadores de funciones, micro amperímetros, miliamperímetros, multímetros, osciloscopios, unidad trazador, unidad amplificador, unidad base de tiempo, etc. El software utilizado es Windows XP, y aplicaciones como Microsoft Office, entre

otros. Como se mencionó anteriormente en esta ubicación funcionan conjuntamente oficinas de profesores y laboratorios, los computadores son utilizados únicamente por los profesores, en donde se almacena información referente a los alumnos, como por ejemplo notas, trabajos, proyectos. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.11 Laboratorio de Control Industrial

El laboratorio de control industrial se encuentra ubicado en la planta baja del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL 021, 022, 024, 025, 026, 030, 031, como se observa en el Anexo 3, Diagrama E3. En esta ubicación funcionan los laboratorios de:

- Control Industrial
- Mandos neumáticos

En el laboratorio de control industrial, se tienen 6 sesiones por semana, cada sesión consta de 8 estudiantes, aproximadamente 10 estudiantes por día.

En el laboratorio de mandos neumáticos, se tiene 1 sesión por semana, cada sesión consta de 9 estudiantes.
A esta ubicación, aproximadamente estarían ingresando diariamente 12 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

En el laboratorio de Control Industrial existen cuatro divisiones interiores y funcionan conjuntamente oficinas, bodegas y laboratorios.

Esta ubicación permanece abierta desde las 9h00 hasta las 18h00, cabe recalcar que durante la mañana, esta ubicación queda sin protección personal.

Tres personas tienen llaves de acceso a esta ubicación, en su totalidad profesores, los mismos que tienen sus oficinas junto al laboratorio.

No han existido robos en los dos últimos años, por precaución se ha instalado una puerta metálica adicional.

En esta ubicación se tienen computadores, auto transformador, compresores de aire, contactores, electro válvulas, entenallas, equipo neumático, motores, multímetros, PLCs, pulsadores, relés, selectores, sensores, taladros, válvulas, etc. El software existente es Windows 98, Windows XP y aplicaciones como Microsoft Office, entre otros. Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas, motivo por lo cual la información almacenada en los computadores es de suma importancia, para cada uno de los profesores que tienen sus oficinas en esta ubicación. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.12 Laboratorio de Control electrónico de potencia

El laboratorio de control Electrónico de potencia se encuentra ubicado en la planta baja del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL 011, 012, 027, 028, 029, como se observa en el Anexo 3, Diagrama E3, en esta ubicación funcionan los laboratorios de:

- Electrónica de potencia
- Conversores estáticos
- Control de máquinas

En el laboratorio de electrónica de potencia, se tienen 16 sesiones por semana, cada sesión consta de 6 estudiantes, aproximadamente 32 estudiantes por día.

En el laboratorio de conversores estáticos, se tiene 8 sesiones por semana, cada sesión consta de 6 estudiantes, aproximadamente 10 estudiantes por día.

En el laboratorio de control de máquinas, se tiene 6 sesiones por semana, cada sesión consta de 6 estudiantes, aproximadamente 8 estudiantes por día.

A esta ubicación, aproximadamente estarían ingresando diariamente 52 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

En esta ubicación existen cuatro divisiones interiores y funcionan conjuntamente oficinas y laboratorios.

Este laboratorio permanece abierto desde las 8h00 hasta las 19h00, está sin protección por una hora durante el día, durante la hora del almuerzo se turnan los responsables del mismo.

Ocho personas tienen llaves de acceso a esta ubicación, tres ayudantes y cinco profesores, los mismos que tienen sus oficinas junto al laboratorio.

Han existido robos durante años anteriores, además se pierden cosas pequeñas del laboratorio, durante las sesiones de los mismos. Esto ha motivado a incrementar la seguridad, mediante una puerta metálica en la entrada principal, la misma que pasa siempre cerrada.

En esta ubicación se tienen computadores, además de equipo electrónico como amperímetros, amplificadores, analizadores, auto transformadores, banco de carga capacitivas, banco de carga inductiva, cámara fotográfica, contadores, fuentes de poder, generador, generador de funciones, generadores de pulsos, motores, multímetros, osciloscopios, variadores de velocidad, etc. El software existente es variado como por ejemplo Windows 2000 y aplicaciones como Microsoft Office, programas de simulación, entre otros. Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas, motivo por lo cual la información almacenada en los computadores es de suma importancia, para cada uno de los profesores que tienen sus oficinas en esta ubicación, además aquí se almacena información referente a un proyecto BID. En el Anexo 2 se presenta una

información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.13 Laboratorio de Taller eléctrico

El laboratorio de taller eléctrico se encuentra ubicado en la planta del subsuelo del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL S25, como se observa en el Anexo 3, Diagrama E4, esta ubicación funciona como taller eléctrico, el mismo que es utilizado por los estudiantes de tecnólogos.

En este laboratorio se tienen aproximadamente 25 estudiantes diariamente, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros.

Esta ubicación permanece abierta desde las 7h00 hasta las 13h00, y de 14h00 a 17h00 y está sin protección durante la hora del almuerzo.

Las llaves de esta ubicación las tiene sólo el profesor encargado.

Han existido robos durante años anteriores, se robaron una suelda Eléctrica ingresando por la puerta. Esto ha motivado a incrementar la seguridad, mediante rejas que cubren las ventanas tanto del lado interior como del lado exterior además de cambiar la puerta y colocar una nueva cerradura.

En esta ubicación no se tienen computadores, se tiene el siguiente equipo, bobinadora eléctrica, cortadora de láminas, dobladoras, entenallas, esmeriles, extintores de incendios, generadores, extractores, grabador de metales, guillotina, juego de llaves, mandril, micrómetros, soldadoras, taladros, tornos, sopletes, etc. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.14 Laboratorio de SEP (Sistemas Eléctricos de Potencia)

El laboratorio de Sistemas eléctricos de potencia se encuentra ubicado en la planta del subsuelo del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL S01, 02, 03, 04 como se observa en el Anexo 3, Diagrama E4.

En esta ubicación funciona únicamente el laboratorio de SEP (Sistemas eléctricos de potencia).

Se tienen 3 sesiones por día de aproximadamente 10 estudiantes cada sesión, esto varía para cada semestre, en promedio estarían ingresando a este laboratorio 30 estudiantes diariamente, además de profesores, ayudantes, personal de limpieza y otras personas.

Esta ubicación permanece abierta desde las 9h00 hasta las 19h00, y está sin protección aproximadamente unas tres horas durante el día.

Siete personas tienen llaves de acceso a esta ubicación, entre ayudantes y profesores.

No han existido pérdidas de materiales durante los últimos años, como medida de precaución se cambian las chapas todos los años.

En esta ubicación se tienen computadores, HUBs, impresoras, relay de corriente, temporizadores, voltímetros, etc. El software existente es variado como por ejemplo Windows 98, Windows 2000, Windows XP, y aplicaciones como Microsoft Office, programas de simulación, entre otros. Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas. En algunos computadores se tiene información almacenada referente a proyectos, tesis de grado, proyectos de investigación, etc. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.15 Laboratorio de Máquinas Eléctricas

El laboratorio de máquinas eléctricas se encuentra ubicado en la planta del subsuelo del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL S16, S17 como se observa en el Anexo 3, Diagrama E4. En esta ubicación funciona únicamente el laboratorio de máquinas eléctricas

En este laboratorio se tienen 2 sesiones por día, cada una de ellas con 6 estudiantes por sesión, aproximadamente 12 estudiantes por día, además de personal de limpieza, profesores y estudiantes.

Esta ubicación permanece abierta desde las 7h00 hasta las 19h00, y está sin protección durante cuatro horas durante el día.

Tres personas tienen llaves de acceso a esta ubicación, dos ayudantes y el jefe de departamento.

Han existido robos durante años anteriores como multímetros, además se pierden cosas pequeñas del laboratorio, durante las sesiones de los mismos.

En esta ubicación se tiene 1 computador, además existe equipo como acoples, alternadores, amperímetros, analizadores, auto transformadores, cargas inductivas, cargas capacitívas, convertidor, convertidor de frecuencia, cosfímetros, década de inducción, dinamómetros, extinguidor de incendios, generadores, indicadores, luxómetros, maquinas, medidores de fase, miliamperímetros, mili voltímetros, motores, multímetros, osciloscopios, rectificadores, reostatos, resistencias, secuencímetros, transformadores, amplificadores, vatímetros, etc. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.2.16 Laboratorio de Alto voltaje

El laboratorio de alto voltaje se encuentra ubicado en la planta del subsuelo del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en las ubicaciones EL S05, S06, S07, como se observa en el Anexo 3, Diagrama E4, en esta ubicación funciona únicamente el laboratorio de alto voltaje.

En el laboratorio de alto voltaje, se tienen 4 sesiones por semana, cada sesión consta de 4 estudiantes, aproximadamente 3 estudiantes por día.

A este laboratorio, aproximadamente estarían ingresando diariamente 3 estudiantes, además de los profesores, personal de limpieza, estudiantes que se acercan a realizar consultas, entre otros, el personal de limpieza se coordina con los encargados del laboratorio para realizar la limpieza unas tres veces a la semana, cabe recalcar que no existe ningún control sobre los mismos.

En esta ubicación existen dos divisiones interiores, funcionan conjuntamente oficinas, y laboratorios.

El laboratorio permanece abierto desde las 15h00 hasta las 19h00 y está sin protección durante las mañanas y durante toda la noche.

Dos personas tienen llaves de acceso, en su totalidad profesores. Han existido robos durante años anteriores, además se pierden cosas pequeñas del laboratorio, durante las sesiones de los mismos.

En esta ubicación se tienen computadores, además de equipo eléctrico y electrónico como aisladores, amperímetros, analizadores de espectros, atenuadores, fuentes de poder, generadores de pulsos, luxómetros, medidores de resistencia, megahómetros, motores, multímetros, osciloscopios, transformadores, unidades de control, vatímetros, voltímetros, etc. Cabe recalcar que en esta ubicación funcionan conjuntamente laboratorios y oficinas, motivo por lo cual la información almacenada en dicha ubicación es de suma importancia, para cada uno de los profesores que ocupan esta ubicación. En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se

encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.3 LEVANTAMIENTO DE LA INFORMACIÓN DEL CENTRO DE CÓMPUTO GENERAL

El Centro de cómputo general se encuentra ubicado en la planta subsuelo del edificio de administración el mismo que ocupa las áreas AD S01, S05, S06, S07, S08, S09, S10 y S11 como se observa en el Anexo 3, Diagrama A1.

Aquí se tiene la parte medular de la universidad, ya que en esta ubicación se encuentran los siguientes servidores:

- Servidor de correo
- Servidor DNS
- Servidor de Caching Web
- Servidor Web
- Servidor de Matrículas
- Servidor SAE

Este es el punto central al cual se conectan los edificios de las ex Facultades, para por ejemplo salir hacia Internet, realizar el proceso de matrículas, llenar la base de datos del SAE la misma que almacena las calificaciones de los alumnos, etc.

Siendo este un lugar de extrema importancia no se tienen seguridades físicas extras para controlar el ingreso autorizado del personal, lo único que se ha colocado es una puerta metálica extra, en años anteriores han existido robos, los mismos que se han producido por la puerta principal.

Otro problema claro que se tiene es que el centro de cómputo general colinda con dos aulas, las cuales se encuentran separadas con el mismo mediante paneles de madera, una persona podría fácilmente acceder al centro de cómputo, mediante

la ruptura de estas separaciones. Además no se tienen guardias en localidades cercanas, para que vigilen el mismo.

El centro de cómputo general no cuenta con un sistema de aire acondicionado, ni sistemas de detección de incendios, la única protección física que tiene es eléctrica, ya que cuenta con un UPS que regula el voltaje que ingresa a cada una de los servidores y equipo activo, además en esta localidad se cuenta con un sistema de puesta a tierra para evitar diferencias de potencial.

El centro general de cómputo pasa abierto desde las 7h30 hasta las 18h00. Durante los períodos laborables el centro general de cómputo pasa siempre con una persona en su interior, las personas se turnan para ir al almuerzo.

Cuatro personas tienen las llaves de acceso al mismo, no existen cambios periódicos de cerraduras.

Otro problema crítico que se tiene es que se han definido políticas de seguridad físicas por el personal que labora en el mismo pero lamentablemente no se han puesto en práctica.

En el Anexo 2 se presenta una información detallada sobre cada uno de los activos que se encuentran en esta ubicación, y los precios referenciales que tendrían estos en el mercado.

1.2.4 LEVANTAMIENTO DE LA INFORMACIÓN DE LOS PUNTOS DE ACCESO VEHICULAR

Se puede acceder al Campus Politécnico a través de cinco puntos de acceso vehicular como son:

- Acceso vehicular Tecnólogos
- Acceso vehicular Química
- Acceso vehicular Eléctrica

- Acceso vehicular Civil
- Acceso vehicular Teatro Politécnico

En cada uno de los puntos antes mencionados se tiene la vigilancia armada de guardias, al Campus Politécnico pueden ingresar con los vehículos, los profesores, estudiantes y trabajadores, para lo cual cada uno de los vehículos que desean ingresar deben tener en el parabrisas el adhesivo de la institución, el mismo que se obsequia a los profesores, y trabajadores y se vende a los estudiantes. Como un dato oficial se tiene que en el semestre Octubre2004/Marzo2005 se vendieron 80 adhesivos a los estudiantes y se obsequiaron 1200 adhesivos entre profesores y trabajadores.

Aquí surge un problema, las personas sacan copias de los adhesivos, e ingresan a la institución vehículos no autorizados o vehículos que no pertenecen a miembros de la misma, es común ver personas que se bajan de sus vehículos y se dirigen a las universidades vecinas.

Además los puntos de vigilancia sólo cuidan que los vehículos ingresen con el adhesivo, no se realiza una vigilancia de los objetos que ingresan a la institución, ni tampoco de los objetos que salen de la misma. La mayoría de objetos robados de la institución han salido fácilmente de la misma a través de los puntos de acceso.

1.3 ANÁLISIS DE RIEGOS [2]

1.3.1 INTRODUCCIÓN

El análisis de riesgos involucra la cuantificación de la probabilidad de ocurrencia de un evento no deseado y el impacto que traerá como consecuencia a la institución si este llegara a ocurrir, este análisis es utilizado para definir los problemas que queremos solucionar y definir los objetivos para alcanzar dicho propósito.

En algunos casos este análisis puede ser completamente obvio. Por ejemplo el administrador de una red de datos observa que se encuentran abiertos puertos innecesarios en el firewall de la red. Conocemos por experiencia que existen vulnerabilidades asociadas a puertos abiertos innecesariamente. Estos puertos no se encuentran asociados a procesos en el negocio de la empresa y los mismos pueden ser cerrados sin afectar al mismo. En este caso la recomendación sería cerrar los puertos abiertos innecesariamente.

En otros casos, las recomendaciones no son tan obvias cuando se consideran las implicaciones. Por ejemplo tenemos corriendo una herramienta para robar el password de los empleados, una vez obtenido el mismo podemos acceder sin problemas a la red, probamos el password por varias semanas y logramos el mismo objetivo.

Desde el punto de vista de los riesgos, estaría en peligro gran parte de información de la institución y puede traer como consecuencia que se afecte a la reputación de la misma. Una opción para reducir el riesgo de ocurrencia de esta acción, podría ser utilizar passwords más robustos y realizar cambios periódicos de los mismos, considerar las implicaciones que trae esta recomendación. Primero se debería enseñar a los usuarios a realizar passwords más robustos y a cambiar periódicamente los mismos.

Segundo, como recomendación se debería tener ayuda permanente para los usuarios, esto puede traer como consecuencia una gran resistencia por parte de los empleados para poner en práctica las recomendaciones. En este caso el análisis de riesgos ofrece pocas opciones, las mismas que deben ser discutidas con los usuarios.

1.3.2 IMPACTO EN LA INSTITUCIÓN

El impacto en la institución es una combinación del impacto causado en la institución por una brecha en la seguridad y la probabilidad de ocurrencia de fallo producida por dicha brecha.

En la práctica existen dos aproximaciones para establecer cuál es el impacto en la institución, una cuantitativa y otra cualitativa. La primera de ellas es la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del costo en caso de que ocurra, y aunque teóricamente es posible conocer el riesgo de cualquier evento y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad.

Especialmente, es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales, en este proyecto de titulación se toma como referencia de análisis el segundo método, el mismo que se explica a continuación. Para cuantificar estas características, la tabla 1.1 muestra una guía para el impacto potencial en la institución y la probabilidad de ocurrencia de una brecha de seguridad.

	Valor	Impacto Potencial
Alto	3	Pérdida de la reputación de la institución
		Pérdida de la confianza en la institución de los estudiantes
		Pérdida de la confianza en la institución de los empleados
		Litigación potencial
		Pérdida definitiva de información crítica de la institución
		Pérdida definitiva de ingresos para la institución
		No se puede cubrir la brecha de seguridad
		La pérdida de activos de la institución bloquea el desempeño de la misma
Medio	2	La reputación de la institución puede mejorar
		Se puede recuperar la confianza de los estudiantes
		Se puede recuperar la confianza de los empleados
		Litigación moderada
		La información crítica puede ser recuperada con mucho esfuerzo
		Mínimo impacto en los ingresos
		La brecha de seguridad puede ser cubierta con recursos internos
		La pérdida de activos de la institución, deteriora el rendimiento de la misma
Bajo	1	No existe pérdida en la reputación de la institución

Tabla 1.1 Impactos potenciales para la institución

A continuación se presenta la asignación de valores relacionados a la probabilidad de ocurrencia.

- Valor alto 3
- Valor medio 2
- Valor bajo 1

1.3.3 CÁLCULO DEL IMPACTO A LA INSTITUCIÓN

Para calcular el impacto a la institución de un riesgo específico se multiplica los valores de probabilidad de ocurrencia y el impacto potencial que causaría el mismo a la institución. Este resultado es utilizado para definir los niveles de control de acceso que se implementarán en el diseño del sistema de control de acceso. La tabla 1.3 muestra los valores asignados a cada ocurrencia.

	Impacto potencial para la institución		
	Bajo	Medio	Alto
Probabilidad	1	2	3
Alta 3	3 - Medio	6 – Medio	9 – Alto
Media 2	2 – Bajo	4 – Medio	6 – Medio
Baja 1	1 – Bajo	2 – Bajo	3 – Bajo

Tabla 1.2 Impacto en la institución

A continuación se muestra en la tabla 1.3 los problemas percibidos en la institución, referentes a la seguridad física.

	Impacto potencial para la institución		
	Bajo	Medio	Alto
Probabilidad			
Alta			Acceso no autorizado
Media			Desastres naturales
Baja		Vandalismo	Ataques terroristas

Tabla 1.3 Impacto de los problemas percibidos en la Politécnica

La tabla 1.3 muestra las brechas de seguridad que actualmente existen en la institución, no se mencionan otros problemas como robos, destrucción de la infraestructura, acceso a información clasificada, ya que estos problemas serían consecuencias de los problemas mencionados en la tabla 1.3. A continuación se procede a explicar cada uno de los problemas mencionados en la tabla 1.3.

Vandalismo.- Este problema depende en gran parte, de la educación de la personas, por ejemplo cuando un profesor le dice a un estudiante que ha perdido el semestre este puede actuar de una mala manera, destruyendo lo que encuentre a su alrededor, de la información obtenida, no se han registrado este tipo de actos en la institución. Se ha dado una calificación media, referente al impacto que este causaría a la institución si este llegara a ocurrir, debido a que la institución se podría recuperar de una manera rápida frente a este tipo de amenazas.

Acceso no autorizado.- Como se ha mencionado anteriormente a la institución ingresan y salen con una gran facilidad personas y objetos, sin necesidad de tener alguna identificación. No existe una manera de identificar claramente a los estudiantes, profesores, trabajadores y visitantes. Los accesos no autorizados de personas y objetos traen consigo consecuencias muy graves para la institución, por ejemplo ingresan personas de dudosa procedencia a la institución y los mismos pueden realizar robos, traficar droga, o en un caso crítico puede ingresar una persona que tiene mucha experiencia en alterar bases de datos en el centro de cómputo general y modificar la base de datos del SAE y hacer parecer a un estudiante de bajo rendimiento como un estudiante de altísimo rendimiento académico, o esta persona podría borrar por completo la base de datos del SAE.

Todos estos problemas vienen como consecuencia de no tener un adecuado control de acceso en la institución trayendo consigo graves consecuencias, estas consecuencias no son sólo internas, también pueden causar una pérdida total de la credibilidad de la institución.

Cabe recalcar que los robos no sólo ocurren por parte de personas ajenas a la institución, estos también pueden ser provocados por los mismos estudiantes, para lo cual se debe contar con un adecuado resguardo en la institución, además de definir políticas de control de acceso adecuadas para responder de una manera inmediata y efectiva ante alguna de estas amenazas.

Otro problema que se ha palpado es el uso inadecuado de los parqueaderos para automóviles en la institución, de la información obtenida se controla el acceso vehicular únicamente revisando que los automóviles tengan el adhesivo de la institución en el parabrisas, de experiencias vividas, las personas sacan copias del adhesivo e ingresan de una manera fácil a la institución y muchas veces dejan parqueados sus vehículos en lugares donde deberían estar personas autorizadas para realizar esta actividad.

Desastres naturales.- Esta es una gran brecha de seguridad, la misma que no depende en una forma directa de las personas, ésta depende de la naturaleza, en caso de ocurrencia y dependiendo del alcance del mismo podría fácilmente parar la producción de la institución. El Ecuador y principalmente Quito se encuentra rodeada de una gran cantidad de volcanes, los mismos que en caso de erupción podrían ocasionar deslaves. Además pueden ocurrir terremotos, causando una gran pérdida económica y en casos extremos de vidas. Del levantamiento de la información realizado, las personas y en sí la institución, no tienen definidas normas de seguridad, además de existir planes débiles para protegerse ante desastres naturales, peor aún, no existen políticas claras que definan que los departamentos deberían sacar respaldos de la información crítica para la institución.

Ataques terroristas.- Esta es una gran brecha en la seguridad que en caso de ocurrencia ocasionaría una gran pérdida a la institución, dependiendo de la magnitud de la misma, se podría llegar al extremo de perder definitivamente la confianza en la institución, tanto de las personas que estudian, trabajan en la misma, como de las instituciones que están ligadas de alguna forma con la misma, como por ejemplo el BID (Banco Internacional de Desarrollo).

Como un ejemplo hipotético, algún estudiante de química o física podría realizar un ataque biológico en contra de la misma institución, o en contra de otras instituciones, en la Politécnica se tienen laboratorios de alta radioactividad, principalmente en la ex facultad de física; si llegara ha ocurrir algún desastre en estos lugares las consecuencias para la institución y los lugares aledaños serían graves.

Del análisis realizado acerca del impacto que trae consigo la ocurrencia de una brecha de seguridad en la institución, se puede observar que el principal problema que se tiene en la institución en cuanto a la seguridad física, es el acceso no autorizado a la institución, trayendo consigo una gran cantidad de problemas como robos, destrucción de la infraestructura, etc.

1.4 ANÁLISIS COSTO BENEFICIO [2]

Como se observó en el análisis de riesgos, el principal riesgo que enfrenta la institución es el acceso no autorizado de las personas hacia la Institución, trayendo como consecuencias la pérdida de la credibilidad de la Institución. Del levantamiento de la información que se ha realizado se ha determinado que la Politécnica ha sido victima de muchos robos por personas de origen desconocido.

En el Anexo 2 se presenta información detallada sobre cada uno de los activos con sus respectivos precios referenciales, que existen en cada uno de los laboratorios del edificio antiguo de la ex Facultad de Ingeniería Eléctrica y el centro de cómputo general, esta información será utilizada en el capítulo 3 para realizar el diseño de seguridad física para el control de acceso de la EPN, mediante la cual se definirá cuáles son las áreas que necesitan una mayor protección que otras.

A continuación se muestra cómo se realizará el análisis para definir cuales son los sitios que necesitan una mayor protección que otros.

La tabla 1.4 muestra un resumen del Anexo 2 en donde se presenta el valor total de los activos que se tienen en cada uno de los laboratorios del edificio antiguo de la ex faculta de Ingeniería Eléctrica y del centro de cómputo general.

Ubicación	Costo Total $
LAB. Comunicaciones	12.804,64
LAB. Postgrado	21.296,00
LAB. Redes	21.296,27
LAB. Sistemas Digitales	28.898,75
LAB. Control y Computación	17.989,04
Cuarto de Telecomunicaciones	8.094,12
LAB. Circuitos Eléctricos	76.989,98
LAB. Diseño Electrónico	20.688,48
LAB. Electrónica	52.924,13
LAB. Control Industrial	25.123,98
LAB. Control Electrónico de Potencia	73.243,67
LAB. Taller Eléctrico	18.237,32
LAB. Sistemas Eléctricos de Potencia	15.548,96
LAB. Maquinas Eléctricas	91.521,69
LAB. Alto Voltaje	38.518,75
Centro de Cómputo General	48.346,22

Tabla 1.4 Resumen del Anexo 2 con el valor total de los activos

Algo que no se toma en cuenta en el Anexo 2 y que es de suma importancia, es el valor de la información que se almacena en cada una de las localidades, la cual no tiene precio, es decir el valor de recuperación de la misma es muy elevado, en el capítulo 3 se detalla como se protegerá cada uno de las áreas antes mencionadas.

De la información obtenida en la tabla 1.4 se puede apreciar claramente que el valor de los activos existentes en cada uno de los puntos a proteger es bastante

elevado, realizando un análisis únicamente de los valores presentados en la tabla 1.4 se puede apreciar que el valor costo beneficio es bastante bajo, es decir el costo de la implementación del sistema de control de acceso es relativamente bajo en comparación con el valor de lo que se quiere proteger.

Para poder determinar cuales serán las áreas que necesitaran una mayor protección que otras en este proyecto de titulación como criterios de diseño no se tomará en cuenta únicamente el valor de los activos tangibles, por ejemplo el laboratorio de maquinas eléctricas tiene un valor total de los activos mayor que el centro de cómputo general, pero como se menciono anteriormente el centro de cómputo general es la parte medular de la Politécnica ya que aquí se almacena información de suma importancia para la institución, motivo por el cual esta área necesita una mayor protección que otras.

1.5 ANÁLISIS DE OBJETIVOS

Como resultado del análisis del levantamiento de información se establecen como objetivos de estudio:

- Mejorar la seguridad física, frente al control de acceso a la institución sin limitar el desempeño de la misma y la libertad académica. Para lo cual el sistema de control de acceso debe ser de fácil uso, y de una baja probabilidad de fallo, cabe recalcar que un sistema de control de acceso tiene 3 elementos fundamentales, la tecnología utilizada en el sistema, disponibilidad del sistema y el más importante, el personal que interactúa con el mismo, ya que de nada serviría si las personas se rehúsan a utilizar el sistema, o lo burlan.

- Definir un sistema de control de acceso físico para la EPN, mediante el uso de tarjetas inteligentes de proximidad y sensores biométricos.

- Del análisis realizado se ha logrado determinar que existen ciertos lugares que necesitan una mayor protección, la solución planteada en este proyecto definirá los mecanismos utilizados para cumplir dicho objetivo.

- Dar una visión de las características de los productos actuales disponibles para cumplir dicho objetivo.

- Mediante un análisis de la tecnología se tendrá una visión del funcionamiento de cada uno de los productos que se tienen en la actualidad para cumplir con el control de acceso.

- Realizar un análisis técnico económico de la solución propuesta, para que las autoridades de la E.P.N tengan una visión del costo beneficio que se tendrá con dicha solución.

- Definir políticas de seguridad referentes al control de acceso físico a la institución, las mismas que serán una guía para definir responsabilidades, expectativas y comportamiento de las personas que interactúan con el sistema [c].

[c] Los individuos sujetos a la política o procedimiento deben "entender" lo que se espera de ellos. [4]

REFERENCIAS DEL CAPÍTULO I

[1] LAWRENCE J. Fenelly, Effective Physical Security, Tercera Edición, Elsevier, United States of America, 2004. Páginas 23-33.

[2] SUDHANSHU kairab, A Practical Guide to Security Assessments, Segunda Edición, Auerbach, United States of America, 2004. Páginas 193-205.

[3] GARCIA M. Lynn, The Design and Evaluation of Physical Protection Systems, primera Edición, Elsevier, United States of America. 2001. Páginas 173-199.

[4] AVILA Nelson., "Folleto, Seguridad en redes", Quito Ecuador. Capítulo 10.

2 ESTUDIO DE LA TECNOLOGÍA

2.1 CONTROL DE ACCESO [5] [6]

El control de acceso, en una forma u otra, es considerado por la mayoría de los profesionales de sistemas de seguridad informática como la piedra angular de los programas de seguridad. Las diferentes características físicas, técnicas y administrativas de mecanismos de control de acceso trabajan juntos para construir la arquitectura de seguridad tan importante en la protección de recursos críticos y sensibles de una organización.

La privacidad individual es uno de las principales razones para llevar a cabo mecanismos de control de acceso en una organización. Hoy en día, las bases de datos contienen extensa información que puede ser accedida de una forma fácil y con poca o quizás ninguna protección.

2.1.1 PRINCIPIOS Y OBJETIVOS DEL CONTROL DE ACCESO

La seguridad generalmente se define como la liberación del peligro. La seguridad informática, específicamente, es la protección de los datos en un sistema contra el acceso no autorizado a los mismos, modificación, o destrucción de los datos y protección del propio sistema informático. Ciertos controles de seguridad reducen el desempeño de la productividad, la seguridad es típicamente un compromiso entre los administradores de seguridad, usuarios del sistema, rendimiento del sistema y el personal administrativo para lograr un equilibrio satisfactorio entre la seguridad y la productividad.

2.1.2 TIPOS DE CONTROLES DE SEGURIDAD

Los controles para proporcionar seguridad informática pueden ser físicos, técnicos, o administrativos. Estas tres categorías de controles pueden ser clasificadas más allá como controles preventivos y detectores.

Los controles preventivos intentan evitar la ocurrencia de eventos no deseados, en cambio los controles detectores, intentan identificar eventos no deseados después de que ellos han ocurrido. Los controles preventivos prohíben el uso libre de recursos del sistema y por consiguiente sólo pueden aplicarse a usuarios que están dispuestos a aceptar las políticas de seguridad. Una política de seguridad eficaz puede ayudar a los usuarios a incrementar la tolerancia por los controles de acceso, ayudándolos a entender cómo tales controles les permiten confiar en sus sistemas informáticos. Entre los controles detectores se pueden citar: auditorías, métodos de detección de intrusos, y comprobadores del sistema.

2.1.3 CONTROL FÍSICO

Se considera la seguridad física como el uso de cerraduras, guardias de seguridad, contraseñas, alarmas, y medidas similares para controlar el acceso al sistema, a los equipos relacionados, y las propias instalaciones. Además, se requieren medidas para proteger los recursos, de robo y destrucción, o corrupción de los sistemas por accidente, o pérdidas ante un desastre natural (ej., diluvios y terremotos).

2.1.3.1 Controles físicos de prevención

Se emplean controles físicos preventivos para impedir a personal no autorizado ingresar a centros de cómputo, bases de datos, y en general lugares dónde se encuentran recursos, utilidades de apoyo, copias de seguridad, medios de comunicación, etc. y ayudan a proteger la información contra los desastres naturales.

Los ejemplos de estos controles incluyen:

- Respaldos de archivos y documentación.
- Guardias de seguridad.

- Sistemas de autenticación.
- Sistemas de doble puerta.
- Candados y llaves.
- Respaldo de energía.
- Controles de acceso biométrico.
- Selección del sitio.
- Extintores de incendio.

2.1.3.1.1 Respaldo de archivos y documentación

Debido a un accidente o debido a que un intruso destruye los archivos de datos o documentación, es escencial tener copias disponibles. Éstos respaldos deben guardarse lo suficientemente lejos de los archivos originales para evitar la destrucción de los mismos debido al mismo problema que destruyó los originales. El material de respaldo debe guardarse en un lugar seguro, construido de materiales incombustibles y debe incluirse un sistema contra incendios.

Los respaldos de la información deben tener el mismo nivel de protección que los archivos originales; es insensato mantener una seguridad firme para los datos en el sistema, pero una floja seguridad para los mismos datos en una situación de respaldo.

2.1.3.1.2 Guardias de seguridad

Se colocan a menudo guardias de seguridad en las entradas a las instalaciones, para interceptar a los intrusos y permitir el ingreso sólo a personal autorizado. Los

guardias son eficaces inspeccionando paquetes u otros artículos para asegurar el ingreso autorizado de los mismos. La efectividad de los guardias de estacionamientos puede reforzarse enormemente si en el edificio se instalan detectores electrónicos con alarmas u otros indicadores de advertencia que terminan en la estación del guardia.

2.1.3.1.3 Sistemas de autenticación

Puede controlarse el acceso físico a diferentes áreas utilizando un sistema eficaz de autenticación. Con este método de control de acceso, los empleados y visitantes deben llevar tarjetas apropiadas siempre que ellos estén en áreas dónde se tenga un sistema de control de acceso. Con sistemas programados de lectores de tarjetas sólo se permite la entrada a personas autorizadas, con lo cual se puede identificar fácilmente a los intrusos.

2.1.3.1.4 Sistemas de doble puerta

Éstos tipos de sistemas pueden ser utilizados a la entrada a las áreas restringidas (ej. centros de cómputo) para obligar a las personas a identificarse ante un guardia antes de ingresar libremente. Las dobles puertas son una manera excelente de impedirles a los intrusos ingresar a lugares restringidos.

2.1.3.1.5 Cerraduras y Llaves

El principal objetivo de estos mecanismos es retrasar el tiempo de acceso de personas no autorizadas a lugares dónde se almacenan diferentes activos o pasivos que son críticos para la institución.

Dependiendo del nivel de seguridad que se desee tener, se pueden tener cerraduras eléctricas, electromagnéticas, o una combinación de éstas.

2.1.3.1.6 Respaldo de la energía

El respaldo de energía es necesario para evitar pérdidas de información, además de ayudar a evitar un daño a los equipos debido a cortes de energía. Para períodos cortos de pérdida de energía, el respaldo de la misma es proporcionado normalmente por baterías. En áreas susceptibles a tiempos largos de reinstalación del suministro eléctrico (15–30 min), normalmente se recomiendan generadores a diesel.

2.1.3.1.7 Controles de acceso biométricos

La autenticación por métodos biométricos es un método más sofisticado de controlar el acceso a áreas restringidas, son más seguros que los sistemas lectores de tarjetas, pero los dos métodos operan en la misma manera. Entre los métodos biométricos para autenticación se incluyen: detectores de huellas digitales, detectores de la geometría de la mano, detectores de la voz, detectores de la firma, detectores de la retina. Éstos son muy utilizados por que éstos no pueden ser robados o compartidos, ellos proporcionan un nivel más alto de seguridad que las tarjetas. La autenticación biométrica se recomienda para tener niveles altos de seguridad y bajo tráfico entrante.

2.1.3.1.8 Selección del sitio [1]

Se debe seleccionar sitios con bajos niveles de riesgo, para que sean utilizados como centros de cómputo o lugares dónde se tiene la parte medular de la empresa o institución. Por ejemplo, las áreas arboladas pueden significar un riesgo de fuego, áreas adyacentes a un volcán puede traer consigo una probabilidad de terremoto, además se tiene que tomar en cuenta las facilidades que tienen personas adversas de producir algún tipo de ataque físico a la institución.

2.1.3.1.9 Extintores de incendios

El control de fuego es importante de prevenir para evitar desastres que pueden interrumpir las actividades. Los centros de cómputo, cuartos de equipos y otro tipo de información importante, debe localizarse lejos de las potenciales fuentes de incendios (ej. cocinas o cafeterías) y debe construirse de materiales incombustibles. Los muebles también deben ser incombustibles. Es importante colocar los tipos apropiados de extintores de incendios los mismos que deben ser de un fácil acceso. Se debe capacitar a los empleados en el uso apropiado de extintores de incendios y en los procedimientos que deben seguir en caso de un incendio.

Los rociadores automáticos son esenciales en cuartos de equipos y los espacios circundantes, los rociadores automáticos son especificados por las compañías de seguros para la protección de cualquier cuarto de equipos que contiene materiales combustibles. Sin embargo, el riesgo que el agua puede causar a los equipos es a menudo mayor que el riesgo de daño por fuego. Para mejorar esto se desarrollaron los sistemas controlados por dióxido de carbono; estos sistemas inundan un área amenazada por fuego con dióxido del carbono que suprime el fuego quitando el oxígeno del aire. Aunque el dióxido del carbono no causa daño a los equipos, es potencialmente letal a las personas en el área en conflicto y se usa ahora sólo en áreas desatendidas.

Actualmente se tienen sistemas que inundan el área con una mezcla de nitrógeno argón y bioxido de carbono conocido como Inergen que normalmente no causa daños al equipo y es menos peligroso para las personas que el dióxido del carbono. Inergen es la mejor protección para los equipos porque no es un gas conductor de energía y al descargarse la temperatura permanece estable y no deja residuos ni sustancias corrosivas. Es el gas apropiado para áreas donde los equipos permanecen encendidos porque al descargarse estos pueden continuar funcionando, además no causa daños a las personas.

2.1.3.2 Controles físicos de detección

Los controles físicos de detección advierten al personal encargado de la seguridad física que se están violando las medidas de seguridad físicas. Entre éstos se tienen:

- Sensores de movimiento.
- Sensores de humo y fuego.
- Circuitos cerrados de televisión.
- Sensores y alarmas.

2.1.3.2.1 Sensores de movimiento

En lugares dónde se tienen bajos niveles de presencia de personas, los sensores de movimiento son útiles para detectar a los potenciales intrusos. Los sensores de movimiento deben ser supervisados constantemente por guardias.

2.1.3.2.2 Sensores de humo y fuego

Los sensores de humo y fuego deben estar localizados estratégicamente para proporcionar a tiempo una advertencia, ante un fuego potencial. Todos estos equipos deben ser probados continuamente para asegurar que están trabajando en condiciones óptimas.

2.1.3.2.3 Circuitos cerrados de televisión [2]

Los circuitos cerrados de televisión tienen dos propósitos fundamentales, el primero es verificar si una alarma es verdadera, para poder dar una respuesta

efectiva en caso de que lo sea. El segundo propósito es el de proveer información adicional detallada acerca de una intrusión como: quién produjo la alarma, dónde y cuándo ocurrió la alarma, dicha información es utilizada para dar una respuesta inmediata, como ejemplo se pueden enviar guardias armados al lugar dónde ocurrió la alarma, cabe recalcar que éstos sistemas deben permanecer bajo vigilancia permanente para que puedan ser efectivos.

2.1.3.2.4 Sensores y Alarmas

Sensores y monitores de alarmas deben ser colocados para asegurar que la temperatura del aire permanece en condiciones aceptables para el equipo. Si no se mantienen las condiciones apropiadas, las alarmas alertan al personal de mantenimiento para corregir la situación antes de que ocurra una potencial interrupción del servicio.

2.1.4 CONTROLES TÉCNICOS

La seguridad técnica involucra el uso de respaldos de hardware, o software de las aplicaciones, hardware y software de las comunicaciones, y los dispositivos relacionados. Los controles técnicos a veces son llamados controles lógicos.

2.1.4.1 Controles Técnicos de prevención

Se usan controles técnicos de prevención para impedir a personal no autorizado acceder a programas.

Los ejemplos de estos controles incluyen:

- Control de acceso al software.
- Software Antivirus.

- Sistemas de control de librerías.
- Contraseñas.
- Tarjetas hibridas (inteligentes y de proximidad).
- Métodos de encripción.
- Control de acceso Dial-up y sistemas call-back.

2.1.4.1.1 Control de acceso al software

El propósito de control de acceso al software es el controlar información compartida entre diferentes usuarios. En muchos sistemas de computación, el acceso a programas y en si a la información es implementado mediante listas de control de acceso que designan qué usuarios tienen acceso a dicha información.

El software de control de acceso proporciona la habilidad de controlar el acceso al sistema estableciendo el empleo por parte de los usuarios de un identificador y de una clave.

Después que se ha concedido el acceso al sistema, el próximo paso es controlar el acceso a los datos y programas que residen en el sistema. El dueño del programa o los datos, puede establecer reglas que designan quién es autorizado para usar los datos o programa.

2.1.4.1.2 Software antivirus

Los virus han alcanzado proporciones epidémicas a lo largo del mundo de la computación y pueden causar rupturas y pérdida de datos así como la pérdida significante de productividad mientras se realiza la limpieza de los mismos.

Además, los nuevos virus están surgiendo a una proporción creciente actualmente, aproximadamente de uno cada 48 horas.

Se recomienda que el software antivirus sea instalado en todos los computadores, para descubrir, identificar, aislar, y eliminar los virus. Este software frecuentemente debe ser actualizado para evitar el contagio de nuevos virus.

2.1.4.1.3 Sistemas de control de librerías

Estos sistemas requieren que todos los cambios a los programas sean llevados a cabo por personal de control de librerías en lugar de los programadores que realizaron los cambios. Esta práctica asegura la separación de deberes, previniendo cambios no autorizados a los programas de producción.

2.1.4.1.4 Contraseñas

Se usan contraseñas para verificar que el usuario de un identificador (ID) es el dueño del identificador. La combinación de ID-contraseña es única para cada usuario y por consiguiente mantiene una tenencia responsable en la actividad en el sistema.

Las contraseñas fijas y usadas durante un período definido son a menudo fáciles de descubrir por los crakers [a]; por consiguiente, se debe tener un gran cuidado para asegurar que estas contraseñas no aparezcan en algún diccionario. Las contraseñas fijas controlan a menudo el acceso a bases de datos.

Contraseñas dinámicas o también conocidas como one-time password. Las contraseñas dinámicas son creadas por un símbolo que se programa para generar una contraseña aleatoriamente.

[a] Se considera un cracker como un experto informático que ingresa en los ordenadores ajenos con fines maliciosos y delictivos, mientras que un hacker es un experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de hacerlo.[6]

2.1.4.1.5 Tarjetas Hibridas

Las tarjetas hibridas normalmente son del tamaño de una tarjeta de crédito y contienen un chip con funciones lógicas e información que puede leerse en un terminal remoto para identificar los privilegios de un usuario específico. Las tarjetas hibridas normalmente encriptan la información de control que se compara con datos que el usuario proporciona (ej. un ID personal o datos biométricos como datos sobre el iris del ojo) para verificar la autorización para acceder a la computadora o red.

2.1.4.1.6 Encripción

La encripción se define como la transformación de texto plano (es decir, los datos leíbles) en texto encriptado (es decir, los datos ilegibles) mediante técnicas de encripción.

Actualmente se considera que la encripción es la única manera segura de proteger los datos para que no sean descubiertos durante su viaje a través de la red.

La encripción puede llevarse a cabo a través de hardware o software. El método de encripción basado en software es el método menos costoso y es conveniente para aplicaciones que involucran transmisiones de un volumen bajo; el uso de software para volúmenes grandes de datos produce un aumento inaceptable de procesamiento. La técnica de encripción en hardware, es utilizado cuándo se tienen grandes volúmenes de datos.

2.1.4.1.7 Sistemas de control de acceso dial-up y call-back

En el acceso dial-up a un sistema de computación incrementa el riesgo de intrusión producido por los crackers. En redes que contienen a computadoras personales o se conectan a otras redes, es difícil determinar si el acceso dial-up

está disponible o no debido a la facilidad con la que un módem puede agregarse a una computadora personal para convertirlo en un punto de acceso dial-up. Se deben controlar todos los puntos de acceso dial-up para permitir el acceso dial-up sólo a usuarios autorizados.

Actualmente, los controladores de acceso dial-up más efectivos utilizan un computador para interceptar llamadas y verifica la identidad de la visita (usando un mecanismo de contraseña dinámica). Previamente, los sistemas call-back interceptan los accesos dial-up, verificando su autorización y volviendo a llamar al número que fue registrado; sin embargo, los crackers han aprendido a burlar estas técnicas de control de acceso.

2.1.4.2 Controles técnicos de detección

Los controles técnicos de detección, advierten al personal de violaciones o intentos de violación de controles técnicos preventivos. Los ejemplos de éstos incluyen auditorías y sistemas de detección de intrusos que se discuten a continuación.

2.1.4.2.1 Auditoría

Una auditoría es un registro de actividades del sistema que habilitan la reconstrucción y examina la sucesión de eventos de una transacción, desde el comienzo hasta la obtención dé los resultados finales. El informe de violación presenta eventos significantes, eventos orientados a seguridad que indican que se realizaron transgresiones de la política de seguridad en la auditoría.

Los informes de violación frecuentemente y regularmente deben ser examinados por funcionarios de seguridad y se deben identificar los accesos desautorizados exitosos o infructuosos.

2.1.4.2.2 Sistemas de detección de intrusos

Estos sistemas rastrean a los usuarios (en base a sus perfiles personales) mientras ellos utilizan el sistema se determina si sus actividades actuales son consistentes con una norma establecida. Si no, la sesión del usuario puede terminarse o un funcionario de seguridad puede ser llamado para investigar. Estos sistemas pueden ser especialmente eficaces en casos en los que los intrusos están pretendiendo suplantar a usuarios autorizados, o cuándo usuarios autorizados están envueltos en actividades desautorizadas.

2.1.5 CONTROLES ADMINISTRATIVOS

Los controles administrativos de seguridad consisten en: procedimientos operacionales, procedimientos de responsabilidad, y suplementos de controles administrativos establecidos para proporcionar un nivel aceptable de seguridad para proteger los recursos de la organización. Además, los controles administrativos incluyen los procedimientos que se establecieron para asegurar que todo el personal que tiene acceso a los recursos tenga las autorizaciones requeridas.

2.1.5.1 Controles administrativos de prevención

Los controles administrativos de prevención son técnicas para controlar la conducta de personas para asegurar la confidencialidad, integridad, y disponibilidad de datos.

Los ejemplos de controles administrativos preventivos incluyen:

- Conocimiento de seguridad y entrenamiento técnico.
- Separación de deberes.

- Procedimientos para contratación y terminación.
- Procedimientos y políticas de seguridad.
- Supervisión.
- Contingencia, recuperación y planes de emergencia ante un desastre.
- Registros de acceso del usuario.

2.1.5.1.1 Conocimiento de seguridad y entrenamiento técnico

El conocimiento de seguridad y el entrenamiento es una medida preventiva que ayuda a que los usuarios entiendan los beneficios de las prácticas de seguridad. Si los empleados no entienden la necesidad por los controles de seguridad, ellos pueden burlar los controles en el futuro y por eso pueden debilitar el programa de seguridad o pueden hacerlo inútil.

Los entrenamientos técnicos pueden ayudar a los usuarios a prevenir el problema de seguridad más común "errores y omisiones" así como asegura que ellos entiendan cómo hacer un backup apropiado, entre otras cosas.

2.1.5.1.2 Separación de Deberes

Este procedimiento separa un proceso en partes, con usuarios diferentes responsables para las diferentes partes del proceso. La separación juiciosa de deberes impide a un individuo obtener el control entero de un proceso.

2.1.5.1.3 Procedimientos para contratación y terminación

Los procedimientos de contratación apropiados pueden prevenir la contratación de personas que probablemente violen las políticas de seguridad. Una investigación completa debe investigar la conducta del individuo, record policial y

referencias. Aunque esto necesariamente no muestra en su totalidad la honestidad e integridad de los individuos, puede ayudar a identificar áreas que deben investigarse con mayor profundidad.

Deben obtenerse tres tipos de referencias:

- Empleo
- Carácter
- Crédito.

Las referencias del empleo pueden ayudar a estimar el desempeño de un individuo para realizar una actividad. Las referencias del carácter pueden ayudar a determinar las cualidades como fidelidad, fiabilidad, y habilidad.

La referencia de crédito puede indicar los hábitos financieros de una persona que a su vez pueden ser un indicador de madurez y buena gana para asumir responsabilidad por las propias acciones de uno.

Además, se debe seguir ciertos procedimientos cuándo algún empleado deja la compañía, sin tener en cuenta las condiciones de terminación. Se deberá remover cualquier privilegio de acceso a los recursos de la institución, de un empleado que ha sido removido de su cargo.

Cualquier condición especial a la terminación (ej. prohibición del derecho para usar cierta información) debe comunicarse al empleado; además se debe firmar un documento que declara estas condiciones.

Todas las terminaciones deben ser comunicadas al administrador de la seguridad informática para asegurar que toda la información acerca de los privilegios de acceso sean revocados.

2.1.5.1.4 Políticas y procedimientos de seguridad

Son importantes políticas y procedimientos en el establecimiento de un programa eficaz de seguridad informática. Las políticas y procedimientos deben reflejar las políticas generales de la organización como protección de la información y recursos. Las políticas deben cubrir el uso de recursos y deben marcar la información sensible, movimiento de recursos, introducción de equipo y medios de comunicación, disposición de la información sensible ante una pérdida. La puesta en práctica de estas políticas es esencial para la efectividad de la seguridad informática.

2.1.5.1.5 Vigilancia

A menudo, un supervisor es la primera persona que nota un cambio en la actitud de un empleado. Las señales tempranas de descontento del trabajo del personal deben incitar a supervisores para considerar a un empleado en una situación crítica o sensible.

Los supervisores deben estar completamente familiarizados con las políticas y procedimientos relacionados a las responsabilidades de su sección. Los supervisores deben requerir que los miembros del personal obedezcan las políticas y procedimientos y deben observar la efectividad de estas pautas. Si se pueden lograr los objetivos de las políticas y procedimientos más eficazmente, el supervisor debe recomendar mejoras apropiadas.

Se debe separar regularmente asignaciones del trabajo para asegurar que se mantiene una separación apropiada de deberes, los trabajos críticos o sensibles deben ser rotados periódicamente entre personal calificado.

2.1.5.1.6 Recuperación, contingencia, y planes de emergencia ante un desastre

El plan de recuperación ante un desastre es un documento que contiene procedimientos como respuesta ante una emergencia. El objetivo primario de este plan, usado junto con los planes de contingencia, es proporcionar *una convicción*

razonable para que la institución pueda recuperarse de los desastres, continúe operando sus aplicaciones críticas aunque en modo degradado y las devuelva a un modo normal de funcionamiento dentro de un tiempo razonable.

Los planes ante una emergencia establecen procedimientos de recuperación que se dirigen hacia amenazas específicas. Por ejemplo, un plan de contingencia podría proporcionar un procedimiento que se debe seguir ante la erupción de un volcán.

2.1.5.1.7 Registro de acceso del usuario

Un registro formal asegura que todos los usuarios son autorizados apropiadamente para el acceso al sistema y a los servicios. Además, proporciona la oportunidad para informar a los usuarios de sus responsabilidades para mantener la seguridad informática y obtener su acuerdo para obedecer las políticas relacionadas y procedimientos.

2.1.5.2 Controles administrativos detectores

Se utilizan los controles administrativos detectores para determinar cómo las políticas y procedimientos cumplen con la detección de fraude y para evitar contratar a personas que representan un riesgo de seguridad inaceptable. Este tipo de control incluye:

- Revisión de la seguridad y auditorías.
- Evaluaciones de desempeño.
- Requerimiento de vacaciones.
- Investigaciones de fondo.

- Rotación de deberes.

2.1.5.2.1 Revisión de seguridad y auditorías

Las revisiones y auditorías pueden identificar casos en los que no están siguiéndose las políticas y procedimientos satisfactoriamente. Se procede corrigiendo las deficiencias y obteniendo apoyo del usuario para el programa de seguridad.

2.1.5.2.2 Evaluación de desempeño

Las evaluaciones regularmente dirigidas son un elemento importante en la calidad. Además, ellas pueden ser un foro eficaz para reforzar los principios de seguridad informática.

2.1.5.2.3 Requerimiento de vacaciones

Los empleados tensos son probablemente más sensibles a tener accidentes o errores mientras realizan su trabajo. Las vacaciones contribuyen a la salud de empleados relevando las tensiones y ansiedades que típicamente desarrollan durante períodos largos de trabajo.

2.1.5.2.4 Investigaciones de fondo

Las investigaciones de fondo pueden descubrir circunstancias pasadas que podrían indicar riesgos potenciales en actuaciones futuras.

Deben dirigirse investigaciones de fondo en todos los empleados considerados para promociones.

2.1.5.2.5 Rotación de Deberes

Como las vacaciones requeridas, se deben rotar los deberes para evitar fraudes hacia la institución, evitando dar la responsabilidad permanente de una actividad a un empleado.

2.2 CONTROL DE ACCESO FÍSICO [1] [2] [5] [6] [7]

Como se mencionó anteriormente el establecer un buen sistema de control de acceso físico es fundamental para mantener una excelente seguridad informática, como se mencionó en la introducción de este proyecto, el objetivo del mismo es realizar un diseño de control de acceso físico utilizando técnicas como tarjetas magnéticas, tarjetas hibridas y métodos de autenticación biométricos, para lo cual se prosigue a definir en mayor detalle este tipo de tecnologías, las mismas que caen dentro de la clasificación de control físico preventivo.

2.2.1 INTRODUCCIÓN Y CONCEPTOS BÁSICOS

Como se mencionó anteriormente uno de los requerimientos primordiales de los sistemas informáticos que desempeñan tareas importantes son los mecanismo de seguridad adecuados a la información que se intenta proteger; el conjunto de tales mecanismos ha de incluir al menos un sistema que permita identificar a las entidades (elementos activos del sistema, generalmente usuarios) que intentan acceder a los objetos (elementos pasivos, como archivos, centros de cómputo), mediante procesos tan simples como una contraseña o tan complejos como un dispositivo analizador de patrones retinales.

Los sistemas que habitualmente utilizamos los humanos para identificar a una persona, como el aspecto físico o la forma de hablar, son demasiado complejos para una computadora; el objetivo de los sistemas de identificación de usuarios no suele ser **identificar** a una persona, sino **autenticar** que esa persona es quién dice ser realmente. Aunque como humanos seguramente ambos términos nos parecerán equivalentes, para un ordenador existe una gran diferencia entre ellos: imaginemos un potencial sistema de identificación estrictamente *hablando*, por

ejemplo uno biométrico basado en el reconocimiento de la retina; una persona miraría a través del dispositivo lector, y el sistema sería capaz de decidir si es un usuario válido, y en ese caso decir de quién se trata; esto es identificación.

Sin embargo, lo que habitualmente hace el usuario es introducir su identidad (un número, un nombre de usuario, etc.) además de mostrar sus retinas ante el lector; el sistema en este caso no tiene que identificar a esa persona, sino autenticarlo: comprobar los parámetros de la retina que está leyendo con los guardados en una base de datos para el usuario que la persona dice ser: estamos reduciendo el problema de una población potencialmente muy elevada a un grupo de usuarios más reducido, el grupo de usuarios del sistema que necesita autenticarlos.

Los métodos de autenticación se suelen dividir en tres grandes categorías, en función de lo que utilizan para la verificación de identidad: (a) algo que el usuario sabe, (b) algo que éste posee y (c) una característica física del usuario o un acto involuntario del mismo. Esta última categoría se conoce con el nombre de **autenticación biométrica**. Es fácil ver ejemplos de cada uno de éstos tipos de autenticación: un *password* es algo que el usuario conoce y el resto de personas no, una tarjeta de identidad es algo que el usuario lleva consigo, la huella dactilar es una característica física del usuario, y un acto involuntario podría considerarse que se produce al firmar (al rubricar la firma no se piensa en el diseño de cada trazo individualmente). Por supuesto, un sistema de autenticación puede (y debe, para incrementar su fiabilidad) combinar mecanismos de diferente tipo, como en el caso de una tarjeta de crédito junto al PIN (*Personal Identification Number*) a la hora de utilizar un cajero automático o en el de un dispositivo generador de claves para el uso de *One Time Passwords*.

Cualquier sistema de identificación (aunque les llamemos así, recordemos que realmente son sistemas de autenticación) ha de poseer unas determinadas características para ser viable; obviamente, ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo máximo de 3% en los sistemas menos seguros), económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto) y

ha de soportar con éxito cierto tipo de ataques (por ejemplo, imaginemos que cualquier usuario puede descifrar el *password* utilizado en el sistema de autenticación; esto sería inaceptable).

Aparte de estas características tenemos otra, no técnica sino humana, pero quizás la más importante: un sistema de autenticación ha de ser aceptable para los usuarios, que serán al fin y al cabo quiénes lo utilicen. Por ejemplo, imaginemos un potencial sistema de identificación para acceder a los recursos de la Universidad, consistente en un dispositivo que fuera capaz de realizar un análisis de sangre a un usuario y así comprobar que es quién dice ser; seguramente sería barato y altamente fiable, pero nadie aceptaría dar un poco de sangre cada vez que desee consultar su correo.

2.2.2 SISTEMAS BASADOS EN ALGO CONOCIDO: CONTRASEÑAS

El modelo de autenticación más básico consiste en decidir si un usuario es quién dice ser simplemente basándonos en una prueba de conocimiento que *a priori* sólo ese usuario puede superar, esa prueba de conocimiento no es más que una contraseña que en principio es secreta. Evidentemente, esta aproximación es la más vulnerable a todo tipo de ataques, pero también la más barata, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad.

También se utiliza como complemento a otros mecanismos de autenticación, por ejemplo en el caso del Número de Identificación Personal (PIN) a la hora de utilizar cajeros automáticos.

En todos los esquemas de autenticación basados en contraseñas se cumple el mismo protocolo: las entidades (generalmente dos) que participan en la autenticación acuerdan una clave, clave que han de mantener en secreto si desean que la autenticación sea fiable. Cuándo una de las partes desea autenticarse ante otra se limita a mostrarle su conocimiento de esa clave común,

y si ésta es correcta se otorga el acceso a un recurso. Lo habitual es que existan unos roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior.

2.2.3 SISTEMAS BASADOS EN ALGO POSEÍDO: TARJETAS

Las tarjetas (en cualquiera de sus tecnologías) han sido utilizadas desde finales de la década de los 60's. Debido a la creciente necesidad de automatizar y simplificar diversos procesos (identificación de personas, pagos, etc.) se hizo necesaria la creación de un medio confiable y barato para realizar dichos procesos. Muchos han sido los intentos por cubrir semejante necesidad.

Dichos intentos han tomado la forma de una tarjeta, aunque las tecnologías utilizadas para implementar la confiabilidad necesaria han sido muy variadas.

Después de la invención de las tarjetas de cinta magnética, como lo son las tarjetas de crédito, han aparecido nuevas formas de realizar transacciones, y por otro lado han aparecido nuevos mecanismos de autentificación dónde las tarjetas comunes de cinta magnética no pueden ser empleadas. Por ejemplo, en el caso del dinero digital es indispensable la seguridad y la inviolabilidad de la información en la tarjeta, cosa que es muy simple de hacer con las tarjetas de cinta magnética dónde la información puede fácilmente ser extraída de la franja magnética que va exteriormente. En sistemas de autentificación como por ejemplo el servicio médico, ya no basta con la simple tarjeta pues cualquier persona puede suplantar al dueño de ella y así obtener la atención. A continuación se describen cada una de estas tecnologías y las ventajas y desventajas de utilizar cada una de ellas, en el control de acceso físico de las personas.

Las ventajas de utilizar tarjetas como medio para autenticar usuarios son muchas frente a las desventajas; se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora *hardware* de alta seguridad tanto para almacenar datos como para realizar funciones de encripción. Además, su uso es factible tanto para controles de acceso físico como para *controles de acceso*

lógico a los *hosts*, y se integra fácilmente con otros mecanismos de autenticación como las contraseñas; y en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuándo la introduzca en el lector o marcarla como inválida en una base de datos (por ejemplo, si se equivoca varias veces al teclear su PIN, igual que sucede con una tarjeta de crédito normal).

Como principal inconveniente de las tarjetas podemos citar el costo adicional que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas; aparte, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella no puede acceder al sistema, o hemos de establecer reglas especiales que pueden comprometer nuestra seguridad (y por supuesto se ha de marcar como tarjeta inválida en una base de datos central, para que un potencial atacante no pueda utilizarla).

2.2.4 TARJETAS DE BANDA MAGNÉTICA [8] [9]

Los medios de cinta magnética proporcionan un sistema barato y flexible para mantener información que deba ser modificable.

Una cinta magnética consiste de material magnético combinado con pintura o encuadernado; dicho material es sujeto a un campo magnético. Este campo alinea los polos magnéticos del material magnético, y lo hace adecuado para la lectura y la escritura. La cinta magnética puede ser laminada o estampada en cualquier superficie lisa, tal como una tarjeta de crédito, una tarjeta-llave de un cuarto de hotel, o un distintivo de identificación. La información es leída o escrita de la cinta por un lector.

Un lector consiste de una cabeza de grabación magnética, la cual puede leer y grabar información magnética en la cinta. La información en la tarjeta consiste de un código binario. Desde esta forma de datos de bajo nivel, un formato de datos de alto nivel (tales como el ISO/ANSI BCD o el ISO/ANSI ALPHA) es usado para convertir el código binario a caracteres alfanuméricos.

Las tarjetas de banda magnética comenzaron a aparecer en la industria bancaria a finales de los años 70. Una vez que los estándares internacionales fueron desarrollados, las tarjetas de banda magnética llegaron a ser un medio efectivo de proporcionar un servicio conveniente al cliente.

Hoy en día las tarjetas de banda magnética son ampliamente usadas en bancos, ventas al menudeo, controles de acceso en hoteles y boletos de aerolíneas.

De hecho, la infraestructura existente de equipos lectores / grabadores de cintas magnéticas es tan grande que cambiarlo a una tecnología alternativa sería un proceso altamente costoso y muy lento.

2.2.4.1 Características

El material del que está construida una tarjeta de banda magnética puede ser de PVC o de mylar, siendo ambos muy robustos.

Las dimensiones de las tarjetas de banda magnética están estandarizadas por el ANSI (*American National Standard Institute*) y por el ISO (*International Standars Organization*), y fueron definidas para facilitar la manipulación y almacenamiento de las mismas. La franja magnética existente en estas tarjetas posee tres pistas con usos y formatos independientes entre sí.

La pista 1 tiene una densidad de 210 bpi (bits por pulgada) con palabras de 6 bits más 1, para paridad impar. La codificación de 6 bits es un subconjunto del código ASCII.

Teniendo la tarjeta 3.375" de ancho, y siendo reservadas 0.293" al comienzo y 0.273" al final para sincronía, puede contener 84 palabras de información: ((3.375" - 0.293" - 0.273") * 210 bpi) / 7bits/palabra = 84.27 palabras.

La pista 2 tiene una densidad de 75 bpi con palabras de 4 bits más 1 bit para paridad impar. La codificación de 4 bits permite la formación de sólo 10 caracteres

numéricos más 6 de códigos. El número máximo de palabras es de 42 en una tarjeta: ((3.375" - 0.293" - 0.273") * 75 bpi) / 5 bits/palabra = 42.13 palabras.

El comienzo y el final de la pista también son reservados para sincronía. La pista 3 tiene una densidad de 210 bpi como la pista 1 y palabras de 4 bits más 1 bit de paridad impar como en la pista 2. En este caso, el número máximo de palabras posibles de almacenar es de 117: ((3.375" - 0.293" - 0.273") * 210 bpi) / 5bits/palabra.

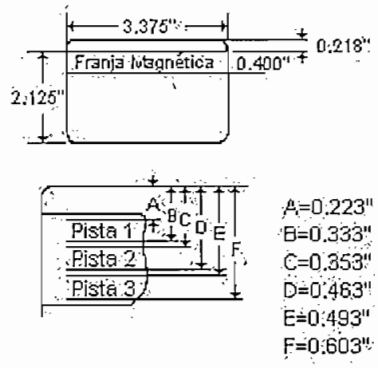


Figura 2.1 Dimensiones de la tarjeta de banda magnética

La cinta magnética y el lector se comunican vía un campo magnético.

La lectura es llevada a cabo deslizando la tarjeta de banda magnética a través del lector (aunque de igual modo puede hacerse que la cabeza de grabación se mueva a lo largo de la tarjeta). El lector recoge los cambios en la polaridad en la cinta con la cabeza de grabación magnética. Para la escritura, el lector crea un campo magnético que alterará la polarización de una pequeña región de la cinta, y de este modo escribirá información en la cinta.

El intercambio de datos entre la tarjeta y la unidad de lectura / grabación típicamente ocurre a velocidades de cerca de 12.000 bits por segundo.

ISO tiene dos especificaciones para parámetros tales como las técnicas de codificación / decodificación de los datos: [ISO/ANSI ALPHA e ISO/ANSI BCD], pero muchas aplicaciones no se adhieren a ellas. Esta falta de adherencia es

debida tanto a la flexibilidad del equipo disponible como al deseo de mejorar la seguridad.

La cinta magnética es susceptible a alteración o borrado causada por otros campos magnéticos; de igual modo es susceptible a daño físico y a daño causado por el medio ambiente.

La necesidad de prevenir el daño a la información almacenada en la cinta como resultado de un contacto inadvertido con campos magnéticos que pueden ser encontrados en el uso diario de una tarjeta ha llevado a muchos fabricantes, integradores e ingenieros a desarrollar tarjetas con propiedades magnéticas más resistentes. La resistencia de una cinta magnética es típicamente discutida en términos de coercitividad (medida en oersteds), la cual es definida como la fuerza del campo magnético requerido para borrar una cinta codificada. Generalmente, las tarjetas de baja coercitividad [300 oersteds] son más fácilmente cambiadas o codificadas que las tarjetas de alta coercitividad [3.000 oersteds].

Existen limitaciones para manejar niveles útiles de coercitividad, de cualquier modo, dado que cintas con una coercitividad de entre 3.000 y 5.000 oersteds pueden ser difíciles de leer, grabar o modificar.

El mejor ambiente para las tarjetas de banda magnética es un área limpia, seca y fría. Las temperaturas típicas de almacenamiento son entre -40 y 80 ° C. Las temperaturas típicas de operación son entre 0 y 55 ° C.

Existen otros tipos de tarjetas con franja magnética con fines específicos, que no tienen las dimensiones o densidades descritas anteriormente, pero con métodos de lectura y escritura semejantes. Algunos ejemplos del uso de estas tarjetas son los boletos magnéticos usados en trenes y subterráneos.

También es importante aclarar que es común la creación de aplicaciones en las que no es necesaria la compatibilidad en densidad y/o código utilizado con respecto a los estándares ANSI.

2.2.4.2 Técnicas de codificación / decodificación de datos

El ANSI y el ISO han definido dos normas para representar información sobre franjas magnéticas. Formato de datos ANSI/ISO BCD el cual consiste de 4 bits de datos y un bit de paridad impar P el cual es el bit más significativo. Los 4 bits restantes contienen información codificada y códigos de control como se muestra en la tabla 2.1.

P	INF (BIN)	INF (HEX)	CARÁCTER	FUNCION	P	INF (BIN)	INF (HEX)	CARÁCTER	FUN
1	0000	0	0	Información	0	1000	8	8	Información
0	0001	1	1	Información	1	1001	9	9	Información
0	0010	2	2	Información	1	1010	A	:	Control
1	0011	3	3	Información	0	1011	B	;	Inicio
0	0100	4	4	Información	1	1100	C	<	Control
1	0101	5	5	Información	0	1101	D	=	Campo Sep
1	0110	6	6	Información	0	1110	E	>	Control
0	0111	7	7	Información	1	1111	F	?	Fin

Nomenclatura
INF=Información
FUN=Función
P=Paridad

Tabla 2.1 Formato de datos ANSI/ISO BCD

Los datos codificados en una franja magnética empiezan con un flujo de ' 0 ' para permitir la sincronización con el lector. Un carácter llamado start sentinel = 01011b *le dice* al lector dónde comienza el flujo codificado de información en grupos de 5 bits cada uno. Al final de los datos, se encuentra el carácter end sentinel = 11111b que es seguido por un código de redundancia longitudinal (LRC).

El LRC es un comprobador de paridad para las sumas de todos los bits de información b0, b1, b2, y b3 de todos los caracteres precedidos. El START SENTINEL, END SENTINEL, y LRC son llamados caracteres de trama, y son removidos por el lector durante el proceso de reformateo. El formato de datos ANSI/ISO ALFA: consiste de 6 bits de información y un bit de paridad impar como el bit más significativo. El Formato de Datos ALFA es mostrado en la tabla 2.2. El formato de datos ALFA se relaciona estrechamente al código ASCII.

Se puede convertir los datos de ALFA a ASCII quitando el bit de paridad y agregando 0100000b = 20H.

P	INF (BIN)	INF (HEX)	CARÁCTER	FUNCION	P	INF (BIN)	INF (HEX)	CARÁCTER	FUN
1	000000	00	SP	Especial	0	001000	08	(	Especial
0	000001	01	|	Especial	1	001001	09	)	Especial
0	000010	02	"	Especial	1	001010	0A	*	Especial
1	000011	03	#	Especial	0	001011	0B	+	Especial
0	000100	04	$	Especial	1	001100	0C	,	Especial
1	000101	05	%	Inicio	0	001101	0D	-	Especial
1	000110	06	&	Especial	0	001110	0E	.	Especial
0	000111	07	'	Especial	1	001111	0F	/	Especial

P	INF (BIN)	INF (HEX)	CARÁCTER	FUNCION	P	INF (BIN)	INF (HEX)	CARÁCTER	FUN
1	010000	10	0	Información	0	011000	18	8	Información
0	010001	11	1	Información	1	011001	19	9	Información
0	010010	12	2	Información	1	011010	1A	:	Especial
1	010011	13	3	Información	0	011011	1B	;	Especial
0	010100	14	4	Información	1	011100	1C	<	Especial
1	010101	15	5	Información	0	011101	1D	=	Especial
1	010110	16	6	Información	0	011110	1E	>	Especial
0	010111	17	7	Información	1	011111	1F	?	Especial

P	INF (BIN)	INF (HEX)	CARÁCTER	FUNCION	P	INF (BIN)	INF (HEX)	CARÁCTER	FUN
1	100000	20	@	Especial	0	101000	28	H	Información
0	100001	21	A	Información	1	101001	29	I	Información
0	100010	22	B	Información	1	101010	2A	J	Información
1	100011	23	C	Información	0	101011	2B	K	Información
0	100100	24	D	Información	1	101100	2C	L	Información
1	100101	25	E	Información	0	101101	2D	M	Información
1	100110	26	F	Información	0	101110	2E	N	Información
0	100111	27	G	Información	1	101111	2F	O	Información
P	INF (BIN)	INF (HEX)	CARÁCTER	FUNCION	P	INF (BIN)	INF (HEX)	CARÁCTER	FUN
1	110000	30	P	Información	0	111000	38	X	Información
0	110001	31	Q	Información	1	111001	39	Y	Información
0	110010	32	R	Información	1	111010	3A	Z	Información
1	110011	33	S	Información	0	111011	3B	;	Especial
0	110100	34	T	Información	1	1100	3C	<	Especial
1	110101	35	U	Información	0	1101	3D	=	Especial
1	110110	36	V	Información	0	1110	3E	>	Especial
0	110111	37	W	Información	1	1111	3F	?	Fin

Nomenclatura
INF=Información
FUN=Funciona
P=Paridad

Tabla 2.2 Formato de información ANSI/ISO ALPHA

2.2.4.3 Two-Frecuency Coherent Phase Recording

La técnica de codificación utilizada en la grabación/lectura de las tarjetas de banda magnética fue desarrollada por Aiken en 1954 y es conocida como "Two-Frequency Coherent Phase Recording" (Grabación de Fase Coherente y Dos Frecuencias). Este método permite la grabación de datos en forma serial sin necesidad de pulsos de sincronía en un canal separado y con la posibilidad de utilizar una velocidad de lectura variable.

En la pista a utilizar tenemos, a espacios fijos, transiciones de flujo magnético (la franja magnética no es más que una cinta de material ferromagnético semejante al usado en las cintas de audio) estas transiciones a espacios fijos son usadas como señal de reloj. Entre una transición y otra puede o no existir una transición intermedia. Si existe dicha transición, el bit grabado es un 1; si no existe la transición intermedia, el bit grabado es 0.

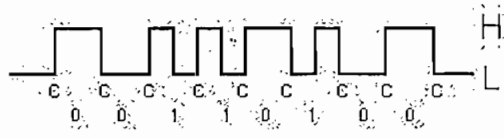


Figura 2.2 Generación de flujo de bits en un campo magnético

Se debe notar que a cada espacio regular existe una transición de nivel lógico alto (H) a un nivel lógico bajo (L) o de nivel lógico L a un nivel lógico H (no importa el sentido de transición, únicamente importa la existencia de ésta), cada transición es un pulso de reloj.

La permanencia del nivel en H o L de un pulso de reloj hasta el próximo pulso de reloj significa que el dato es un 0. Si hubiera una transición de H a L o de L a H entre un pulso de reloj y otro, entonces el bit grabado es un 1.

Como se puede apreciar, no importa el sentido de la transición magnética. Por cada espacio de 0.0133" siempre existirán dos transiciones magnéticas que sirven

de señal de reloj. Equidistantes a estas dos, o sea, a 0.00667" de una y de otra puede existir una transición indicando un bit 1.

Los "trenes de ceros" indicados son transiciones consecutivas con distancia de 0.0133" (bits 0) siempre existentes en el comienzo de las tarjetas que sirven para la sincronía de lectura a velocidad variable (esto explica el uso de 0.223" de la tarjeta sin información).

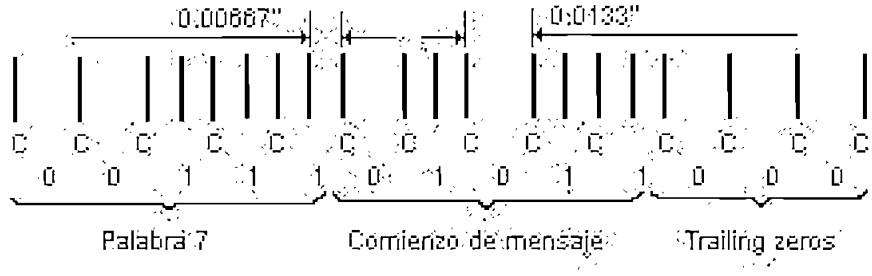


Figura 2.3 Dimensiones de las transiciones del flujo de bits

Las palabras son grabadas en la tarjeta de forma tal que el bit menos significativo queda a la derecha y el bit de paridad queda a la izquierda cuándo se mira la tarjeta como en la figura 2.3. Como la tarjeta se lee de derecha a izquierda, el bit menos significativo es el primero en ser leído.

2.2.4.4 Grabación y lectura en una tarjeta de banda magnética

Básicamente, la grabación magnética de una tarjeta se hace a través de la cabeza magnética con un gap, en la cual se provoca una inversión en el sentido de la corriente que circula por su embobinado a cada transición de flujo magnético deseada. A cada inversión en el sentido de la corriente, corresponde una inversión en el sentido de magnetización. En la franja magnética aparecen imanes con polos invertidos correspondiendo cada inversión a una transición de reloj o de dato 1.

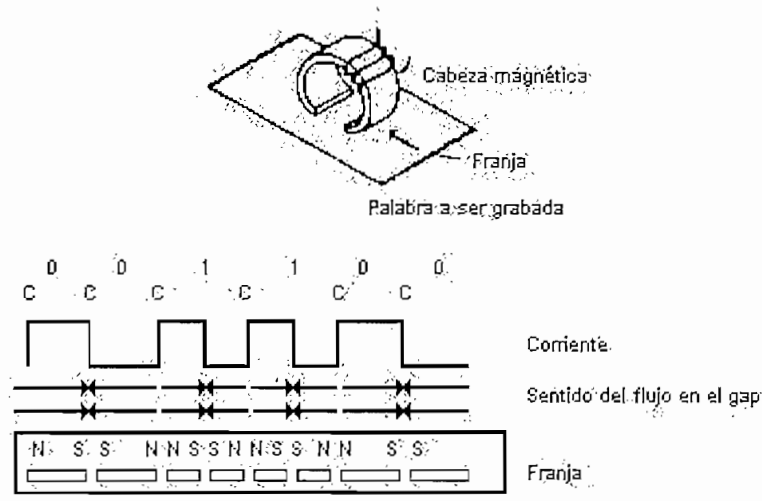


Figura 2.4 Escritura de la información codificada en la tarjeta magnética

Al pasar la tarjeta previamente grabada sobre una cabeza de lectura que posee un gap semejante al de la cabeza de grabación, ésta generará una tensión proporcional a la variación de flujo, obedeciendo así a la ley de Lenz. Cuándo el flujo es constante, la tensión generada es igual a cero.

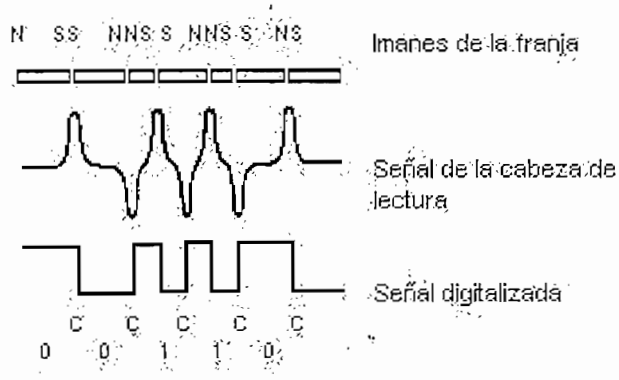


Figura 2.5 Lectura de la información codificada en la tarjeta magnética

2.2.4.5 Ventajas y desventajas de las tarjetas de banda magnética

La cinta magnética convencional, tal y como está especificada por ISO, tiene algunas deficiencias:

- La capacidad de datos es baja. Pueden surgir problemas de espacio en aplicaciones que requieren demasiada información puesto que, como ya se

mencionó, el máximo número de caracteres en una pista es 117, y el máximo en la tarjeta (utilizando sus 3 pistas) es de 243.

- La tarjeta magnética especificada por los estándares ISO y ANSI es vulnerable a la pérdida de datos causada por campos magnéticos producidos por fuentes magnéticas muy comunes, tales como imanes en pequeñas cantidades. Esta vulnerabilidad de las cintas magnéticas convencionales de baja coercitividad debida al daño magnético reduce el número de aplicaciones potenciales para la tarjeta. Por ejemplo, a nadie le gustaría "llevar dinero" (como es el caso del monedero electrónico) en una tarjeta que puede dañarse fácilmente teniendo como consecuencia la pérdida de dicho "dinero".

- La confiabilidad en la lectura de las tarjetas es pobre, con un porcentaje típico de falla en transacciones de 10%. Estudios dirigidos por el Doctor Denise Jeffreys han mostrado que el 60% de las fallas en las transacciones es debido a la desmagnetización de las tarjetas. Esta desmagnetización es debida a la baja coercitividad de los materiales magnéticos utilizados.

- El estándar ISO/ANSI puede ser fácilmente copiado, falsificado y duplicado, llevando esto a significativos fraudes en el mercado.

Las deficiencias descritas anteriormente están siendo superadas por las nuevas tecnologías de cinta magnética. Adicionalmente, estas tecnologías están disponibles a un pequeño costo extra sobre la tecnología convencional.

- Hay iniciativas significativas en la industria para incrementar la capacidad de datos en las tarjetas de banda magnética. El objetivo es crear una tarjeta de banda magnética con una capacidad de 100 caracteres, utilizando las tres franjas se podrán obtener 300 caracteres.

- La pérdida de datos debida a campos magnéticos comunes puede ser resuelta con el uso de material para cinta magnética de alta coercitividad, en el rango de 3.000 a 4.000 oersteds.

Entre algunas de las aplicaciones que se tienen en las tarjetas de banda magnética se tienen:

- Tarjetas de crédito y débito
- La tarjeta de efectivo o monedero electrónico.
- Licencia de Conductores.
- Control de Acceso, Tiempo y Asistencia.

2.2.5 SMART CARDS [10] [11] [12]

El término *smart card* es en sí es muy ambiguo y es usado de diferentes maneras. Para la ISO *smart card* corresponde a lo que ella denomina ICC (*Integrated Circuited Card*) y envuelve a todos los dispositivos dónde un circuito integrado cumple con los estándares impuestos para tarjetas plásticas de identificación ID1. La tarjeta es de 85.6mm x 53.98mm x 0.76mm y es igual a la tarjeta de cinta magnética que las entidades financieras emplean como instrumento de pago. La característica más notable de estos dispositivos radica en que internamente traen un dispositivo (microchip) con el cual pueden almacenar, modificar y procesar información que almacenan y que pueden ingresar en algún momento. Hay una gama de tarjetas que caen dentro de la categoría de *smart card* y la mayoría de ellas se distinguen por la manera en que procesan la información, las capacidades del chip, así como también el tipo de contacto que traen.

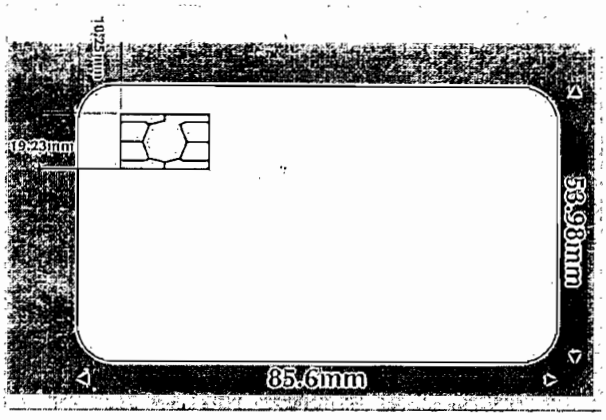


Figura 2.6 Dimensiones de smart cards

Esta tecnología tiene su origen en la década de los setenta cuándo inventores de Alemania, Japón y Francia inscribieron las patentes originales. Debido a varios factores que se presentaron, y de los cuales la inmadura tecnología de semiconductores tuvo un mayor peso, muchos trabajos sobre *smart cards* estuvieron en investigación y desarrollo hasta la primera mitad de los años ochenta.

2.2.5.1 Tipos de Smart Cards

A pesar de haber un estándar establecido por la ISO tanto para la manufacturación así como para las funcionalidades básicas que debiera incorporar una smart card existen dos tipos de clasificaciones. La primera de ellas tiene que ver con el tipo de chip que va en su interior, así como también la forma en que procesa la información. La otra manera de clasificarlas está relacionada con el tipo de contacto que tiene que tener la tarjeta para entrada y salida, así como también la fuente de poder.

Hasta el momento, se tienen tarjetas denominadas "Súper Smart Cards" las cuales tienen un teclado incorporado y un display LCD.

2.2.5.2 Caracterización por el tipo de Microchip

En lo referente a *smart cards* podemos decir que principalmente se distinguen dos tipos que se clasifican por sus capacidades de procesamiento, pero hay autores

que prefieren agruparlas en tres clases, dependiendo de la lógica con que modifican internamente los datos que pueden almacenar.

Desde el punto de vista de procesamiento se tiene que el primer tipo de *smart cards* se conoce como *smart cards* de *memoria* y son el modelo más simple y más económico de implementar. El segundo tipo corresponde a las llamadas *smart cards inteligentes* y son éstas las que traen en su interior una unidad central de procesamiento *CPU*.

2.2.5.3 Smart Cards de Memoria

Las smart cards de memoria son las más comunes de hallar en aplicaciones comerciales como tarjetas de prepago. Este tipo de tarjeta funciona como un simple buffer de información que el usuario modifica cuándo realiza una transacción con ella. Cabe recalcar que existen dos tipos de tarjetas de memoria, tarjetas recargables utilizadas por ejemplo para controles de acceso vehicular y tarjetas no recargables, como en el caso de telefonía la tarjeta viene de fábrica con el contenido de minutos que el usuario puede ocupar. Al hacer una llamada con la tarjeta, la máquina en cada minuto va descontando uno de los minutos que trae la tarjeta, de esa manera se evita que el usuario se sobregire.

Todos los tipos de smart cards deben incorporar algún tipo de memoria. Hasta el momento los tipos de memorias que emplean son:

- ROM memoria de lectura solamente.
- PROM memoria de lectura solamente y programable.
- EPROM una ROM programable y borrable.
- EEPROM una PROM borrable.
- RAM memoria de acceso aleatorio.

Un chip en particular puede emplear más de alguno de los tipos de memoria anteriores. Aquellos tipos de memoria tienen características propias en sus métodos de uso.

2.2.5.3.1 Características

- Los microchips de memoria puede ser vistos como un pequeño floppy disk con seguridad opcional.

- Las tarjetas de memoria pueden contener desde 103 bits hasta 16.000 bits de datos.

- Son menos caras que las *smart cards* inteligentes pero con esto sólo arriesgan la seguridad en el manejo de los datos.

- Para este tipo de tarjetas, la seguridad de la información almacenada recae casi enteramente en el lector de tarjetas que las procesa.

Son ideales cuándo los requerimientos de seguridad permiten el uso de tarjetas con baja o mediana seguridad.

2.2.5.3.2 Smart Cards de Memoria con Lógica de Seguridad

Son como las tarjetas de memoria pero incorporan la habilidad de controlar el acceso a los datos. Por lo general emplean códigos de acceso muy grandes, de alrededor 64 bits o más. Claramente emplean memorias EEPROM para implementar esta funcionalidad, debido a que los datos almacenados en la memoria necesitan ser modificados.

2.2.5.4 Smart Cards Inteligentes

En esta clase de *smart cards* caen todas aquellas tarjetas que en su interior traen un microchip que puede procesar la información que almacena la tarjeta. Para el

caso de autentificación un usuario podría tener en la memoria de la *smart card* almacenada, la información relativa a la retina.

Cuándo se quiera autentificar sólo tendría que mostrar su retina y contrastarla con la que viene en la tarjeta. Es por eso que se dice que este tipo de tarjetas son inteligentes, pues en cierto modo pueden hacer decisiones.

2.2.5.4.1 Características

- Las *smart cards* que incorporan el microchip pueden adherir, borrar y de alguna manera manipular información en su memoria. Pueden ser vistas como un computador en miniatura con un puerto de entrada/salida, sistema operativo y disco duro.

- El microchip trae un microprocesador que está disponible en arquitecturas de 8, 16 y 32 bits.

- Su capacidad de almacenamiento de datos varía entre 300 a 32.000 bytes con expectativas de incrementar esto último con los avances tecnológicos.

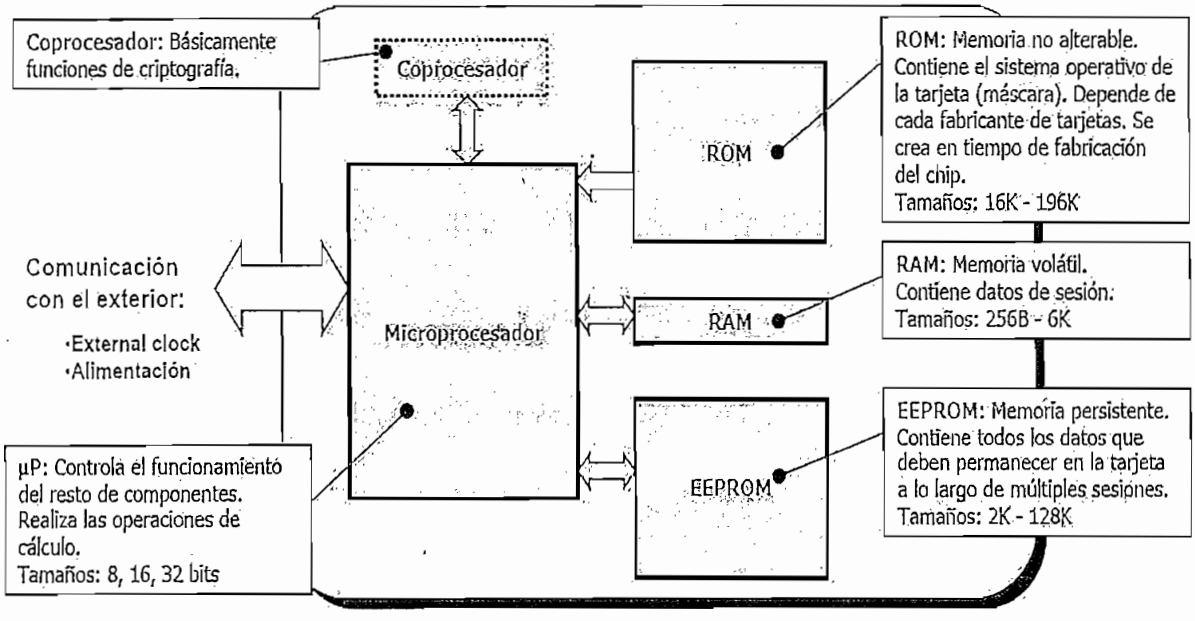


Figura 2.7 Estructura interna de Smart card inteligente

caso de autentificación un usuario podría tener en la memoria de la *smart card* almacenada, la información relativa a la retina.

Cuándo se quiera autentificar sólo tendría que mostrar su retina y contrastarla con la que viene en la tarjeta. Es por eso que se dice que este tipo de tarjetas son inteligentes, pues en cierto modo pueden hacer decisiones.

2.2.5.4.1 Características

- Las *smart cards* que incorporan el microchip pueden adherir, borrar y de alguna manera manipular información en su memoria. Pueden ser vistas como un computador en miniatura con un puerto de entrada/salida, sistema operativo y disco duro.

- El microchip trae un microprocesador que está disponible en arquitecturas de 8, 16 y 32 bits.

- Su capacidad de almacenamiento de datos varía entre 300 a 32.000 bytes con expectativas de incrementar esto último con los avances tecnológicos.

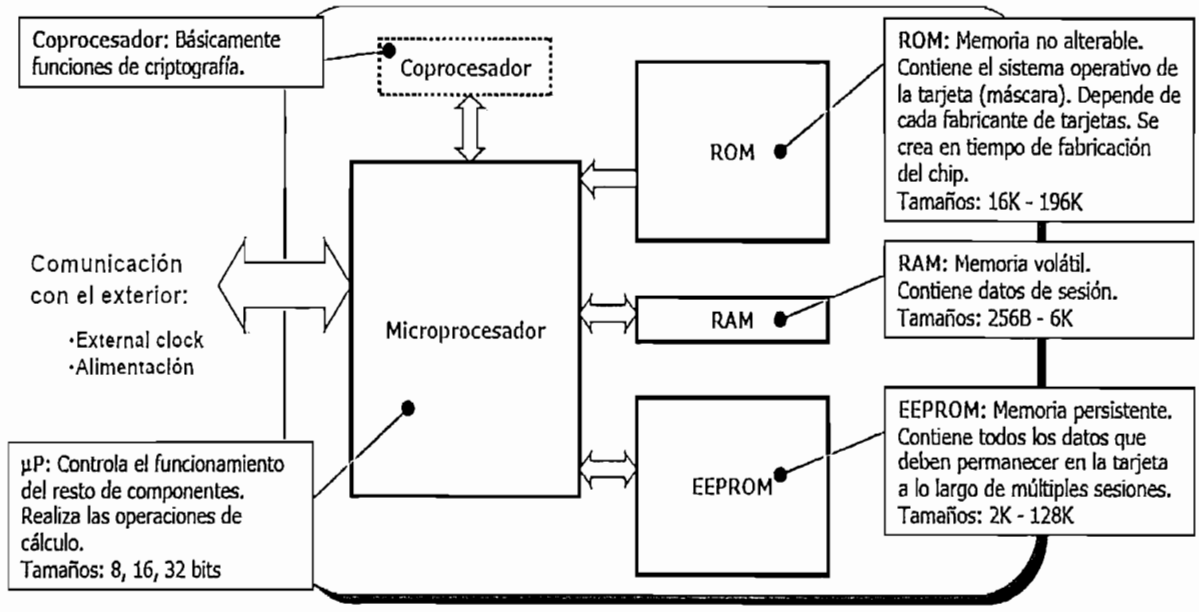


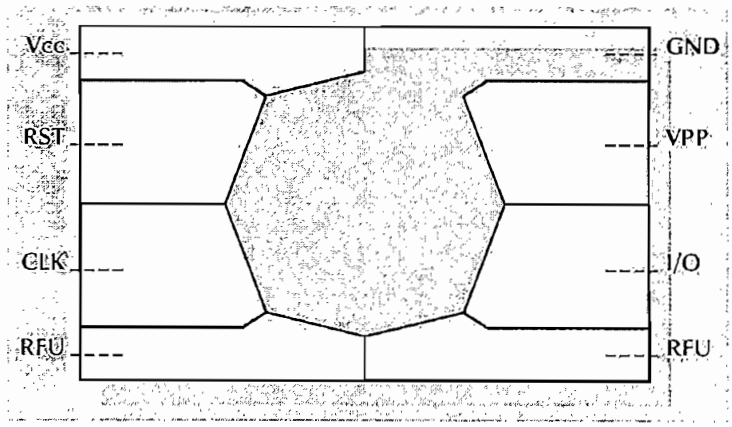
Figura 2.7 Estructura interna de Smart card inteligente

2.2.5.5 Clasificación de Smart Cards por el Tipo de Contacto

En su forma más simple, una smart card debe tener un contacto para comunicarse con el dispositivo lector, así como las tarjetas de franja magnéticas y a la vez debe tener una fuente de dónde obtener la energía necesaria para que funcione el chip o se recargue la batería. Con los avances de la tecnología se ha llegado al punto de no requerir de una batería como fuente de poder para la tarjeta, sino que la smart card obtiene su energía basándose en el principio de Faraday.

Más aún, no necesitan tener contacto con el lector, pues pueden transmitirles la información vía transmisión broadcast [b].

La manera de distinguir las *smart card* de esta categoría de las comunes es por la placa dorada del chip. Aunque la ISO definió 8 contactos para las tarjetas ICC, solamente seis se encuentran actualmente en uso y son empleados para que la tarjeta se comunique con el mundo exterior.



VCC	Voltaje de entrada estable	**GND**	Tierra
RST	Reset	**VPP**	Voltaje pico pico
CLK	Reloj	**I/O**	Entrada salida del dispositivo
RFU	Sin asignación		

Figura 2.8 Pinout del chip de la smart card

[b] Cuando una antena radia en todas direcciones se dice que su difusión

2.2.5.6 Smart Cards de Lectores sin Contacto

Una smart card sin contacto requiere solamente aproximarse al lector. Ambos, el lector y la tarjeta tienen una antena y es a través de este enlace sin contacto que enviándose ondas como las de radio se pueden comunicarse. Muchas tarjetas sin contacto también obtienen la energía para su microchip interno a través de esta señal electromagnética. El tamaño promedio de este tipo de tarjetas es de dos a tres pulgadas para las smart cards que no emplean batería, y son ideales para aplicaciones que requieran una interfàz muy rápida, como una gran masa de clientes que requieren acceso muy rápido.

Este tipo de tarjetas utiliza la tecnología de identificación por radiofrecuencia (RFID). La tecnología de identificación por radiofrecuencia (RFID) es un método de identificación automática sin contacto; es la tecnología más nueva y de más rápido crecimiento en el segmento de identificación automática en la industria.

RFID permite identificación automática, localización y monitoreo de personas, objetos y animales en una infinidad de aplicaciones que van desde simple inventario hasta sistemas complejos de casetas de cobro en carreteras.

La tecnología RFID ha revolucionado la industria de la identificación automática ofreciendo avances significativos en comparación con sistemas tradicionales como código de barras, tarjetas de banda magnéticas y chips de contacto.

2.2.5.6.1 Funcionamiento

De la manera más simple, un sistema RFID integra un número de identificación único en un pequeño microchip, y éste va a ser colocado en el objeto a ser identificado.

El microchip se activa sólo cuándo hay una señal de radio en una frecuencia específica mandada por un lector o transmisor. Cuándo el microchip es activado, inmediatamente responde mandando de regreso una señal de radio modificada que contiene el número de identificación de ese microchip.

El lector o transmisor se desempeña como radio transmisor y radio receptor. Cuándo el microchip responde a la señal y manda su número de identificación, el lector puede automáticamente mandar la señal a una computadora para su procesamiento. Este sistema tiene la ventaja sobre otros sistemas de identificación automática que no requiere línea de vista o contacto físico del lector con el microchip para ser leído.

Aunque en la tecnología RFID los microchips, antenas y lectores son el corazón del sistema, casi siempre son una parte muy pequeña de toda la solución. Los sistemas RFID generalmente incluyen computadoras, software, redes y sistemas de comunicación además de los lectores y los microchips.

Además de bajas frecuencias (125 khz–134,2 Khz.), las tarjetas de RFID operan en la banda HF 13,56 Mhz, y en la banda UHF 860–960 Mhz. Ambos tipos de tarjetas obtienen la energía que necesitan para operar de la señal de radio frecuencia generada por el lector.

2.2.5.7 Estándares en Smart Cards

Como una manera de prevenir la proliferación de múltiples sistemas de *smart cards* se han establecido estándares tanto en las funcionalidades mínimas que debiera tener una tarjeta, así como los protocolos y diseño. De esta manera la *ISO* fue la primera organización en establecer un modelo de *smart card*. A pesar de ello, hoy en día casi todas las tarjetas tienen aspectos en común pero eso no obliga a que un diseño en especial deba regirse por éstos estándares.

2.2.5.7.1 Los Estándares de la ISO

La *smart card* más básica que cumple los estándares es la de la serie **ISO 7816**. Aquellos estándares son derivados desde los estándares de tarjetas **ID (identificación)** y detalla la parte física, eléctrica, mecánica y la interfaz de programación para comunicarse con el microchip. A continuación se presenta un resumen de los estándares ISO 7816.

La descripción de cada una de las partes de la **ISO 7816** es:

- IS 7816-1 (1987): Características Físicas.
- IS 7816-2 (1988): Dimensiones y ubicaciones de los contactos.
- IS 7816-3 (1989): Señales Electrónicas y Protocolo de Transmisión
- IS 7816-4 (1995): Respuestas y Comandos Inter-industrias.
- IS 7816-5 (1994): Sistema de Numeración y procedimiento de registro.
- IS 7816-6 (1996): Elementos de datos Ínter industrias.
- (DIS) 7816-7: Comandos Ínter industrias y Consultas Estructuradas para una Tarjeta.
- (DIS) 7816-8: Comandos Ínter industria Relacionados con Seguridad.
- (DIS) 7816-10: Señales electrónicas y Respuesta al *Reset* para una Smart Card Sincrona.

2.2.5.7.2 Estándar de OpenCard

OpenCard es un estándar abierto que provee interoperabilidad de aplicaciones de *smart card* a través de desktop's, laptop's, etc. OpenCard promete proveer el 100% de aplicaciones para *smart card* en *Java* puro. Las aplicaciones para *smart cards* a menudo no son puras debido a que ellas se comunican con un dispositivo externo y/o usan librerías en el cliente. OpenCard también provee a los desarrolladores con un interfaz a PC/SC para el uso de los dispositivos existentes en plataformas de *Win32*.

OpenCard para cumplir con las metas propuestas tomó los protocolos de los estándares. Básicamente la aplicación se comunica con el lector, el cual vuelve a comunicarse con la *smart card* usando un protocolo, que en este caso es el establecido en el ISO 7.816.

La idea de OpenCard es conectar la *smart card* con una aplicación de *Java*. Para ello tiene establecido un protocolo llamado APDU (*Aplication Protocol Data Unit*), el que puede ser considerado un paquete de datos que contiene una instrucción completa o una respuesta completa desde la tarjeta. Para proveer esta funcionalidad, APDU tiene una estructura bien definida que está inserta dentro de los documentos pertenecientes a la familia de especificaciones de la ISO 7.816.

La idea detrás de todo lo anterior es que a través de un dispositivo lector que se conecta a un PC, sería posible realizar transacciones seguras vía Internet, independiente de la plataforma dónde esté conectada la tarjeta, gracias a *Java*.

2.2.5.7.3 Tipos de Protocolos de Comunicación

Hay dos protocolos de uso general que están en uso hoy en día:

T=0 doble transmisión de caracteres semi asíncrona.
T=1 doble transmisión de bloque semi asíncrona.

El protocolo T=0 es un protocolo predominante en Francia y fue un protocolo especificado solamente en el documento ISO 7816-3. En 1992 la ISO estandarizó el protocolo T=1 como una corrección a el ISO 7816-3. Por supuesto que el IC (circuito integrado) y el dispositivo de interfaz deben operar con el mismo protocolo. El método por el cual ellos alcanzan una óptima configuración en común ha sido el objeto de muchas discusiones al respecto en los últimos años. Al consenso que se ha llegado es tener una instrucción que seleccione el tipo de protocolo, esta instrucción es la llamada PTS (*Protocol Type Selection*).

Hay efectivamente un comando especial que envía el dispositivo de interfaz al IC después de la respuesta al *reset*. Para mantener compatibilidad con sistemas comerciales que solamente pueden emplear el protocolo de comunicación T=0, es necesario hacer algunos cambios al estándar original de la ISO 7816-3. Un nuevo concepto está propuesto el cual identifica el principio de los dos modos de operación:

- Modo Negociable.
- Modo Específico.

Una ICC (*Integrated Circuit Card*) què opera en un modo negociable puede cambiar su protocolo de comunicación por el uso del comando PTS. Una ICC que opera en el modo específico no puede aceptar un comando PTS pero puede ponerse dentro del modo negociable para una confirmación adicional del comando reset.

2.2.5.7.4 El Voltaje de Programación Vpp

La señal Vpp está diseñada para proveer el voltaje necesario que se requiere para habilitar escrituras en la memoria no volátil. Las tarjetas más comunes emplean memorias EEPROM dónde fuertes voltajes son generados en el chip.

Sin embargo, el tipo de memorias EEPROM requiere que grandes voltajes (usualmente 12,5 a 21 Volts) sean externamente provistos en el conector de la ICC. Se han tenido problemas en el pasado con los terminales que suplían los voltajes equivocados y producían efectos drásticos.

Debido a lo anterior y a las ventajas significantes de tener memorias re-escribibles, la memoria EEPROM es la más popular en circuitos integrados de smart cards, y de aquí que el rol del pin Vpp esté en disminución.

2.2.5.7.5 Ventajas

- Una de las principales ventajas es la autonomía de la que gozan estas tarjetas. Cualquier lector autorizado puede operar sobre una tarjeta de chip sin necesidad de que existan conexiones físicas a PC's o a bancos de datos. De este modo, la decisión de cualquier operación radica en el controlador mismo, y no en la respuesta que dicho lector pueda obtener de una base de datos almacenada en un PC.

- Fácil implantación: Hay dos tipos de periféricos: los autónomos y los que van controlados por PC. Los autónomos pueden reprogramarse con un Terminal portátil y los que van conectados a un PC, lo hacen por medio de una conexión clásica RS232.

2.2.5.7.6 Aplicaciones

- Control de Presencia y Accesos

- Activación de maquinaria para personal concreto, como pueden ser alarmas, maquinaria peligrosa, etc.

- Tarjeta de garantía de producto.

- Tarjeta monedero para utilizar en aparatos existentes dentro de la empresa, como pueden ser teléfonos, comedores, etc.

- Control de consumo de agua y energía en producción

Además de las tarjetas antes mencionadas, existen tarjetas hibridas las mismas que incluyen un código único utilizado para realizar el control de acceso físico, además se pueden incluir otras funcionalidades como puede ser la de almacenar la historia clínica de las personas.

2.2.6 SISTEMAS DE AUTENTICACIÓN BIOMÉTRICOS

A pesar de la importancia de la criptología en cualquiera de los sistemas de autenticación de usuarios mencionados anteriormente, existe otra clase de sistemas en los que no se aplica esta ciencia, o al menos su aplicación es secundaria. Es más, parece que en un futuro no muy lejano éstos serán los sistemas que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario, éstos sistemas son más amigables para el usuario (no va a necesitar recordar *passwords* o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética.

Estos sistemas son los denominados **biométricos**, basados en características físicas del usuario a autenticar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de autenticación biométricos; la criptología se limita aquí a un uso secundario, como la encripción de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), lo que significa que todo equipo biométrico mide e identifica alguna característica propia de la persona. Todos los seres humanos tenemos características morfológicas únicas que nos diferencian.

Por tanto, la medición biométrica se puede considerar como el método ideal de identificación humana.

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo que captura una imagen digital o analógica de la característica a analizar, comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos), y un interfaz para las aplicaciones que los utilizan. El proceso general de autenticación sigue unos pasos comunes a

todos los modelos de autenticación biométrica: captura o lectura de los datos que el usuario a validar presenta, extracción de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), comparación de tales características con las guardadas en una base de datos, y decisión de si el usuario es válido o no. Es en esta decisión dónde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación.

Por tasa de falso rechazo (*False Rejection Rate*, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (*False Acceptance Rate*, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Por último, y antes de entrar en más detalle con los esquemas de autenticación biométrica clásicos, quizás es conveniente tratar sobre uno de los grandes mitos de estos modelos: la vulnerabilidad a ataques de simulación. Hoy en día cualquier sistema biométrico - con excepción, quizás, de algunos modelos basados en voz - son altamente inmunes a éstos ataques. Los analizadores de retina, de iris, de huellas o de la geometría de la mano son capaces, aparte de decidir si el miembro pertenece al usuario legítimo, de determinar si éste está vivo o se trata de un cadáver.

2.2.7 TIPOS DE BIOMETRÍA

La biometría puede ser dividida en dos grandes grupos:

- Características fisiológicas :
  - huella digital
  - iris

- retina
- geometría de la mano

➢ Características de comportamiento

- Firma
- Voz

2.2.8 HUELLA DIGITAL [17] [18]

2.2.8.1 Introducción

Típicamente la huella dactilar de un individuo ha sido un patrón bastante útil para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico: desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica.

La Dactiloscopia es el nombre que se le da normalmente al procesamiento de huellas dactilares en círculos policiales y judiciales. En este ámbito se han desarrollado algoritmos muy estrictos para el tratamiento de huellas (pensados en principio para ser aplicados manualmente por operadores humanos). La mayoría de sistemas computarizados tradicionales están basados en imitar éstos métodos.

La preclasificación se utiliza para reducir el número de comparaciones exhaustivas a realizar. Si podemos clasificar una huella cualquiera perteneciente a una de 5 clases disjuntas, sólo habrá que comparar con las huellas almacenadas que pertenezcan a esa clase. Aunque la clase que se define para esta preclasificación no son siempre las mismas, siempre se basan en los puntos singulares de la huella como se muestra en la figura 2.9. En la *figura* 2.9 se observa cómo los dos puntos singulares más importantes de toda la huella: el

núcleo (o core) y el delta. El núcleo puede definirse como el punto de máxima curvatura de la cresta más interna mientras que el delta es el centro de un conjunto de crestas inferiores al núcleo que dibujan varios triángulos concéntricos. Las preclasificaciones se suelen basar el número de deltas (0, 1 o 2) y en su posición relativa respecto al núcleo.

Figura 2.9 Puntos singulares en una huella dactilar

Las leyes judiciales de cada país definen el llamado "Sistema Dactiloscópico" y este define las clases de la precalificación. Por ejemplo, el sistema norteamericano define las clases: arco (*arch*), arco de carpa (*tented arch*), lazo izquierdo (*left loop*), lazo derecho (*rigth loop*) y anillo de cresta (*whorl*). Un ejemplo de cada uno aparece en la figura 2.10. De hecho también existe la clase *scar* que define huellas parcialmente borradas por cicatrices permanentes.

Figura 2.10 Tipos de huellas (dactiloscopia de Henry, EE.UU.)

El método estándar (y el marcado por la legislación en todo el mundo) para la comparación exhaustiva de huellas es el de la extracción de minucias. Las minucias son los puntos singulares encontrados en el trazo de las crestas (puntos dónde se bifurcan, terminan). En una huella puede haber más de 100 minucias.

En muchos países se establece que dos huellas con 12 o más minucias coincidentes no pueden ser diferentes (las minucias deben coincidir en tipo, posición respecto al núcleo y dirección respecto a la horizontal). Nótese que basta con encontrar 12 coincidencias, para poder autenticar a una persona.

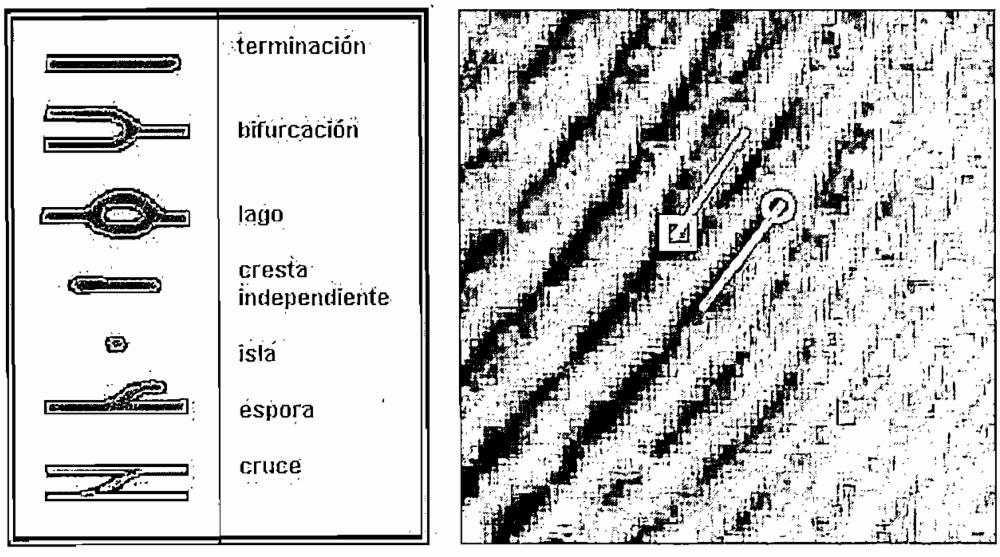


Figura 2.11 Tipos de minucias (izquierda). (Derecha) ejemplo de dos tipos: bifurcaciones (cuadrado) y fin de cresta (círculo).

A continuación se describen los pasos a seguir para autenticar a las personas mediante las huellas dactilares.

2.2.8.2 Obtención de la imagen

Cuándo un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta), aquí se toma una imagen como se muestra en la figura 2.12.

Figura 2.12 Huella obtenida

2.2.8.3 Mejoramiento de la Imagen

La información direccional de la imagen de un bloque específico está contenida en la magnitud de la Transformada del coseno discreto de Fourier del bloque. La imagen es dividida en bloques de 32x32 píxeles, los cuales son mejorados utilizando la magnitud de la Transformada del coseno discreto de Fourier del bloque. El mejoramiento es realizado sobre un área de 256x256 píxeles.

La Transformada del coseno discreto de Fourier es calculada de acuerdo a:

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\exp\left\{-j2\Pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \quad \{1\}$$

Dónde:

F = Transformada del coseno discreto de Fourier

u, v = Parámetros de frecuencia en el eje x, eje y.

M, N= Número de píxeles tomados en cada uno de los cuadros

La imagen mejorada g(x, y) en cada bloque es obtenida por:

$$g(x,y) = F^{-1}\left\{F(u,v)x|F(u,v)|^{k}\right\} \quad \{2\}$$

Dónde F (u, v) es la Transformada del coseno discreto de Fourier de un bloque de 32x32 píxeles y F^{-1} es la Transformada Inversa del coseno discreto de Fourier obtenida de acuerdo a:

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)\exp\left\{j2\Pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right\} \qquad \{3\}$$

Experimentalmente se ha encontrado que un valor de k = 1.2 es el óptimo para el mejoramiento de la imagen. Este método presenta un problema en los bordes de cada bloque por lo que se necesita un traslape de 26 píxeles entre cada bloque para eliminar este efecto.

Figura 2.13 Imagen mejorada mediante la transformada de Fourier

2.2.8.4 Imagen Direccional

De acuerdo con la clasificación de Henry, la estructura global de las huellas pueden ser clasificadas en lazo derecho, lazo izquierdo, arco, arco de capa. De esta forma la estructura de la huella dactilar de algún usuario pertenece a alguna de éstas clases. La imagen direccional nos da información de la estructura global de la imagen de la huella dactilar. Por lò que una primera fase de identificación es verificar que la imagen de la huella pertenezca a su clase. Después del mejoramiento de la imagen se procede a calcular la orientación local de cada píxel. Después de obtener la dirección de cada píxel se realiza un promediado de éstas tomando bloques de 15x15 píxeles. De esta imagen sólo se toma la región

central de 240x240 píxeles. La región central de la imagen esta formada por 16x16 bloques, cada uno de 15x15 píxeles, estos bloques son conocidos como la entrada a una red neuronal no supervisada.

2.2.8.5 Segmentación.

En el procesamiento de las imágenes de huellas dactilares es usualmente necesario remover las partes que no llevan información válida. La segmentación es útil para este propósito. Una buena técnica de segmentación debe ser insensible al contraste de la imagen original y debe ser independiente a si la imagen es mejorada o no.

El *método compuesto* que combina los métodos de segmentación basados en la información de *dirección* y *varianza* es altamente eficiente para determinar regiones inválidas.

Figura 2.14 Huella Binarizada (segmentación de la huella)

Una vez obtenida la imagen binaria de la huella dactilar es más fácil obtener las minucias a partir del esqueleto de la imagen, por lo que un algoritmo de esqueletización es aplicado a fin de obtener dicha imagen. La figura 2.15 muestra el esqueleto de la imagen de la figura 2.14

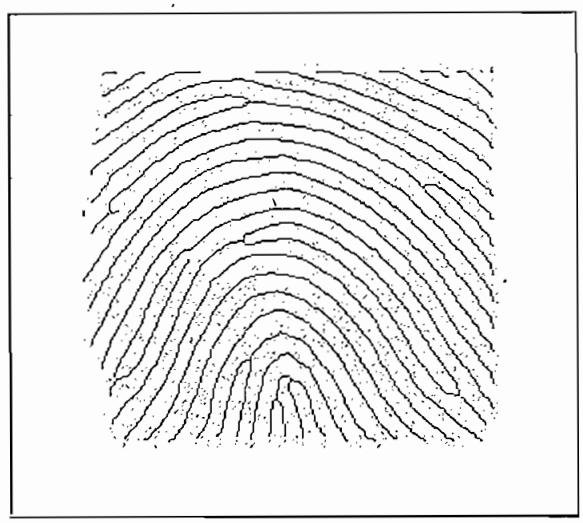


Figura 2.15 Huella Esqueletizada

Después de esqueletizar la imagen en ocasiones se suelen obtener falsas minucias dependiendo si el usuario presionó excesivamente o suavemente la superficie del sensor. Por esta razón, a la imagen esqueletizada se le aplica un algoritmo de detección de este tipo de falsas minucias. Una vez detectadas las falsas minucias, se eliminan de la imagen.

Posteriormente se prosigue con la extracción de las minucias, una vez detectadas las bifurcaciones y terminaciones dentro de la imagen, se forma una plantilla, la cuál contiene el tipo de minucia detectada, posición, distancia a sus cinco vecinos más cercanos, y ángulo de orientación de la minucia. Con esta plantilla que se obtiene para cada minucia, se forma una base de conocimiento para cada individuo. Si la imagen pertenece a su clase de acuerdo con la estructura global de la huella dactilar del individuo, esta base de conocimiento se compara con la imagen del individuo a fin de poder decidir si pertenece o no al individuo.

Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones retinales); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en

cuenta contra estos sistemas es el psicológico, no técnico: hemos dicho en la introducción que un sistema de autenticación de usuarios ha de ser aceptable por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso.

2.2.9 IRIS Y RETINA

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: analizan patrones retinales, o analizan el iris. Estos métodos se suelen considerar los más efectivos: para una población de 200 millones de potenciales usuarios la probabilidad de coincidencia es casi 0, y además una vez muerto el individuo los tejidos oculares degeneran rápidamente, lo que dificulta la falsa aceptación de atacantes que puedan robar este órgano de un cadáver.

La principal desventaja de los métodos basados en el análisis de patrones oculares es su escasa aceptación; el hecho de mirar a través de un binocular (o monocular), necesario en ambos modelos, no es cómodo para los usuarios, ni aceptable para muchos de ellos: por un lado, los usuarios no se fían de un haz de rayos analizando su ojo y por otro un examen de este órgano puede revelar enfermedades o características médicas que a muchas personas les puede interesar mantener en secreto, como el consumo de alcohol o de ciertas drogas. Aunque los fabricantes de dispositivos lectores aseguran que sólo se analiza el ojo para obtener patrones relacionados con la autenticación, y en ningún caso se viola la privacidad de los usuarios, mucha gente no cree esta postura oficial (aparte del hecho de que la información es procesada vía software, lo que facilita introducir modificaciones sobre lo que nos han vendido para que un lector realice otras tareas de forma enmascarada).

2.2.10 RETINA

La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia interocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

2.2.11 IRIS [13] [14] [15]

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad, inalterable durante toda la vida de la persona.

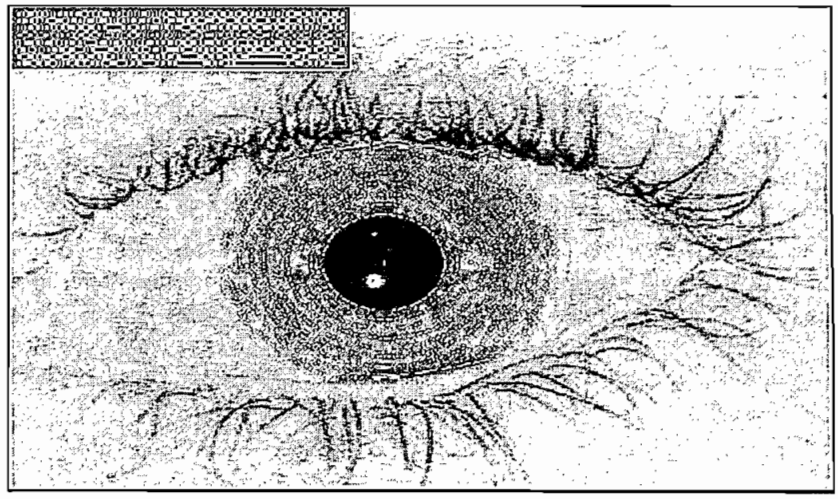


Figura 2.16 Iris humano con la extracción de su iris code

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 *KBytes*) suficiente para los propósitos de autenticación.

Esa muestra, denominada *iriscode* (código del iris) (en la figura 2.16 se muestra una imagen de un iris humano con su *iriscode* asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos. Para poder autenticar a una persona se realizan los siguientes pasos:

- Reconocer el borde.
- Estirar zona de interés (pupila)
- Clasificar el patrón.
- Distinguir la persona.

El reconocimiento consiste en averiguar espacialmente la ubicación de los bordes del iris en la imagen, para luego poder estirarlo. Con este objetivo se realiza una función a la que se le ingresa la imagen del ojo (como la observada en el inicio) y devuelve una **imagen** que contiene sólo la información relevante (se recorta la imagen original para que quede sólo el iris); el **centro** del iris de la imagen recortada; el **radio interior** del iris; y el **radio exterior**.

Los pasos para reconocer son:

- Determinar el centro del iris.

- Estimar el radio interior.
- Recortar la imagen.
- Estimar radio exterior.

2.2.11.1 Centro del iris

Determinar el centro del iris es lo mismo que hallar el centro de la pupila ya que son círculos concéntricos. Por medio de un histograma, se puede determinar con bastante exactitud la región de la pupila.

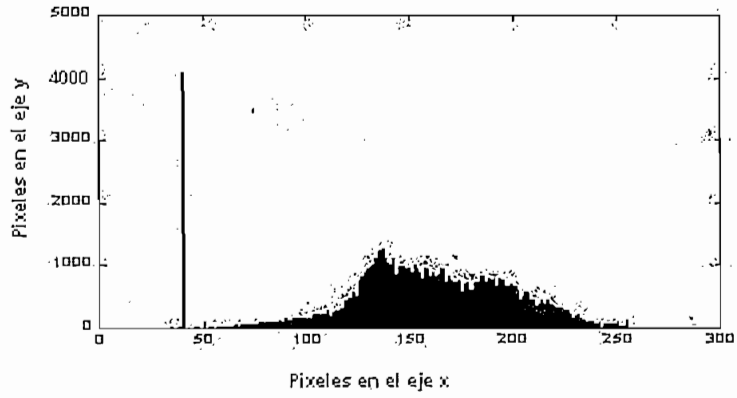


Figura 2.17 Histograma del centro del iris

A partir de esta información se puede analizar la imagen con la pupila, a esta imagen analizada se le realiza el promedio de los valores de las coordenadas de los píxeles en las dos direcciones por separado, obteniendo las coordenadas del centro de la pupila y el iris.

2.2.11.2 Radio Interior

Dada la imagen analizada del punto anterior y conociendo el centro, se puede contar la cantidad de píxel que hay a ambos lados del centro en una dirección.

Para disminuir el error se eligen las direcciones vertical y horizontal y se calculan los radios (dos por dirección) y se realiza el promedio.

2.2.11.3 Recortar la imagen

Como los ojos tienen dimensiones parecidas entre ellos y además se conoce las coordenadas del centro; se decide recortar la imagen 110 píxel desde el centro hacia las cuatro direcciones cardinales.

2.2.11.4 Radio exterior

Si se observa el histograma, tiene un segundo máximo cerca del valor 150, se puede probar que este máximo corresponde al radio exterior del iris. Si bien los resultados tienen más ruido que el caso del radio interior se puede distinguir con bastante claridad.

Al tener disponible ojos asiáticos, gran parte del iris está oculto por los parpados, por lo que el radio se estima sólo en una dirección siendo concientes del error introducido en algunas imágenes.

2.2.11.5 Estiramiento

Luego de haber estimado el centro de la pupila, el radio interno y externo del iris, la siguiente etapa es tomar una sección determinada del iris y "estirarla".

2.2.11.6 Sección elegida

La sección a tomar va estar limitada por los radios interno y externo del iris, ya que es ahí dónde se encuentra la información relevante. La pregunta ahora es, ¿con cuánta información podemos reconocer?

Si bien es cierto que cuanta más área se abarca, más información se tendrá no hay que olvidar que el algoritmo se vuelve más lento a medida que se aumenta el tamaño de las imágenes con que se trabaja.

Por otro lado, hay que considerar la posibilidad de que los ojos pueden ser de personas asiáticas, y éstos presentan una parte importante del parpado sobre el iris.

Después de varios experimentos los científicos han llegado a definir la sección comprendida entre -30 grados por debajo de la horizontal y 15 grados por encima, como se puede ver en la figura 2.18:

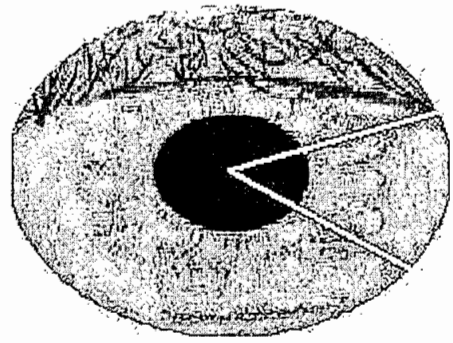


Figura 2.18 Sección elegida del iris

El siguiente paso es el estiramiento del área del iris elegida, para lo cual se realiza una interpolación lineal.

El resultado obtenido es:

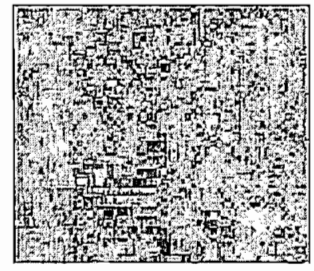


Figura 2.19 Interpolación de la región elegida

2.2.11.7 Clasificación

Luego de reconocer y estirar la parte del iris de interés, hay que clasificar el ojo para poder distinguir a quién pertenece. Según la bibliografía consultada [13] una forma práctica y simple es aplicar a la imagen estirada la **transformada del coseno discreto de Fourier.** Con la hipótesis de que cada ojo es diferente, entonces cada imagen tiene una transformada distinta, y se puede distinguir la influencia de determinadas frecuencias.

En este caso se separa la imagen en sectores (áreas con frecuencias similares). Se calcula el valor medio de cada sector, para luego comparar con los distintos ojos. Permitiendo así determinar la procedencia, ya que imágenes similares de ojos (de la misma persona) tiene valores en frecuencia muy parecidos.

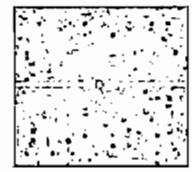


Figura 2.20 Transformada de Fourier de la figura 2.19

Si bien a simple vista no hay nada apreciable en particular, alcanza para poder distinguir en las distintas zonas los distintos aportes.

Para establecer las regiones de aporte de las distintas frecuencias en la imagen se tienen en consideración algunas propiedades de la transformada de Fourier. La transformada es simétrica por su punto medio, lo que facilita los cálculos (sólo se realizan en la mitad de la imagen). Además, alcanza sólo con utilizar un cuarto de la misma ya que no aporta información imprescindible.

Luego de probar la cantidad de zonas a considerar, se decide dividir en 8 regiones radiales y 7 tangenciales.

Figura 2.21 Regiones radiales y tangenciales de la imagen

A cada región se le asigna un número lo que posibilita calcular la media en cada región.

Para hacer el cálculo se realiza un **and** entre la transformada y cada región, y se almacena en un vector cuyo índice es el número de región de la imagen.

Una vez finalizado este proceso se necesita comparar los parámetros obtenidos con los de una base de datos.

2.2.12 GEOMETRÍA DE LA MANO

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quién dice ser.

Cuándo un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura como se observa en la figura 2.22. Una vez que la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias) en un formato de tres dimensiones. Transformando éstos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida, etc.); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas

situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

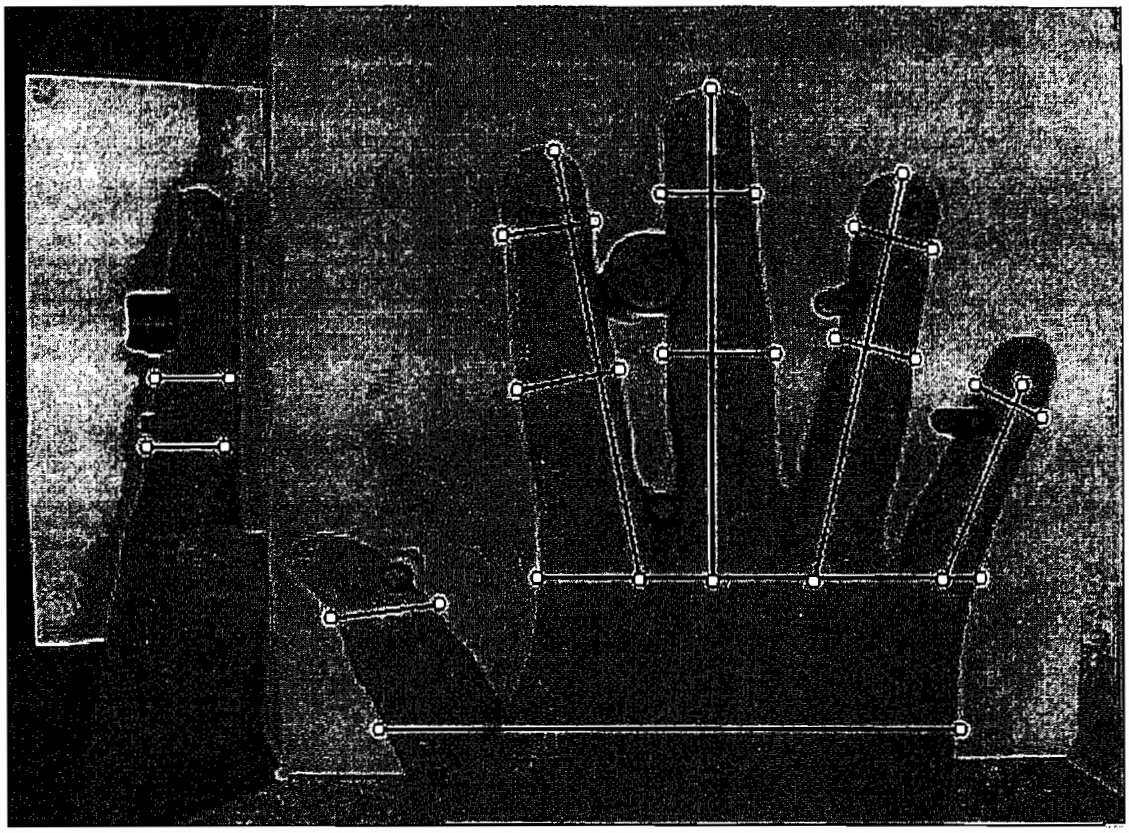


Figura 2.22 Geometría de una mano con ciertos parámetros extraídos

2.2.13 VERIFICACIÓN DE ESCRITURA

Aunque la escritura (generalmente la firma) no es una característica estrictamente biométrica, como hemos comentado en la introducción se suele agrupar dentro de esta categoría; de la misma forma que sucedía en la verificación de la voz, el objetivo aquí no es interpretar o entender lo que el usuario escribe en el lector, sino autenticarlo basándose en ciertos rasgos tanto de la firma como de su rúbrica.

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma.

En los modelos biométricos se utiliza además la forma de firmar, las características dinámicas (por eso se les suele denominar *Dynamic Signature Verification*, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo.

Como se mencionó anteriormente para utilizar este tipo de sistemas de autenticación se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características, el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente.

Contra este problema la única solución (aparte de una concientización de tales usuarios) es relajar las restricciones del sistema a la hora de *aprender* firmas, con lo que se decrementa su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuándo éstos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

2.2.14 VERIFICACIÓN DE LA VOZ [16]

El sistema verificador de voz también es conocido como reconocimiento de locutor el mismo que se divide en dos áreas: La Identificación de locutor, y la Verificación de locutor (VL). Un sistema de identificación de locutor asignará al usuario en cuestión la identidad del individuo registrado que mejor se aproxime a las características de la señal de voz. Por otra parte, un sistema de VL deberá decidir si la persona que declara una cierta identidad es o no quién dice ser. La pronunciación emitida por un locutor cualquiera es comparada con el modelo del cliente cuya identidad fue declarada.

De esta forma, si el modelo de locutor y la pronunciación coinciden dentro de los límites permitidos (umbral de decisión), la identidad será aceptada y en caso contrario será rechazada.

Como se puede ver, en este tipo de sistemas sólo existen dos respuestas posibles: aceptar o rechazar al locutor. Como se mencionó anteriormente se pueden tener problemas al momento en el que el sistema debe decidir si aceptar o negar la autenticación de la persona.

La tasa dónde se igualan la tasa de falso rechazo y la tasa de falsa aceptación es conocida como EER (*Equal Error Rate*) y es comúnmente utilizada como medida de desempeño en VL y otros sistemas biométricos.

Todos los sistemas de VL cuentan con una base de datos de usuarios registrados, denominados clientes. Esta base de datos está compuesta por modelos que representan las características del habla de cada uno de los clientes. Estos modelos se consiguen mediante el procesamiento de sesiones de entrenamiento en las cuales el usuario del sistema pronunciará varias frases.

Existen diversos tipos de sistemas de VL, entre ellos se pueden distinguir los sistemas de texto dependiente y los de texto independiente. Los sistemas de texto dependiente requieren que el usuario pronuncie una palabra o frase determinada por el sistema. Los sistemas de texto independiente están preparados para realizar el proceso de VL cualquiera sea la palabra o frase pronunciada.

Se pueden distinguir dentro de cada uno de éstos tipos de sistema aquellos de pronunciación continua o los de palabra aislada. En éstos últimos las palabras deberán estar separadas entre sí por pequeños instantes de silencio.

El estado del arte en VL permite llegar a EER entre 0,3% a 1% a bajos niveles de ruido. Con estas tasas de errores VL se presenta como una alternativa interesante si es utilizada en combinación con, por ejemplo, números de identificación personal.

Las investigaciones realizadas actualmente, concernientes a los tipos de ruidos involucrados y las técnicas de cancelación utilizadas, han ayudado a mejorar el desempeño de éstos bajo condiciones más ruidosas. De hecho, la robustez a niveles más severos de SNR (*Signal-to-Noise Ratio*) es fundamental para que estos sistemas tengan éxito en aplicaciones reales.

2.2.14.1 Medidas de desempeño

Los errores en un sistema de VL se producen al aceptar un impostor o al rechazar a un cliente. Es importante mencionar que si el sistema en cuestión posee un umbral de decisión demasiado estricto tenderá a rechazar clientes y si éste es demasiado permisivo tenderá a aceptar impostores, por lo que para aumentar el desempeño del sistema se deben minimizar conjuntamente ambos tipos de errores. Para encontrar el umbral de decisión óptimo se definen dos curvas: la curva de Falsa Aceptación y la curva de Falso Rechazo. La curva de Falso Rechazo se construye moviendo el umbral de decisión en un amplio rango e, identificando para cada uno de éstos puntos, qué porcentaje de las ocasiones en las cuales el cliente trató de verificarse y fue rechazado. Por su parte, la curva de falsa aceptación se obtiene desplazando el umbral de decisión e identificando para cada punto qué porcentaje de los impostores fue aceptado.

La intersección de éstas curvas indica el umbral óptimo para el cual se minimiza el error del sistema. Este umbral óptimo se denomina TEER por la abreviación en inglés de *Threshold of Equal Error Rate* y es definido a posteriori, es decir, luego de una serie de intentos de verificación tanto por parte del cliente como por

impostores. A partir del TEER se puede encontrar el porcentaje de error del sistema de VL (EER) al evaluar este valor en algunas de las curvas definidas anteriormente.

La figura 2.23 ilustra gráficamente la situación descrita; en ella se observan las curvas de falsa aceptación y falso rechazo cuya intersección corresponde al TEER.

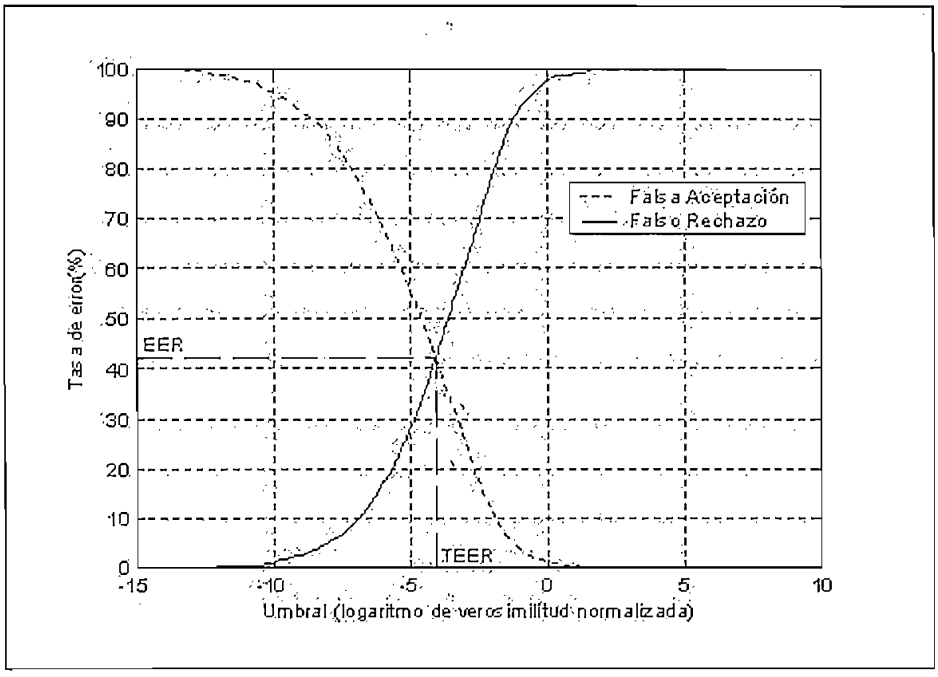


Figura 2. 23 Curvas de falsa aceptación y falso rechazo, TEER y EER.

Las curvas de Falsa Aceptación y de Falso Rechazo pueden ser construidas para cada uno de los clientes o ser el promedio para todos los usuarios. Así, el umbral de decisión puede ser optimizado para cada cliente $TEER_{SD}$ (TEER *Speaker Dependent*), o común a todos los usuarios, $TEER_{SI}$ (TEER Speaker *Independent*).

Los sistemas de VL requieren que los usuarios del sistema estén registrados, por esto se deben realizar sesiones de entrenamiento. El número y periodicidad de éstas influirá en el desempeño final del sistema de VL ya que un mayor número de elocuciones de entrenamiento genera un modelo más representativo del cliente. Además, al realizar sesiones separadas en el tiempo, se logra considerar las variaciones naturales en la voz del cliente asociados a estados de ánimo o de

salud. La diferencia de condiciones entre las sesiones de entrenamiento y de verificación influye en el desempeño del sistema, por lo que se debe procurar utilizar los mismos micrófonos o canales de transmisión en ambas instancias, o aplicar técnicas de compensación.

La señal de voz correspondiente a las sesiones de entrenamiento es sometida a una etapa de pre-procesamiento que consiste en un filtrado *anti-aliasing*, conversión análoga-digital, detección de inicio-y-fin de la señal de voz útil, y pre-énfasis. Posteriormente, en la etapa de extracción de parámetros, la señal se divide en cuadros o *frames*, se realiza una ponderación al interior de éstos por una ventana (ej. tipo *Hamming*) para luego realizar un análisis espectral que permitirá obtener los parámetros deseados. Con estos parámetros el sistema de VL deberá ser capaz de entrenar un modelo que represente al cliente. Por su parte, las elocuciones de verificación serán sometidas al mismo proceso, salvo que los parámetros obtenidos serán comparados con los modelos del cliente mediante la verosimilitud (en el caso de utilizar modelos estocásticos HMM). Si esta verosimilitud calculada es mayor que el umbral de decisión definido para el cliente en particular o para todo el conjunto de clientes, $TEER_{SD}$ ó $TEER_{SI}$, respectivamente, la identidad clamada por el locutor será aceptada.

Como se ha mencionado anteriormente, la señal de voz pre-procesada es dividida en *frames* considerando que dentro de cada una de estas ventanas la señal es estacionaria. El ancho de los *frames* (tramás) varía entre 10 ms y 30 ms. Existe un compromiso entre la resolución en el tiempo y en la frecuencia, por lo que la elección del ancho de los *frames* dependerá de cuánto se desea priorizar una ante la otra. Generalmente también se emplea una superposición entre *frames* consecutivos, con objeto de obtener una transición más suave entre ellos.

Dentro de cada *frame* se realiza algún tipo de análisis espectral que resulta en un conjunto de parámetros característicos del intervalo correspondiente. Este análisis se puede realizar con filtros DFT (*Discrete Fourier Transform*) o polinomios predictivos LPC (*Linear Prediction Coding*).

Los parámetros que se extraen dentro de un *frame* pueden ser estáticos o dinámicos. En el primer caso corresponden a una "fotografía" de la señal en el dominio espectral en la ventana en cuestión. En el segundo caso, los coeficientes miden la velocidad o aceleración de los parámetros estáticos.

	Ojo-Iris	Ojo-Retina	Huellas Dactilares	Geometría de la mano	Escritura-Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Baja	Baja	Alta	Alta	Media	Media
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas	Artritis, reumatismo	Firmas fáciles o cambiantes	Ruido, resfriados
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 2005 (USD)	5000	5000	1320	1832	1000	1200

Tabla 2.3 Comparación de métodos biométricos

2.3 ENCRIPCIÓN [3] [4] [6]

En el mundo real, si una universidad quiere proteger los expedientes de sus alumnos los guardará en un armario, bajo llave y vigilado, para que sólo las personas autorizadas puedan acceder a ellos para leerlos o modificarlos; si queremos proteger nuestra correspondencia de curiosos, simplemente usamos un sobre; si no queremos que nos roben dinero, lo guardamos en una caja fuerte. Lamentablemente, en una red no disponemos de todas estas medidas que nos

parecen habituales: la principal forma de protección va a venir de la mano de la encripción. La encripción de los datos nos va a permitir desde proteger nuestro correo personal para que ningún curioso lo pueda leer, hasta controlar el acceso a nuestros archivos de forma que sólo personas autorizadas puedan examinar (o lo que quizás es más importante, modificar) su contenido, pasando por proteger nuestras claves cuándo nos conectamos a un sistema remoto o nuestros datos bancarios cuándo realizamos una compra a través de Internet; para incrementar la seguridad en los métodos de autenticación antes mencionados se pueden utilizar métodos de encripción.

Un esquema de encripción convencional tiene cinco ingredientes (Fig. 2.24):

Texto plano (<<plaintext>>): es el mensaje original o datos que actúan como entrada al algoritmo.

Algoritmo de encripción: el algoritmo de encripción lleva a cabo varias substituciones y transformaciones en el texto plano.

Clave secreta: la clave secreta es también una entrada al algoritmo de encripción. Las substituciones y transformaciones exactas realizadas por el algoritmo dependen de la clave.

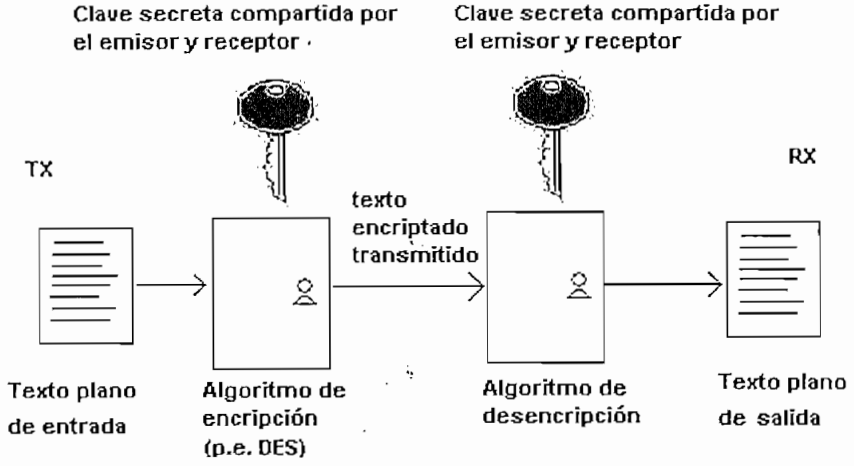


Figura 2.24 Modelo simplificado de la encripción simétrica

Texto encriptado: es el mensaje aleatorio que se produce en la salida. Depende del texto plano y de la clave secreta. Para un mensaje dado, dos claves diferentes producen dos textos encriptados diferentes.

Algoritmo de desencripción: es esencialmente el algoritmo de encripción ejecutado en sentido contrario. Toma como entradas el texto encriptado y la clave secreta y produce el texto plano original.

2.3.1 ENCRIPCIÓN CONTINÚA

Se encripta continuamente todas las letras o palabras, existe el problema de que al conocer la repetitividad en el lenguaje, se puede romper el código.

Una de las principales desventajas que tiene este tipo de encripción es que es susceptible a ataques por substitución, como ejemplos de éstos códigos podemos tener: código de Vernam, Rivest Chipre #4 (RC #4).

2.3.2 ENCRIPCIÓN EN BLOQUES

Se encripta y desencripta información en bloques fijos en lugar de hacerlo por cada letra o palabra. Se genera un bloque encriptado de mayor tamaño por lo que se consumen mayores recursos en almacenamiento o ancho de banda.

Como ejemplos de éstos códigos se pueden tener:

- Data Encryption Estándar (DES)
- International Data Encription Algoritm (IDEA).

2.3.3 RUPTURA DEL CÓDIGO

Tan pronto como se desarrolla un método de encriptamiento, hay gente tratando de romper el código, existen varios métodos para romper el código:

2.3.3.1 Conociendo el texto plano

Si se llega a conocer un texto antes de encriptar y su respectivo texto encriptado, se puede continuar desencriptando cualquier información.

2.3.3.2 Conociendo determinado texto plano

Depende de la habilidad de los interceptores para conocer un determinado texto encriptado. Como ejemplo se tiene la violación del código japonés en la segunda guerra mundial.

2.3.3.3 Criptoanálisis

Análisis matemático para romper un código, se requiere mucha habilidad y recursos computacionales. Una de las más famosas organizaciones dedicadas al criptoanálisis es la National Security Agency (NSA).

2.3.3.4 Fuerza bruta

Tratar de probar todas las combinaciones posibles

2.3.3.5 Ingeniería Social

Métodos no tecnológicos para tratar de obtener información de los códigos.

2.3.3.6 Substitución

Una parte de un mensaje previo es colocado en una respuesta, no se requiere romper el código.

2.3.3.7 Ataques de sincronismo

Teóricamente conociendo los tiempos requeridos para encriptar y desencriptar se puede romper el código.

2.3.4 ENCRIPCIÓN SIMÉTRICA

Esta técnica también llamada de clave única, era el único tipo de encripción en uso antes de la introducción del encripción de clave pública a finales de la década

de los 70. La encripción simétrica ha sido utilizada para las comunicaciones secretas por incontables individuos y grupos, desde Julio César hasta la fuerza Alemana de los U-boat y actualmente los diplomáticos, militares y los comerciantes. Es todavía el algoritmo de encripción más utilizado mundialmente de las dos técnicas de encripción.

Entre las ventajas que se tienen en este tipo de encripción es que es rápido, relativamente seguro y ampliamente entendido. Como desventaja se tiene que se requiere compartir información confidencial, además de tener una administración compleja y no tiene algún mecanismo de autenticación.

2.3.4.7 Data Encription Standard (DES)

Desarrollado por IBM en acuerdo con NSA a mediados de los año 70, la llave tiene 8 bytes cada byte tiene un bit de paridad por lo que se tiene 56 bits de longitud, este método de encripción es utilizado en ATMs (cajeros automáticos) y POS (puntos de venta).

2.3.4.8 International Data Encryption Algorithm (IDEA)

Es un método simétrico de código en bloque desarrollado por el Swiss Federal Institute en los años 90. Usa una llave de 128 bits, no tiene restricciones de exportación.

2.3.4.9 CAST

Soporta longitud variable de llaves, desde 40 hasta 256 bits. Utiliza bloques de 64 bits igual que DES, es de 2 a 3 veces más rápido que DES, fue desarrollado por Carlisle Adams y Strafford Travares y patentado por Entrust Technologies.

2.3.4.10 Rivest Chipher #4 (RC4)

Desarrollado por Ron Rivest de RSA, utiliza un tamaño variable de llave usualmente 128 bits, recientemente se aprobó la exportación de la versión de 40 bits, es utilizada en Nestcape Navigator e Internet Explorer.

2.3.5 ENCRIPCIÓN ASIMÉTRICA

Como ventaja de este método de encripción se tiene que no se necesita intercambiar información confidencial, además soporta autenticación y puede combinarse con mecanismos de encripción simétrica. Como desventaja se tiene que es lenta, se requieren recursos computacionales intensivos y se requiere de preferencia de una autoridad certificadora.

2.3.5.7 Diffie-Helman

Algoritmo desarrollado por Whitfield Diffie y Martin Hellman en la universidad de Standford, este algoritmo se puede utilizar para compartir claves secretas de manera segura por dos entidades que usan encripción simétrica. Utilizado en los protocolos de llaves de IPSEC.

2.3.5.8 Rivest, Shamir, Adelman (RSA)

Desarrollado en el MIT, RSA multiplica grandes números primos para generar claves, es utilizado en SSL.

2.3.5.9 Digital Signature Algorithm (DSA)

Es utilizado para firmas digitales.

2.3.6 INTEGRIDAD DE LOS MENSAJES

Para garantizar la integridad de los mensajes se usan algoritmos que aplicados a los mensajes dan un valor único, permitiendo a las partes involucradas en la comunicación verificar que los datos recibidos son auténticos. Éstos algoritmos se conocen como función hash y los valores resultantes son valores hash.

Existen varios algoritmos hashing, éstos algoritmos deben ser de una sola vía (el texto plano genera un valor hash y no al revés) y deben minimizar la posibilidad de colisiones (cada texto plano debe tener su único valor hash diferente a cualquier otro).

2.3.6.7 MD4 (Message Digest #4)

Fue desarrollado por Ron Rivest de RSA, se basa en una función que toma el mensaje de longitud variable y genera un valor hash de 128 bits.

2.3.6.8 MD5 (Message Digest #5)

Es una mejora de MD4, se crea un mensaje de 128 bits.

2.3.6.9 Secure Hash Algorithm-1 (SHA-1)

Es un algoritmo de una vía utilizado para crear firmas digitales, ligeramente más lento que MD4 y MD5 pero más seguro. Produce un valor hash de 160 bits que es más seguro contra ataques de fuerza bruta que el MD4 o MD5.

2.4 PRODUCTOS EXISTENTES EN EL MERCADO

2.4.1 INTRODUCCIÓN

Como se mencionó anteriormente el objetivo de este proyecto es el de proponer una solución de control de acceso físico, mediante el uso adecuado de la tecnología, para lo cual se utilizarán tarjetas inteligentes de proximidad y sistemas biométricos que utilizan el método de autenticación basado en la geometría de la mano. A continuación se explica por qué se decidió utilizar este tipo de tecnologías y no otras existentes en el mercado como son tarjetas magnéticas o dentro de la gama de sensores biométricos el sistema de autenticación basado en el iris del ojo.

2.4.2 SELECCIÓN DE LA TECNOLOGÍA

2.4.2.1 Selección del tipo de tarjetas

Como se mencionó en el análisis realizado acerca de las tarjetas magnéticas estas son una alternativa económica, para proveer una solución de control de

accesos, pero estas tienen algunas desventajas, entre las principales se pueden mencionar las siguientes:

- La capacidad de datos es baja. Pueden surgir problemas de espacio en aplicaciones que requieren demasiada información el máximo número de caracteres en la tarjeta (utilizando sus 3 pistas) es de 243 caracteres.

- La tarjeta magnética especificada por los estándares ISO y ANSI es vulnerable a la pérdida de datos causada por campos magnéticos producidos por fuentes magnéticas muy comunes, tales como imanes en pequeñas cantidades.

- La confiabilidad en la lectura de las tarjetas es pobre, con un porcentaje típico de falla en transacciones de 10%. Estudios dirigidos por el Doctor Denise Jeffreys de la Universidad de Mássachussets han mostrado que el 60% de las fallas en las transacciones es debido a la desmagnetización de las tarjetas.

- El estándar ISO/ANSI puede ser fácilmente copiado, falsificado y duplicado, llevando esto a significativos fraudes en el mercado.

Para proteger las instalaciones en nuestra institución, los criterios de diseño utilizados en este proyecto no se basan únicamente en el ahorro económico que traerán como consecuencia del control de acceso si se utilizarán algunas de estas tecnologías, también se toma en cuenta el crecimiento que tendrá la institución y los servicios complementarios que se pueden prestar.

En la actualidad las tarjetas magnéticas son menos utilizadas, por el otro lado las tarjetas inteligentes de proximidad han tenido un crecimiento significativo, el mismo que se evidencia en la confianza que obtienen los usuarios al utilizar esta tecnología, a continuación se presentan las ventajas que fueron primordiales para seleccionar este producto en la solución propuesta.

- Se pueden almacenar grandes cantidades de información, relacionada a la persona propietaria de la misma, por ejemplo en caso de un accidente se puede obtener la información de la tarjeta, en la cual se pueden especificar el tipo de sangre, número de teléfono, si la persona es alérgica a algún medicamento, etc.

- Otra aplicación relacionada con el control de acceso, sería almacenar en el chip de la tarjeta inteligente la información relacionada con la imagen de la persona, en caso de que la tarjeta sea robada, cuándo el lector detecta la tarjeta puede mostrar la fotografía del propietario de la misma, con lo cual un guardia puede comprobar la identidad de la misma, o en nuestro caso se puede expandir la solución para que los estudiantes, profesores, y trabajadores, puedan acceder a una sesión en una computadora y dependiendo del tipo de privilegios que tengan, podrán acceder solamente a cierta información.

- Este tipo de tecnologías puede utilizar métodos de encripción dependiendo del fabricante, para que la información pueda viajar en una forma más segura.

- Como se tratan de las tarjetas inteligentes de proximidad, se pueden disminuir los tiempos necesarios para realizar la autenticación, pues una persona que desea autenticarse no necesita sacar la tarjeta de su cartera, el lector la detectara automáticamente cuándo está se encuentre a una determinada distancia del lector de la misma, esto es muy necesario para definir la solución de acceso vehicular.

- Las tarjetas inteligentes de proximidad incrementan la facilidad para el usuario, disminuyendo el tiempo que le toma a una persona autenticarse en el sistema, debido a que el usuario no necesita sacar la tarjeta de su cartera para pasarla por el lector de tarjetas.

2.4.2.2 Selección del tipo de sistema de autenticación biométrico

Como se mencionó en el análisis referente a los sistemas de autenticación biométricos, estos sistemas analizan alguna característica física de las personas para autenticar a las mismas. Estos métodos de autenticación son utilizados en lugares dónde se tienen activos de suma importancia para las instituciones, como pueden ser centros de cómputo.

Para realizar la selección del tipo de solución de autenticación biométrico que se utilizará, se ha referido a la tabla 2.3, dónde se mencionan las ventajas y desventajas de cada uno de los sistemas de autenticación biométricos estudiados en este proyecto.

Otros métodos de autenticación biométricos, como el método que analiza el iris del ojo, pueden ser de alta fiabilidad, pero aquí viene la otra parte que es la más importante en un sistema de control de acceso físico, las personas que interactuarán con el mismo; a la mayoría de personas no le gustaría que obtengan otra información a la que los fabricantes pueden acceder de una manera oculta para el usuario como puede ser el tipo de enfermedades del usuario. Además el uso de estas técnicas no es muy amigable con las personas ya que la toma de la imagen será molesta, sin contar con que el costo es bastante elevado.

Por todos los motivos antes mencionados se seleccionó el método biométrico de autenticación basado en la geometría de la mano, el mismo que es un método de autenticación biométrico fiable, económico y lo más importante es aceptado por los usuarios.

Cabe recalcar que este tipo de tecnología se utilizara en sitios en los que el estudio determine que se debe usar.

2.4.3 SELECCIÓN DE PRODUCTOS

2.4.3.1 Introducción

Antes de entrar en detalles sobre las características de los principales productos existentes en el mercado, se procede a explicar cómo funcionan las partes que intervienen en los sistemas de control de acceso.

Un sistema de control de acceso, en general tiene las siguientes partes:

- Panel de control.
- Lector de tarjetas o lector biométrico.
- Interfaz entre el servidor y el panel de control.
- Servidor de administración.

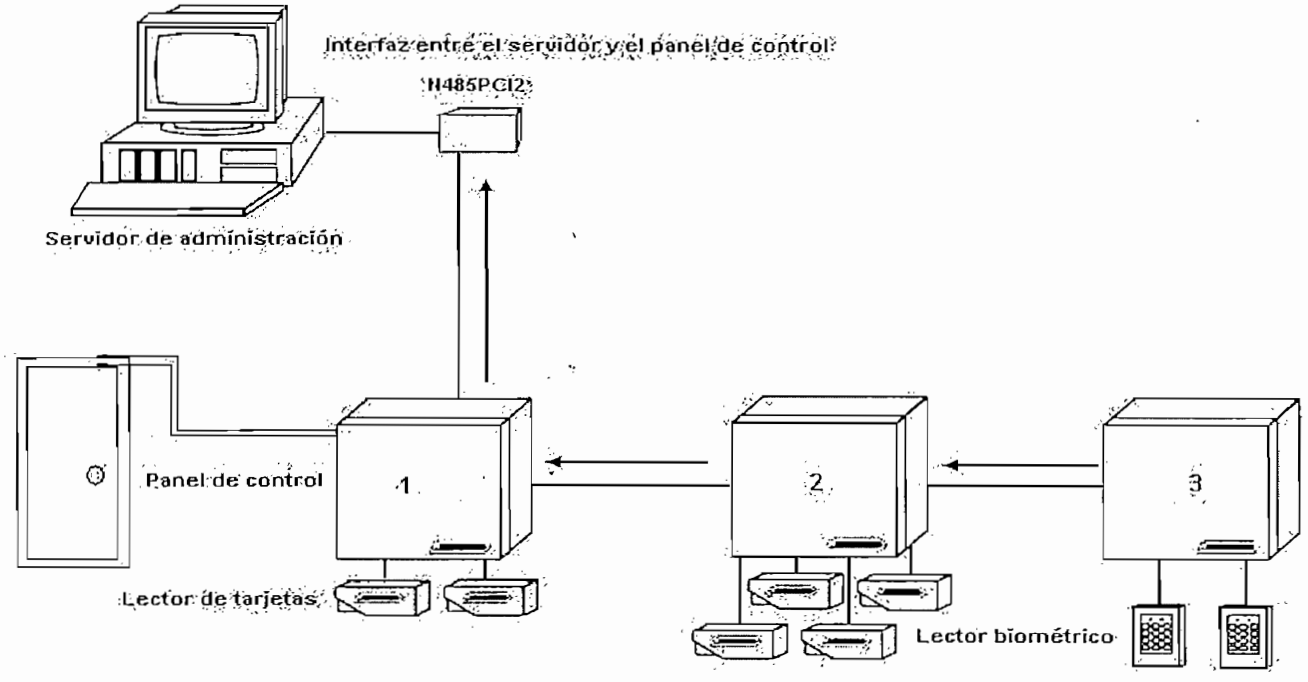


Figura 2.25 Partes de un sistema de control de acceso.

Como se mencionó anteriormente el panel de control es una parte fundamental dentro de un sistema de control de accesos, éste es el encargado de controlar las puertas, decidiendo si el usuario es válido, por lo general no es necesario alimentar eléctricamente al lector de tarjetas o al sensor biométrico ya que el panel de control envía una señal eléctrica por lo general 12 VDC hacia el dispositivo lector. Cabe recalcar que cada panel de control tiene una base de datos interna la cual le permite determinar si el usuario tiene o no privilegios de acceso a determinado lugar, cuándo un usuario ha sido autenticado el panel de

control activa un relé que pertenece al panel de control, el mismo que sirve para abrir el circuito que alimenta una cerradura electromagnética como se muestra en la figura 2.26 [c].

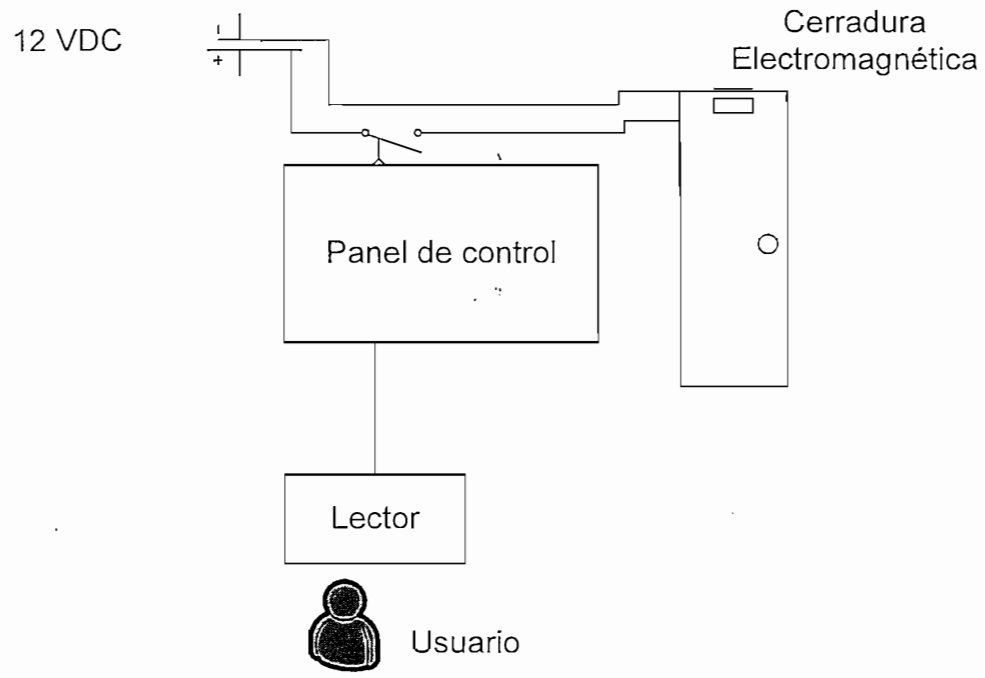


Figura 2.26 Esquema de funcionamiento del panel de control de acceso.

El lector de tarjetas o el lector biométrico, forman el interfaz que existe entre el sistema de control de acceso y el usuario final.

El interfaz que existe entre el servidor de administración y el sistema de control de acceso, permite al administrador del sistema de control de acceso, programar los paneles de control en una forma eficaz, cabe recalcar que los paneles de control pueden también ser programados en una forma independiente, pero esto consumiría demasiado tiempo, para el administrador.

El servidor de administración permite, monitorear continuamente al sistema de control de acceso, observando alarmas existentes en el sistema, como por ejemplo cuándo un usuario no autorizado trata de ingresar al sistema. Además

[c] Las cerraduras electromagnéticas se mantienen abiertas mientras se mantenga el circuito cerrado, por lo contrario las cerraduras eléctricas, necesitan que el circuito se cierre para que estas se abran.

facilita la programación del panel de control al administrador de la red, presentado un software amigable con interfaz gráfica.

A continuación se detalla los principales sistemas de control de acceso existentes en el mercado:

- Sistema de control de acceso propuesto por la empresa NORTHERN COMPUTERS, el mismo que consta de:
  - Paneles de control de acceso N-1000-III/IV
  - Lectoras de proximidad Miniprox Reader II
  - Sensor Biométrico de Recognition Systems Hand Key II
  - Software de Administración WINPACK-2.0

- Sistema de control de acceso propuesto por la empresa KERYSISTEMS, el mismo que consta de:
  - Paneles de control de acceso PXL-500
  - Lectoras de proximidad MS-5000
  - Tarjeta de proximidad KC-10X
  - Software de Administración D-LITE

- Sistema de control de acceso propuesto por la empresa MICROCIRCUITOS, el mismo que consta de:
  - Paneles de control de acceso basados en PLC's SIEMENS SYMATIC S7-200
  - Lectoras de proximidad SP-6820
  - Tarjetas de proximidad AWID
  - Software de Administración INTEL-SYS

2.4.4 PANELES DE CONTROL

2.4.4.1 Northern Computers N-1000-III/IV [20]

2.4.4.1.1 Introducción

Los paneles de control N-1000-III/IV de Northern Computers son las unidades que toman la decisión de permitir o no el acceso en un sistema de control de acceso. Cada panel de control contiene una unidad central de procesamiento (CPU) y memoria para controlar el acceso a puertas o el brazo mecánico para permitir el acceso vehicular. La base de datos del panel de control es programada a través de un dispositivo de programación central (servidor). Una vez que los paneles de control han sido programados operan independientemente del dispositivo programador.

Para poder programar los paneles de control de acceso se necesita un interfaz de programación, el mismo que actúa entre el servidor de administración y los paneles de control.

El dispositivo de interfaz puede ser un N-485-PCI-2 o N-485-HUB-2, se pueden colocar hasta 31 paneles en el lazo de seguridad tipo bus como se muestra en la figura 2.26, "además de este tipo de configuración existe otro tipo de lazo de comunicaciones en forma de anillo utilizado en versiones anteriores como el N1000-II", éstos dispositivos proveen un interfaz RS-232 hacia el servidor de administración, y un interfaz RS-485 hacia los paneles de control de acceso, si se necesita tener una red de control de acceso extendida, como por ejemplo en un campus, se emplea un adaptador RS232 a ehternet mediante el dispositivo LAN485 al inicio del lazo, el mismo que provee un interfaz ethernet, de esta forma el lazo de control de acceso funciona como un dispositivo de red, como se muestra en la figura 2.27.

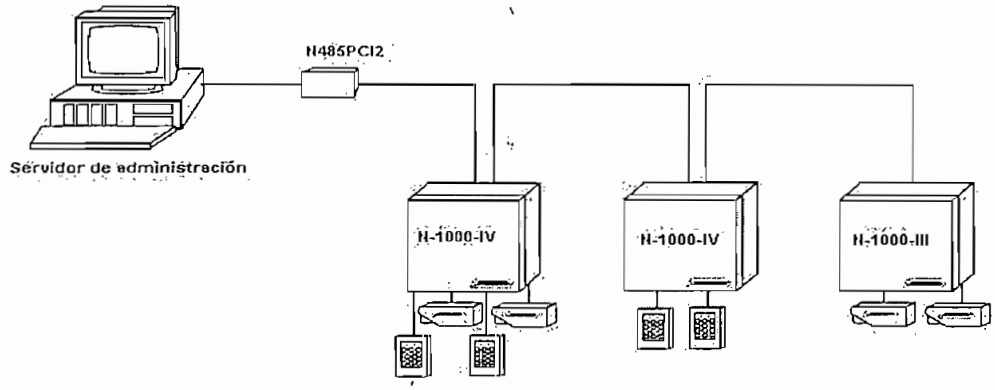


Figura 2.27 Lazo de comunicaciones con un dispositivo de interfaz N-485-PCI-2, red de control de acceso local.

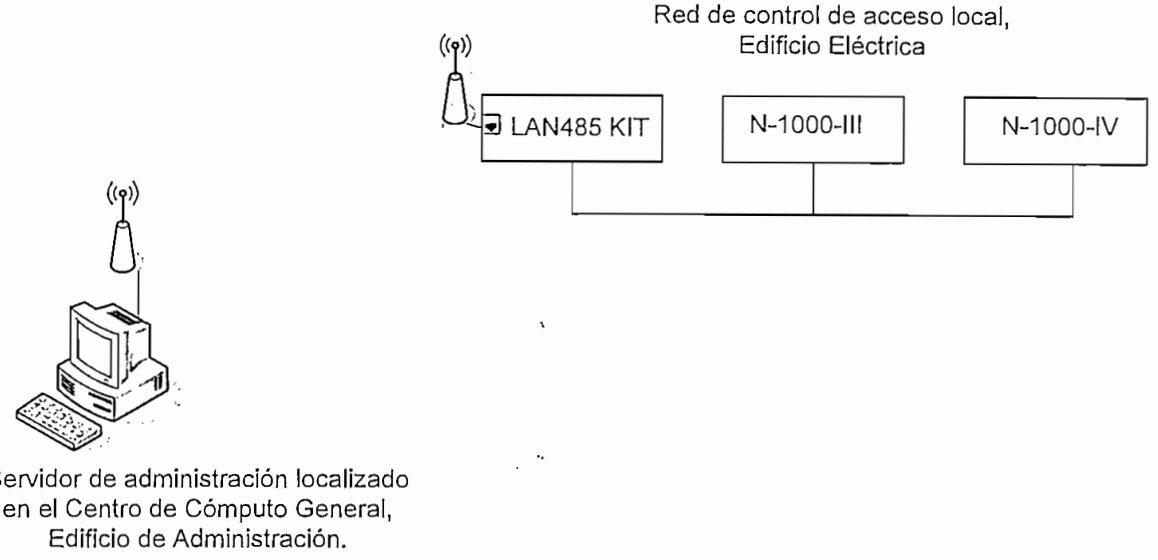


Figura 2.28 Red de control de acceso de campus.

El panel de control N-1000-III puede controlar hasta 2 puertas.

El panel de control N-1000-IV puede controlar hasta cuatro puertas. A continuación se presentan las especificaciones técnicas de éstos dispositivos. Los dos tipos de paneles soportan hasta 16 alarmas [d].

2.4.4.1.2 Especificaciones del hardware

Requerimientos de energía:

Los paneles N-1000-III/IV requieren un voltaje alterno de 16.5 VAC, 60 HZ o 12 voltios continuos (2 Amperios continuos).

Fuente de Salida:

Los paneles N-1000-III/IV proveen 12 VDC, con una corriente de 500 mA para los lectores de tarjetas que requieren 12 VDC. Además pueden administrar 5 voltios continuos para los lectores de tarjetas con requerimientos específicos.

Procesador de 8 bits

[d] Se considera una alarma como un evento no deseado, como puede ser el forzamiento de una cerradura.

Batería de respaldo:

Se tiene una batería adicional en estos paneles, que proporciona un voltaje continuo de 12 voltios, esta batería provee alrededor de 4 horas de operación continua (dependiendo de la carga y el tiempo que tenga la batería). Para mantener el máximo respaldo de energía se recomienda reemplazar la batería cada 4 años, o cada dos años si el sistema opera a altas temperaturas.

Respaldo de memoria:

Una pila de litio retiene la información almacenada en la memoria del panel de control, en caso de pérdida de energía o del respaldo de la misma, durante 7 días (dependiendo de la temperatura del ambiente y del circuito integrado de la RAM).

Fusibles:

Se tienen fusibles de 3 amperios, no se pueden cambiar, se restablecen automáticamente. Dependiendo de la sobrecarga y la temperatura esta operación puede tomar varios minutos, para que el fusible se restablezca.

Puntos de salida por medio de relés:

Estos tipos de paneles proveen cuatro polos dobles, 8 salidas de relé en total, por lo tanto el relé puede estar normalmente abierto o normalmente cerrado, estos mecanismos son utilizados para cerrar o abrir un circuito, por ejemplo una cerradura electromagnética.

Temperatura de operación:

2° C a 43° C

Rango de humedad:

0% a 85 % de humedad relativa, sin condensación

Número máximo de tarjetas:

Cada panel de control puede soportar hasta 5.000 tarjetas, además se puede extender la memoria en caso de requerir soportar mayor número de tarjetas.

Dimensiones de la caja de protección:

Altura: 36 cm

Ancho: 40.6 cm

Profundidad: 10.2 cm

Peso, incluido la caja de protección y la batería de respaldo:

9.5 kg.

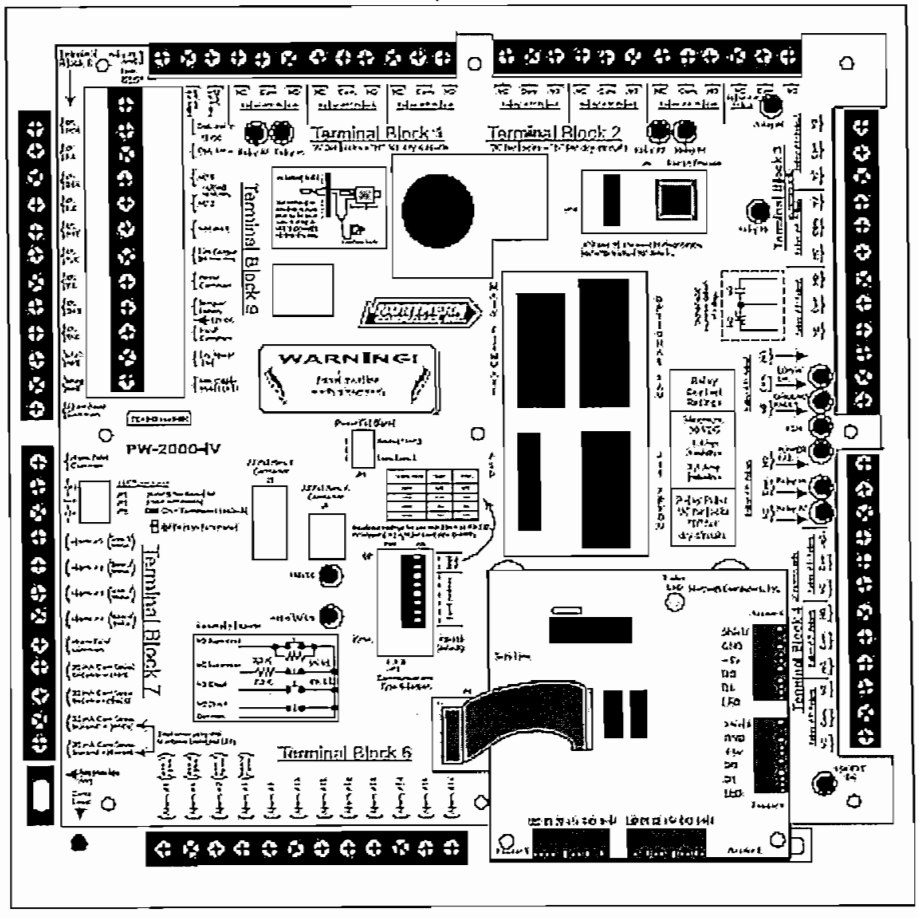


Figura 2.29 Panel de control de acceso N-1000-IV.

2.4.4.2 Kerysistems PXL-500 [19]

2.4.4.2.1 Introducción

Los paneles de control PXL-500 proporcionan soluciones de control de acceso sofisticadas para controlar hasta 128 puertas en una sola red y miles de puertas en una red WAN en varios sitios remotos, además estos paneles de control pueden controlar el acceso vehicular, considerando el brazo mecánico como una puerta.

Los paneles de control PXL-500 contienen toda la funcionalidad de entrada/salida necesaria para controlar dos puertas además de proporcionar 4 tipos de alarmas.

Cada panel de control tiene un interfaz RS-485 para la conexión a otro PXL-500 (hasta 128 por red) y un interfaz RS-232 para realizar la conexión hacia el servidor de administración, el mismo que se comunica con el primer PXL-500 en la red, si se desea realizar una red de control de acceso extendida, cada panel de control necesita tener una tarjeta adicional para obtener una salida ethernet.

2.4.4.2.2 Especificaciones del hardware

Requerimientos de energía:

12 VDC, 1 A

Respaldo de memoria:

Batería de litio para mantener la información almacenada en la RAM y el reloj, durante 5 días.

Temperatura de operación:

-18° C a 60° C

Rango de humedad

0% a 90 % de humedad relativa, sin condensación

Número máximo de tarjetas:

500 tarjetas por controlador.

Dimensiones de la caja de protección:

Altura	32.02 cm.
Ancho	22.86 cm.
Profundidad	10.16 cm.

Peso:

1.99 Kg

Número de alarmas: 4

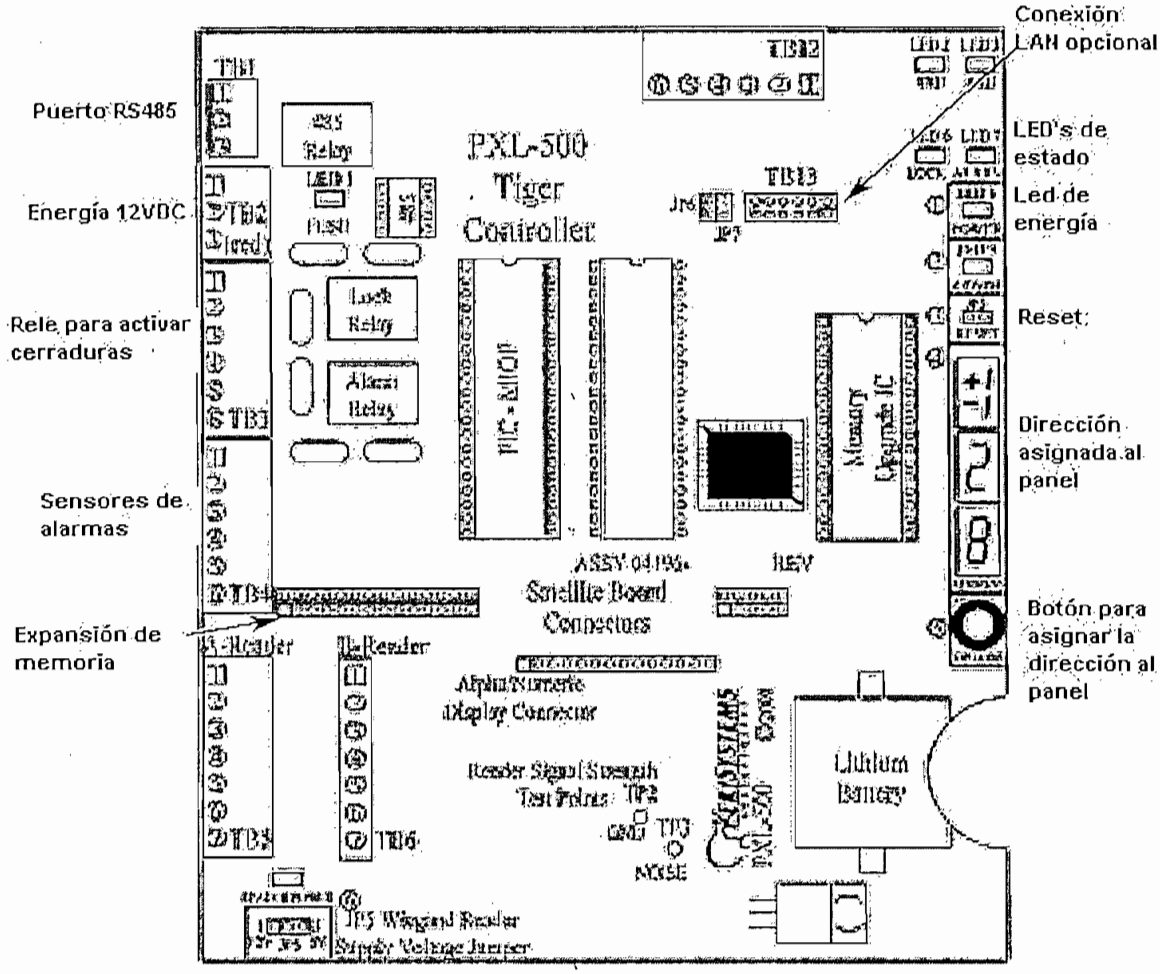


Figura 2.30 Panel de control PXL-500

2.4.4.3 Siemens Simatic S7-200/CPU 226 Micro System [21]

2.4.4.3.1 Introducción

Los paneles de control de Siemens, basados en PLCs permiten realizar la automatización de cientos de aplicaciones, como por ejemplo controlar luces, niveles de calor, niveles de agua, etc. Como el motivo de este proyecto de titulación define una solución de control de acceso físico, se tomará una pequeña parte de esta alternativa, éstos paneles de control pueden controlar hasta dos puertas, se considera un brazo mecánico de acceso vehicular como una puerta más, además trae la opción de conectar el panel de control en red mediante un dispositivo adicional.

Cabe recalcar que para realizar una red de control de acceso extendida se debe colocar un convertidor RS-485/ethernet al inicio del lazo de control de acceso local.

2.4.4.3.2 Especificaciones del hardware

Requerimientos de energía.

85 - 240 VAC (Voltios alternos, 60 Hz).

Fuente de salida:

24 VDC.

Batería de respaldo:

No provee batería de respaldo.

Respaldo de memoria mediante un capacitor de 5 F.

50 h.

Temperatura de operación.

0 a 55°C.

Número máximo de tarjetas.

5.000 tarjetas por panel.

Capacidad para conectar dos lectores de tarjetas con interfaz RS232.

Microprocesador de 16 bits, con memoria de programa y datos.

24 tipos de alarmas.

24 entradas y 16 salidas con capacidad de 2 Amperios cada uno.

Tiempo de procesamiento:

0.37 µs.

Dimensiones.

Altura: 80 mm

Ancho: 90 mm

Profundidad: 62 mm

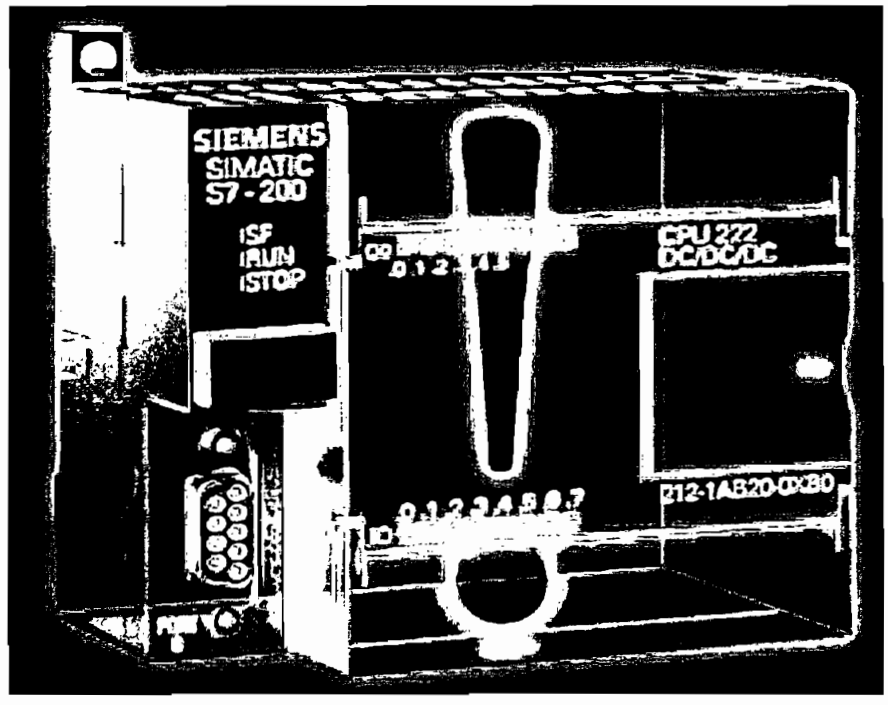


Figura 2.31 PLC SIMATIC S7-200/CPU226

2.4.5 LECTORES DE TARJETAS DE PROXIMIDAD

2.4.5.1 HID Miniprox Reader ProxCard II [22]

2.4.5.1.1 Introducción

Esta marca de lectores de tarjetas proximidad es compatible con la marca de paneles de control de Northern Computers, puede ser fácilmente instalada en interiores o exteriores. Además este lector proporciona ayuda visual, mediante un led que se mantiene en color rojo, si el usuario ha sido autenticado correctamente éste cambia de color a verde.

2.4.5.1.2 Especificaciones del hardware

Rango máximo de lectura:

Hasta 14 cm.

Dimensiones:

Altura	15.2 cm
Ancho	4.3 cm
Profundidad	2.5 cm.

Material:

Poli carbonato UL 94

Fuente de alimentación:

5 a 16 VDC

Requerimientos de corriente:

Promedio: 30 mA (5 VDC); 20 mA (12 VDC)

Máximo: 110 mA (5 VDC); 110 mA (12 VDC)

Temperatura de operación:

-30 °C a 65°C

Humedad de operación:

0-95% de humedad relativa, sin condensación

Peso:

108 gm

Frecuencia de transmisión: 125 KHz

Distancia máxima del cable entre el panel de control y el lector de tarjetas: 150 m.

Cable recomendado:

ALPHA 1295 (22 AWG) 5 conductores, con blindaje.

Seguridad:

La trama consta de 85 bits para la identificación, generando un total de 137 billones de códigos únicos, además utiliza encripción DES.

Figura 2.32 Lector de Tarjetas HID Miniprox Reader ProxCard II

2.4.5.2 Kerysistems Proximity Readers MS-5000 [19]

2.4.5.2.1 Introducción

Este tipo de lectores de tarjetas de proximidad es compatible con la marca de paneles de control KERISYSTEMS PXL-500.

2.4.5.2.2 Especificaciones del hardware

Rango máximo de lectura:

Hasta 15cm.

Dimensiones:

Altura:	10.9	cm
Ancho:	7.6	cm
Profundidad:	1.0	cm

Fuente de alimentación:

5-14 VDC

Requerimientos de corriente:

Típico 100 mA

Temperatura de operación

-40° C a 65°C

Peso:

90g

Frecuencia de operación:

125 KHz frecuencia de excitación, 62.5 KHz obtención de la información

Distancia máxima desde el panel de control hasta el lector de tarjetas:

100 m.

Tipo de cable. Sin especificación.

Seguridad: Sin especificación.

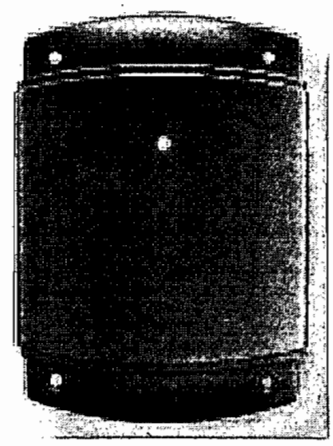


Figura 2.33 Lector de tarjetas de proximidad MS-5000

2.4.5.3 AWID Sentinel-Prox SP-6820 [23]

2.4.5.3.1 Introducción

Este tipo de lector de tarjetas de proximidad es compatible con los paneles de control de SIEMENS SIMATIC ST-200. Este tipo de lectores es ideal tanto para exteriores como para interiores.

2.4.5.2.2 Especificaciones del hardware

Rango de lectura:

15.2-20.3 cm

Dimensiones:

Alto	11.7 cm
Ancho	7.9 cm
Profundidad	1.7 cm

Fuente de alimentación

5-12 VDC

Requerimientos de corriente

Típico 50-80 mA

Temperatura de operación

-35° C a 65° C

Humedad de operación:

0 a 95% sin condensación

Peso:

227 g

Frecuencia de transmisión:

125 kHz

Formatos de salida

Wiegand y RS-232

Cable:

5 conductores (#22 AWG) con blindaje.

Seguridad:

Sin especificación

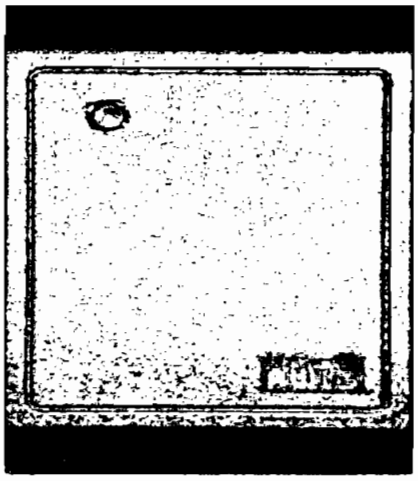


Figura 2.34 Lector de tarjetas de proximidad SP-6820

2.4.6 SENSORES BIOMETRICOS BASADOS EN LA GEOMETRIA DE LA MANO

2.4.6.1 IR Recognition Systems HandKey II [24]

2.4.6.1.1 Introducción

Recognition Systems, Inc. provee seguridad y conveniencia de la tecnología de autenticación biométrica, al alcance de la mayoría las aplicaciones de control de acceso. El HandKey II utiliza la tecnología de autenticación biométrica basada en la geometría de la mano, verifica el tamaño y forma de la mano de una persona en menos de un segundo, este tipo de tecnologías es compatible con los paneles de control de Northern Computers.

2.4.5.2.2 Especificaciones del hardware

Dimensiones:

Altura	29,6 cm.
Ancho	22,3 cm.
Profundidad	21,7 cm.

Peso:

2,7 kg

Tiempo de verificación:

Menos de un segundo

Alimentación de energía:

12-24 VDC

Retención de memoria:

Hasta 5 años mediante una batería de litio.

Longitud del código de identificación.

1 a 10 dígitos mediante el teclado, o lector de tarjetas

Puerto de comunicación:

RS-485 (4 hilos), soporta Impresora serial RS-232 (imprimir los reportes de una forma independiente del software de administración)

Velocidad de transmisión:

1.200 a 28,8 Kbps

Capacidad de usuarios:

512 Usuarios, expandidle a 3.2512.

Batería de Respaldo:

Hasta 3 horas en funcionamiento total.

Emulador de lector de tarjetas:

Puede emular un lector de tarjetas magnéticas, de códigos de barras y tarjetas inteligentes, facilitando la operación en una red de seguridad mixta.

Opcional:

BB-200 Batería de respaldo de operación
MD-500 MODEM Interno de alta velocidad
EN-200 Módulo de comunicación Ethernet
EM-801 Memoria de expansión hasta 9.728 usuarios
EM-803 Memoria de expansión hasta 32.512 usuarios
DC-102 Convertidor RS-232 a RS-485
KP-201 Teclado auxiliar
PROX Lector de tarjetas HID

Figura 2.35 HandKey II

2.4.6.2 IR Recognition Systems Handpuch3000

2.4.6.2.1 Introducción

IR Recognition Systems, es un sistema de tecnología biométrica, para el control de acceso y asistencia del personal. HandPuch 3000 verifica la identidad de la persona que desea autenticarse en menos de 1 segundo.

2.4.6.2.2 Especificaciones del hardware

Dimensiones:

Altura: 29.6 cm

Ancho: 22.3 cm.

Profundidad: 21.7 cm

Peso:

2.7 kg

Tiempo de verificación:

Menos de 1 segundo

Alimentación de energía:

12-24 VDC o 12-24 VAC 50/60 Hz

Retención de memoria:

Hasta 5 años mediante una batería interna de litio

Longitud del código de identificación:

De 1 a 10 dígitos

Velocidad de transmisión:

1.200 – 28,8K bps

Puerto de comunicación:

RS-485 (4 hilos) soporta conexión en red, además tiene un puerto serial para conectar una impresora.

Capacidad de usuarios:

512 Usuarios, expandidle a 32.512

Control de puertas:

Controla una puerta.

Opcional:

BB-200 Batería de respaldo

MD-500 MODEM Interno de alta velocidad

EN-200 Tarjeta de comunicaciones ethernet

BC-100 Lector de códigos de barras (sobre montado)

EM-801 Memoria de expansión hasta 9.728 usuarios

EM-803 Memoria de expansión hasta 32.512 usuarios

DC-102 Convertidor RS232 a RS485.

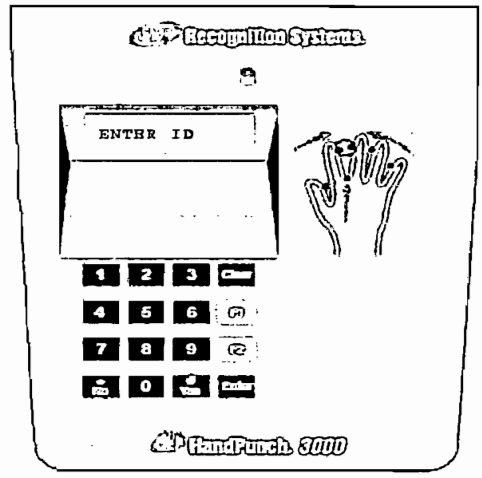


Figura 2.26 HandPuch 3000

2.4.7 SOFTWARE DE ADMINISTRACIÓN PARA LOS SISTEMAS DE CONTROL DE ACCESO.

2.4.7.1 Northern Computers WIN-PACK 2.0 [20]

2.4.7.1.1 Introducción

WIN-PAK 2.0 es la última versión de la industria. WIN-PAK 2.0 ha realizado innovaciones como es la integración de monitoreo de video digital, además puede

ser instalado en Sistemas Operativos como, Windows 2000 y Windows NT 4.0. Utiliza arquitecturas de bases de datos flexibles y robustas como Microsoft SQL Server 2000 o SQL Server 7.

2.4.7.1.2 Beneficios obtenidos

Control de acceso utilizando (N-1000-III/IV)

- Número total de tarjetas:
  Ilimitado con el software WIN-PAK 2.0.
  5.000 tarjetas por cada panel de control N-1000-III/IV con opción de expansión de memoria.

- Zonas de tiempo: Sin límite con el software WIN-PAK 2.0 / 32 por cada panel de control N-1000-III/IV.

- Almacenamiento de información de control de acceso en tiempo real, la cantidad de información almacenada se encuentra limitada únicamente por el dispositivo de almacenamiento.

- Número máximo de controladores: ilimitado, dependiendo del tipo de conexión de red, LAN o WAN.

- Número máximo de lectores: ilimitado, dependiendo del tipo de conexión de red.

- Controlador de ascensor: Hasta 32 grupos definidos controlando hasta 27 paradas.

Monitoreo de alarmas:

- Puntos monitoreados: 31.744.

- Alarmas del tipo Pop-up cuándo se detecta una alarma se puede desplegar una pantalla mostrando el video del lugar en que se detectó la alarma.

- Passwords para usuarios: 5.
- Ejecución de diferentes archivos de sonido, uno diferente para cada evento.

Tecnología Soportada:

- Lectores de Proximidad
- Teclado
- Lectores de banda magnética
- Lectores de códigos de barras
- Biométricos (Mano)
- Integración de video Digital y CCTV.
- Activación desactivación de tarjetas.

2.4.7.1.3 Requerimientos mínimos del hardware

Para sistemas pequeños de uno a 10 lectores con un máximo de hasta 250 tarjetas en total, y dos puertos de comunicación serial, se recomienda la siguiente configuración mínima.

- CPU Pentium II de 233Mhz
- RAM de 256 megabytes
- Disco duro de 2.1GB

- 2 Puertos de comunicación serial
- Disco de respaldo de Video.
- 1 puerto paralelo
- Monitor de 15" SVGA
- Sistemas Operativos Soportados:
  - Microsoft® Windows NT 4.0 con Service Pack 6
  - Windows 98SE (solo como Workstation).

Nota.- Esta configuración es suficiente para una estación de trabajo pero esta no es suficiente para que sea utilizada como servidor.

Para sistemas de control medianos, incluyendo identificación mediante una fotografía, sistemas que tienen de 1 a 100 lectores y soportan hasta 5.000 tarjetas, y hasta 8 puertos de comunicación seriales, se recomienda la siguiente configuración mínima en hardware la misma que puede ser utilizada como estación de trabajo o como servidor. Además esta configuración puede ser utilizada para sistemas stand-alone (estaciones de trabajo). El incremento de RAM podría mejorar el desempeño del sistema.

- CPU Pentium III de 700Mhz
- RAM de 256 megabytes
- Disco duro SCSI de 6 GB
- Dos puertos de comunicación serial.
- Disco SCSI de respaldo de video de 8 GB

- 1 puerto paralelo
- Monitor de color de 17" (1024 x 768 píxeles)
- Sistemas Operativos Soportados:
  - Microsoft® Windows 2000 Professional, con Service Pack 2;
  - Microsoft® Windows NT 4.0 Service Pack 6.
- SQL Server 7

Para sistemas que son utilizados en redes de control de acceso de área extendida, con alta capacidad de lectores, soportando sobre las 25.000 tarjetas, esta configuración puede ser utilizada como servidor.

- CPU Pentium 4 de 2Ghz.
- RAM de 512 megabytes
- Disco duro de 18 GB, 15.000rpm SCSI
- Dos puertos de comunicación serial
- Disco de respaldo de video de 20 GB SCSI
- 1 puerto paralelo
- Monitor SVGA de 19" (1280 x 1024 píxeles)
- Sistemas operativos soportados:
  - Microsoft® Windows 2000 Professional con Service Pack 2
  - Microsoft® Windows NT 4.0 Service Pack 6

- SQL Server 2000.

NOTA.- Es recomendado utilizar múltiples procesadores para los sistemas de gran alcance.

2.4.7.2 Kerysistems, D-LITE [19]

2.4.7.2.1 Introducción

D-Lite es un software que le permite administrar de una forma sencilla, la base de datos, dónde se almacena información relacionada a las tarjetas de proximidad de KERISYSTEMS. El programa le proporciona una interfaz amistosa al usuario para poder facilitar la administración de la red de seguridad. Además se tiene una extensa ayuda vía online. La comunicación entre el programa de D-Lite y el panel de control se hace a través de una conexión serial, directa entre el lector de tarjetas y un puerto serial en la computadora de administración. El programa de D-Lite puede administrar hasta 500 tarjetas por unidad de panel de control y puede manejar un número casi ilimitado de unidades de paneles de control.

2.4.7.2.2 Requerimientos mínimos del hardware

- Procesador Celaron o Pentium de 90 MHz.
- RAM de 128 MB
- Disco duro de 20 GB
- Monitor SVGA (800x600 pixels de resolución)
- CD-ROM
- Teclado

- Mouse
- Un puerto Serial libre
- Sistemas operativos soportados:
  - Windows 95™, Windows 98™, Windows NT™.

2.4.7.3 Microcircuitos INTEL-SYS

2.4.7.3.1 Introducción

Este software le permite administrar de una forma sencilla, la base de datos, dónde se almacena información relacionada a las tarjetas de proximidad de AWID. El programa le proporciona una interfaz amistosa al usuario para poder facilitar la administración de la red de seguridad, además de facilitar la administración de otras aplicaciones que se pueden realizar con los PLCs como son, el control de la iluminación.

2.4.7.3.2 Beneficios obtenidos

- Base de datos para soportar un número ilimitado de usuarios.
- Base de datos para definición de máximo 30 horarios (zonas de tiempo)
- Programación horaria para activación / desactivación de sensores.
- Capacidad para combinar usuarios, niveles de acceso y zonas de tiempo sin restricción.
- Reportes de accesos e intrusión, con diferentes opciones de clasificación y selección de información.
- Monitoreo permanente de los paneles de control, sensores y demás puntos de información.

- Indicación de alarmas, con priorización y ayuda en línea
- Lenguaje de comunicación con el operador: español
- Capacidad de generación de reportes, con opciones de configurar los formatos de presentación y filtros.
- Capacidad para incluir en la base de datos de usuarios, la fotografía digitalizada.
- Capacidad de configurar el sistema para que las transacciones de usuario disparen la presentación de datos y fotografía del mismo.

2.4.7.3.3 Requerimientos mínimos del hardware

- CPU Pentium II de 233Mhz
- RAM de 256 megabytes
- Disco duro de 2.1GB
- 2 Puertos de comunicación serial
- 1 puerto paralelo
- Monitor de 15" SVGA
- Sistemas Operativos Soportados:
  - Microsoft® Windows NT 4.0.
  - Windows 95.
  - Windows 98SE.

2.4.8 SELECCIÓN DE LA MEJOR OPCIÓN PARA EL SISTEMA DE CONTROL DE ACCESO.

2.4.8.1 Primera opción (NORTHERN COMPUTERS):

2.4.8.1.1 Introducción

La solución considerada cómo primera opción consta de los siguientes elementos:

- Paneles de Control de Northern Computers N-1000-III/IV.
- Lector de tarjetas de proximidad HID Miniprox Reader ProxCard II.
- Tarjetas inteligentes de proximidad HID ISO PROX II.
- Sensor Biométrico, IR Hankey II.
- Software de administración de Northern Computers, WINPACK 2.0.

2.4.8.1.2 Ventajas

- Red de seguridad mixta, es decir se tendrán trabajando conjuntamente los sistemas de lectores de tarjetas inteligentes de proximidad y los sensores biométricos.
- Los paneles de control de acceso pueden controlar dos o 4 puertas, dependiendo del modelo que se utilice.
- Se pueden tener hasta 16 tipos de alarmas para controlar cada una de las puertas, como por ejemplo se puede detectar si la puerta no se ha cerrado correctamente, o si ha existido un intento de violación de acceso.
- Se pueden tener redes de control de acceso de área extendida, mediante la utilización de un convertidor RS-485 / ethernet al inicio de la red de control de acceso local.

- Se dispone de una batería de respaldo, la misma que permite al sistema de seguridad trabajar sin alimentación eléctrica durante 4 horas.

- Cada uno de los paneles de control puede almacenar información de hasta 5.000 tarjetas, cabe recalcar que la memoria puede ser ampliada para soportar un mayor número de tarjetas.

- Respaldo de memoria mediante una batería de litio, la información almacenada en la memoria puede permanecer en la misma hasta 7 días, sin energía.

- Los lectores de proximidad pueden detectar una tarjeta hasta 14 cm de distancia.

- Los lectores de proximidad pueden ser colocados a una distancia máxima de 150 m del panel de control.

- Los lectores de proximidad pueden trabajar tanto en interiores como exteriores.

- La información viaja encriptada entre el lector de tarjetas y el panel de control.

- El software de administración es fácil de utilizar, permite monitorear continuamente las alarmas, permite integrar al sistema de control de acceso el monitoreo de un circuito cerrado de televisión.

- El rango de temperatura de operación lo hace ideal para trabajar en climas como el del Ecuador.

- El sensor biométrico Hand Key II puede ser utilizado como un emulador de un lector de tarjetas inteligentes.

- El software de administración permite imprimir en las tarjetas inteligentes de proximidad la foto de identificación del usuario, nombre del usuario, CI (cédula de identidad) y el logotipo de la empresa o institución.

2.4.8.1.3 Desventajas

- La información encriptada sólo puede viajar de los lectores de tarjetas hacia el panel de control, pero la información viaja sin ninguna protección desde el sensor biométrico que en nuestra solución estará emulando un lector de tarjetas hacia el panel de control.

- Los paneles de control nó tienen en su electrónica interna un supresor de variaciones bruscas de voltaje, motivo por lo cual se necesita proteger el sistema mediante otros mecanismos.

- El software de administración funciona únicamente sobre sistemas operativos de Microsoft.

- El software de administración no permite incrementar su funcionalidad, es decir no existe algún dll (librería de enlace dinámico) disponible o algún otro mecanismo para poder incrementar su funcionalidad.

2.4.8.1.4 Análisis de costos

EQUIPOS SISTEMA DE CONTROL DE ACCESOS	UNIT. $
LECTOR DE PROXIMIDAD MINIPROX READERCARD II	170,73
CONTROLADOR - PANEL DE CONTROL, N-1000-III	1.541,49
CONTROLADOR - PANEL DE CONTROL, N-1000-IV	2.037,44
CONVERTIDOR RS485-ETHERNET	280,44
SOFTWARE DE ADMINISTRACION DEL SISTEMA, WINPACK 2.0	825,44
LECTOR BIOMETRICO HAND KEY II	1.832,44
TARJETAS INTELIGENTES DE PROXIMIDAD HID ISO PROX II.	8,00

Tabla 2.4 Análisis de costos primera opción

Nota.- Los precios antes mencionados no incluyen IVA, la empresa EXEC sistemas proporciona soporte técnico en el país de todos los productos NORTHERN COMPUTERS. [25]

2.4.8.2 Segunda opción (KERISYSTEMS):

2.4.8.2.1 Introducción

La segunda opción consta de los siguientes elementos:

- Panel de Control de KERISYSTEMS PXL-500.
- Lector de tarjetas de proximidad MS-5000
- Tarjetas de proximidad KC-10X
- Software de administración de KERISYSTEMS, D-LITE

2.4.8.2.2 Ventajas

- Respaldo de memoria mediante una batería de litio, la información almacenada en la memoria puede permanecer en la misma hasta 7 días.
- Los lectores de proximidad pueden detectar una tarjeta hasta 15 cm de distancia.
- El software de administración es fácil de utilizar, tiene un interfaz similar a la de Excel.
- Los paneles de control tienen dimensiones pequeñas, además de un bajo peso.
- Las tarjetas de proximidad pueden trabajar en ambientes interiores y exteriores.

- El rango de temperatura de los paneles de control, permite trabajar al sistema en lugares dónde se tienen bajas temperaturas con un mínimo de -18 ° C.

- El software de administración permite imprimir en las tarjetas inteligentes de proximidad la foto de identificación del usuario, nombre del usuario, CI (cédula de identidad) y el logotipo de la empresa o institución.

2.4.8.2.3 Desventajas

- Cada panel de control puede soportar sólo hasta 500 tarjetas.

- La información no viaja encriptada.

- No se tiene una red de seguridad mixta. Es decir sólo se puede instalar en la red lectores de tarjetas de proximidad, y no sensores biométricos que verifican la geometría de la mano, cabe recalcar que esta solución si permite utilizar sensores basados en el análisis de la huella, pero como se mencionó anteriormente esta tecnología no será utilizada en este proyecto por los motivos antes mencionados.

- Los paneles de control pueden sòportar máximo 4 alarmas.

- La distancia máxima a la que se puede conectar el lector de tarjetas de proximidad del panel de control es 100 m.

- El software de administración funciona únicamente sobre sistemas operativos de Microsoft.

- No se tiene una batería interna que permita al sistema funcionar en caso de ausencia de energía.

- Para poder tener una red de control de acceso extendida cada panel de control debe tener una tarjeta adicional ethernet.

- Los paneles de control no tienen en su electrónica interna un supresor de variaciones bruscas de voltaje, motivo por los cual se necesita proteger el sistema mediante otros mecanismos.

- El software de administración no permite incrementar su funcionalidad, es decir no existe algún dll (librería de enlace dinámico) disponible o algún otro mecanismo para poder incrementar la funcionalidad.

- Interacción con Access como base de datos.

2.4.8.2.4 Análisis de costos

EQUIPOS SISTEMA DE CONTROL DE ACCESOS	UNIT. $
LECTOR DE PROXIMIDAD MS-5000	198,73
CONTROLADOR – PANEL DE CONTROL, PXL-500	600,24
TARJETA ETHERNET	282,44
SOFTWARE DE ADMINISTRACION DEL SISTEMA, D-LITE	600,00
LECTOR BIOMETRICO DE HUELLA, VERIFLEX	1.100,00
TARJETAS DE PROXIMIDAD KC-10X	7,50

Tabla 2.5 Análisis de costos Segunda opción

Nota.- Los precios antes mencionados no incluyen IVA, la empresa EXEC sistemas proporciona soporte técnico en el país de todos los productos KERYSISTEMS. [25]

2.4.8.3 Solución 3 (MICROCIRCUITOS):

2.4.8.3.1 Introducción

La solución numero 3 consta de los siguientes elementos:

- Panel de Control de SIEMENS SIMATIC S7-200/CPU226.

- Lector de tarjetas de proximidad AWID PS-6200.
- Tarjetas de proximidad AWID.
- Software de administración INTEL-SYS.

2.4.8.3.2 Ventajas

- Los paneles de control de acceso pueden controlar dos puertas, o más dependiendo del modelo de PLC que se utilice.
- Se pueden automatizar diferentes aplicaciones, como por ejemplo los niveles de agua de una cisterna.
- Se dispone de una batería de respaldo, la misma que permite al sistema de seguridad trabajar sin alimentación eléctrica durante 5 horas.
- Cada uno de los paneles de control puede almacenar información de hasta 5.000 tarjetas, cabe recalcar que la memoria puede ser ampliada para soportar un mayor número de tarjetas.
- Respaldo de memoria mediante una batería de litio, la información almacenada en la memoria puede permanecer en la misma hasta 50 horas, después de que se corte la fuente de alimentación.
- Los lectores de proximidad pueden detectar una tarjeta hasta 20.3 cm de distancia.
- El software de administración es fácil de utilizar, permite monitorear continuamente las alarmas,
- Se pueden definir hasta 30 zonas de tiempo.

- Capacidad para combinar usuarios, niveles de acceso y zonas de tiempo sin restricción.

- Reportes de accesos e intrusión, con diferentes opciones de clasificación y selección de información.

- Monitoreo permanente de los paneles de control, sensores y demás puntos de información.

- La distancia máxima a la que se puede conectar el lector de tarjetas de proximidad del panel de control es de 150 m.

- Se pueden tener redes de control de acceso de área extendida, mediante la utilización de un convertidor RS-485 / ethernet al inicio de la red de control de acceso local.

- Los paneles de control tienen mecanismos de proteger su electrónica, ante variaciones bruscas de voltaje.

2.4.8.3.3 Desventajas

- No se puede tener una red de control de acceso mixta, es decir no se pueden definir sitios de mayor seguridad que otros.

- La información no viaja con ningún tipo de encripción, trayendo como consecuencia una deficiencia en la seguridad de la misma.

- El software de administración puede funcionar únicamente sobre sistemas Microsoft.

- Los paneles de control no tienen en su electrónica interna un supresor de variaciones bruscas de voltaje, motivo por lo cual se necesita proteger el sistema mediante otros mecanismos.

- El software de administración no permite incrementar su funcionalidad, es decir no existe algún dll (librería de enlace dinámico) disponible o algún otro mecanismo para poder incrementar la funcionalidad para que se adecuen a las necesidades de la Politécnica.

- El software de administración no permite imprimir en las tarjetas de proximidad la foto de identificación del usuario, nombre del usuario, CI (cédula de identidad) y el logotipo de la empresa o institución.

- Interacción con Access como base de datos.

2.4.8.3.4 Análisis de costos

EQUIPOS SISTEMA DE CONTROL DE ACCESOS	UNIT. $
LECTOR DE PROXIMIDAD ALCANCE ESTANDAR AWID SP6820	170,63
CONTROLADOR - PANEL DE CONTROL, 24I/16O. SIEMENS S7226.	738,00
TARJETAS DE PROXIMIDAD AWID.	6,80
SOFTWARE DE ADMINISTRACION DEL SISTEMA	618,75
CONVERTIDOR RS-485/ETHERNET	299,75

Tabla 2.6 Análisis de costos tercera opción

Nota.- Los valores antes mencionados no incluyen IVA, la empresa MICROCIRCUITOS proporciona soporte técnico en el país de todos los productos SIEMENS Y AWID.

2.4.8.4 Selección de la mejor opción para el sistema de control de acceso

De las tres propuestas antes mencionadas se puede apreciar claramente que las propuestas de Northern Computers y la propuesta de Microcircuitos son las más adecuadas para ser utilizadas en este proyecto de titulación, la opción propuesta por KERYSYSTEMS es ideal para sistemas de control de acceso local, pero tiene un costo bastante elevado para sistemas de control de acceso extendidas, debido a que cada panel de control necesitaría una tarjeta ethernet adicional, esto no

sucede con las otras dos propuestas en las cuales se puede conectar un solo convertidor RS-485 / Ethernet al inicio de la red de control de acceso local simulando de esta manera toda la red de control de acceso local como una única salida ethernet, a continuación se presenta un resumen de costos de los productos de las tres propuestas.

	NORTHERN COMPUTERS	KERYSISTEMS	MICROCIRCUITOS
LECTORA DE PROXIMIDAD	170,73	198,73	170,63
PANEL DE CONTROL DE 4 PUERTAS	2.037,44	1.768,00	1.476,00
SOFTWARE DE ADMINISTRACION	825,44	600,24	618,75
LECTOR BIOMETRICO	1.832,24	1.100,00	
TARJETAS INTELIGENTES DE PROXIMIDAD	8,00	7,50	6,80
CONVERSOR ETHERNET	280,44	282,44	299,75

Tabla 2.7 Resumen de costos de las tres opciones analizadas

Como se puede observar los precios son muy similares entre las tres propuestas, del análisis técnico económico realizado de las tres propuestas se propone utilizar la propuesta número 1 a cargo de la empresa Northern Computers, a continuación se define los parámetros que la hace mejor que las otras dos propuestas:

- Red de control de acceso mixta, es decir pueden trabajar conjuntamente lectoras de tarjetas de proximidad y lectoras biométricas basadas en la geometría de la mano, esta es una característica fundamental para el desarrollo de este proyecto ya que como se explica en el capítulo 3, existen lugares que necesitan mayor protección que otros, como por ejemplo el centro de cómputo general.

- La información viaja encriptada en una forma segura desde el lector de tarjetas de proximidad hacia cada uno de los paneles de control, de esta forma se minimiza el riesgo de que algún cracker pueda determinar fácilmente la información que viaja en la red de control de acceso.

- El software de administración permite imprimir en las tarjetas inteligentes de proximidad la foto del propietario de la misma, como se ha mencionado anteriormente, es necesario tener alguna identificación en la tarjeta para poder determinar que la tarjeta pertenece a la persona que la lleva.

- El software de administración permite administrar conjuntamente los sistemas de circuitos cerrados de televisión, facilitando la administración del sistema, como se ha mencionado anteriormente, otro aspecto de suma importancia que debe existir en un sistema de control de acceso es un sistema de circuito cerrado de televisión para poder definir claramente cual es la causa de una alarma.

- Las lectoras de tarjetas de proximidad pueden leer tarjetas de proximidad únicamente o tarjetas inteligentes de proximidad, las cuales permitirán almacenar en la misma diferente información referente al usuario de la misma como por ejemplo puede ser la información de la fotografía digital de la persona, mediante la cual un guardia de seguridad podría comparar la imagen desplegada en la computadora con la imagen de la persona, cabe recalcar que la información almacenada en la tarjeta inteligente no puede ser leída por la lectora de proximidad aquí presentada, se necesita otra lectora que entienda la información almacenada en la tarjeta inteligente, la lectora presentada puede leer únicamente el código que genera la tarjeta de proximidad para permitir o no el acceso.

Como segunda opción se propone utilizar la solución de MICROCIRCUITOS, cabe recalcar que esta propuesta es ecuatoriana, desarrollada por el Ing. Bolívar Ledesma de la EPN. La propuesta de MICROCIRCUITOS trata de dar una solución de control de acceso equitativa para todas las áreas, es decir no permite tener una red de control de acceso mixta. Se podría mejorar la propuesta de MICROCIRCUITOS desarrollando aún más el software de administración y realizando pruebas para hacer emular un lector biométrico como un lector de tarjetas inteligentes, pudiendo llegar a ser esta propuesta mejor que la opción de Northern Computers en costo y en calidad.

REFERENCIAS DEL CAPITULO II

[1] LAWRENCE J. Fenelly, Effective Physical Security, Tercera Edición, Elsevier, United States of America, 2004. Páginas 1-8, 101-114, 195-202, 209-217.

[2] GARCIA M. Lynn, The Design and Evaluation of Physical Protection Systems, primera Edición, Elsevier, United States of America. 2001. Páginas 113-143, 173-200.

[3] STALLINGS William, Comunicaciones y Redes de Computadores, Sexta Edición, Madrid España, 2000. Páginas 605-628.

[4] AVILA Nelson., "Folleto, Seguridad en Redes", Quito Ecuador. Capítulo 3, Encripción.

[5] Handbook of Information Security Management. 2000 http://secinf.net/info/misc/handbook/. Capítulo1 Control de Acceso, Capítulo 10 Seguridad Física.

[6] Information Security Management Handbook, Auerbach, United States of America, 2003. Capítulo 1 Metodologías y sistemas de control de acceso, Capítulo 5 Encripción, Capítulo 10 Seguridad Física

[7] VILLALÓN Antonio, Seguridad en Unix y Redes, Versión 2.1, Valencia España. Páginas 117-123.

[8] Tecnología de tarjetas. http://www.geocities.com/gcataneo/tecnologia.htm

[9] Tarjetas magnéticas. http.//www.fortunecity.com/westwood/calvin/275/cards/iso7811.zip

[10] LÓPEZ M. Héctor, Tecnología de Smart card, 1998. http://www.dcc.uchile.cl/~rbaeza/cursos/proyarq/hlopez/node1.html

[11] GUTHERY Scott, JURGENSEN Tim, Smart card developer's kit. Macmillan, United States of America. 1998. http://es.tldp.org/manuales-lucas/doc-unixsec/unixsec-html/node1.html.

[12] Smart cards. http://www.fortunecity.com/westwood/calvin/275/cards/iso7816.zip

[13] ALMEIDA Rosario, LUCERNA Pablo, Reconocimiento del iris. Web

[14] LIONEL Martin, Person identification technique using human iris recognition, Francia. 2001.

[15] UNANDER Joseph, Image reconstruction of the iris spectrally http://www.cis.rit.edu/research/thesis/bs/2000/unander/tableofcontents.html.

[16] BECERRA Nestor, VILLAR Miguel, Verificación de identidad de individuos mediante la voz.

[17] GARCÍA ORTEGA, Sistema de reconocimiento de huellas dactilares para el control de acceso a recintos, México, 2001.

[18] RODRÍGUEZ Fernando, Suárez francisco, Identificación dactilar basada en filtros Galvor.

[19] Sistemas de Control de Acceso, kerysystems.
http://www.kerisys.com

[20] Sistemas de Control de Acceso, Northern Computers.
http://www.northern-computers.co.uk.

[21] SIEMENS.
http://www.siemens.com/s7-200

[22] HID
http://www.HIDCorp.com

[23] AWID
http://www.awid.com

[24] IR Recognition Systems.
http://www.hanreader.com

[25] EXEC SISTEMAS
http://www.execsistemas.com

3 DISEÑO DEL SISTEMA DE SEGURIDAD FÍSICO

3.1 INTRODUCCIÓN

Como se mencionó en el capítulo 1, el presente proyecto de titulación tiene como principal objetivo dar una solución de control de acceso físico de las personas hacia cada uno de los laboratorios del edificio antiguo de la ex facultad de Ingeniería Eléctrica, el centro de cómputo general de la EPN y los cinco puntos de acceso vehicular, para lo cual se ha realizado el levantamiento de la información como se muestra en el Anexo 1, para poder saber cuáles son los problemas percibidos por parte de los usuarios de cada uno de los puntos antes mencionados frente al control de acceso físico.

En este capítulo se presenta una solución al problema antes mencionado, planteando un diseño de seguridad física, basado en la utilización de la propuesta número 1 de los productos existentes en el mercado; esta propuesta se encuentra detallada en el capítulo 2, la cual presenta la solución de control de acceso de la empresa Northern Computers. Además se presenta un análisis de costos sobre la solución planteada.

Para que el presente diseño de seguridad sea de fácil entendimiento, se ha dividido el diseño en:

- Diseño del sistema de control de acceso.
- Diseño eléctrico y de respaldo de energía del sistema de control de acceso.
- Diseño de respaldo de transmisión de información para el sistema de control de acceso.

A continuación se presentan cada uno de los diseños antes mencionados con sus respectivos análisis de costos, además de plantear una simbología para la identificación de cada uno de los elementos en el sistema.

3.2 DISEÑO DEL SISTEMA DE CONTROL DE ACCESO [1][2][3]

3.2.1 INTRODUCCIÓN

En este capítulo se plantea el diseño del sistema de control de acceso, para lo cual se ha decidido realizar un sistema de control de acceso en profundidad además de centralizado como se muestra en la figura 3.1, es decir cada uno de los edificios conformará una red de control de acceso local, la misma que se interconectará con un punto central de concentración en el centro de cómputo general, formando una red de control de acceso de campus. Además cada uno de los puntos de control de acceso vehicular, se conectará a la red de control de acceso local más cercana, por ejemplo el punto de acceso vehicular de la Ex facultad de Ingeniería Eléctrica pertenecerá al sistema de control de acceso de la ex Facultad de Ingeniería Eléctrica.

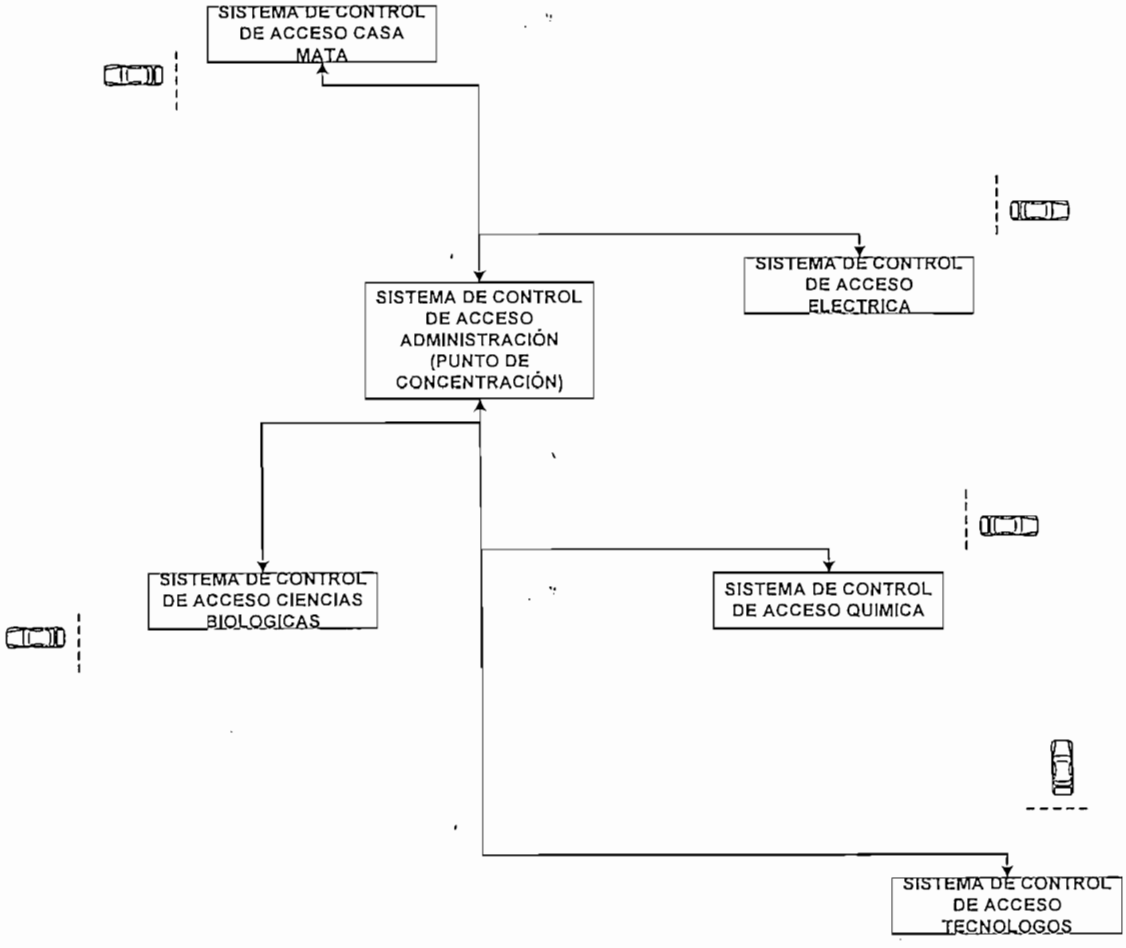


Figura 3.1 Red de Control de Acceso Vehicular de la EPN

El sistema de control de acceso centralizado mostrado en la figura 3.1, tiene como principal objetivo facilitar la administración del sistema de control de acceso, para lo cual en el centro de cómputo general se colocará un servidor para controlar cada una de las redes de control de acceso locales, además en esta ubicación se encontrará el cuarto de vigilancia en el mismo que se encontrará un guardia monitoreando continuamente el sistema.

Otro aspecto fundamental que se tomará en cuenta en el diseño de seguridad y el diseño eléctrico es que todos los cables que se utilizarán para que funcionen las redes de control de acceso locales deben ir en tubería CONDUIT EMT metálica, separadas, es decir irán los cables eléctricos en una tubería y los cables de seguridad irán en otra, además las tuberías estarán ocultas en la mayor cantidad de tramo posible como se muestran en los diagramas presentados en el Anexo 3. Cabe recalcar que no se utilizará tubería PVC debido a que una persona puede fácilmente cortar la tubería y de esta forma tener acceso al sistema de control de acceso.

El tipo de cable que se utilizará para conectar las cerraduras electromagnéticas será cable gemelo flexible número 22 AWG debido a que las cerraduras electromagnéticas necesitan una alimentación eléctrica de 12 VDC y una corriente de 1 A y este tipo de cable puede soportar una corriente máxima de 6 A. El cable que se utilizará para conectar los lectores de tarjetas de proximidad y los lectores biométricos será cable UTP cat 5e, cabe recalcar que se necesitan 5 cables de los 8 que se encuentran en un cable UTP, los otros 3 cables serán utilizados para conectar el sensor de apertura de puerta que se colocará en cada una de las entradas principales a las localidades.

Para ingresar en cada ubicación se utilizará una tarjeta inteligente, en tanto que para que las personas puedan salir de cada una de las ubicaciones se colocará un interruptor junto a la puerta por la parte interior de cada una de las ubicaciones.

Cabe recalcar que en los paneles de control utilizados se pueden utilizar otros mecanismos para abrir las puertas como por ejemplo interruptores. La figura 3.2 muestra un ejemplo de conexión.

En cuanto al cable, se utilizará un cable gemelo flexible número 2x22 AWG para conectar el interruptor al panel de control debido a que sólo se necesita dos conductores para realizar dicha conexión simulando un ingreso de un código válido, de esta manera una persona podrá abrir la puerta desde adentro de cada ubicación mediante la utilización del interruptor.

Existe otro mecanismo para abrir la cerradura electromagnética mediante la utilización de dos lectoras de tarjetas, conectadas en paralelo, esta opción no se tomará en cuenta ya que involucra un mayor costo y los beneficios son similares.

En las ubicaciones que tienen sistemas independientes de alarmas se mantendrán estos sistemas en forma independiente, para no desaprovechar la infraestructura existente.

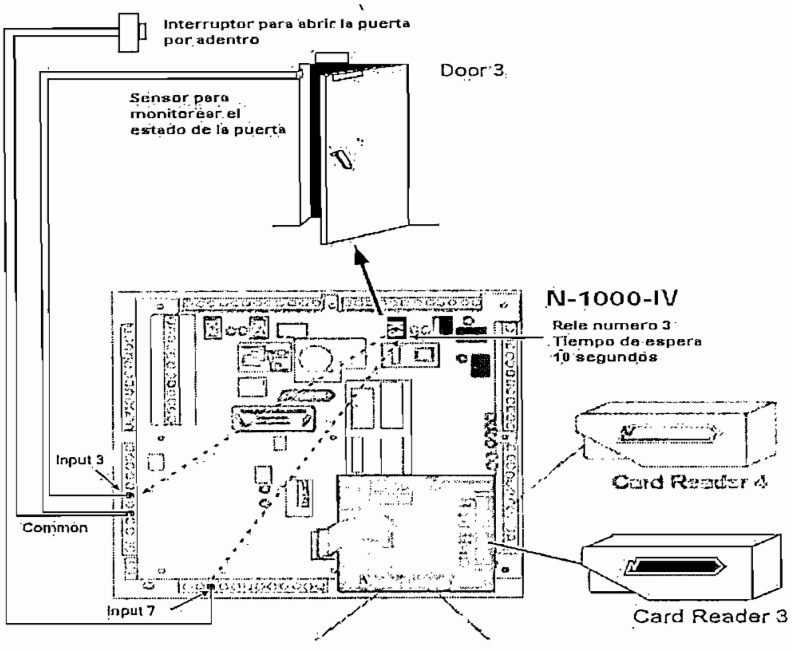


Figura 3.2 Ejemplo de conexión para abrir una puerta por dentro y por fuera de la ubicación [a].

[a] Cuando un usuario desea ingresar a estas ubicaciones presenta su tarjeta al lector, si el código es válido el panel de control abre el relé para que la cerradura electromagnética se abra, si el usuario se encuentra en el interior de la ubicación y desea salir de la misma presiona el interruptor y el panel de control abre la cerradura electromagnética.

Como se mencionó en el capítulo 2 los paneles de control de la empresa Northern Computers se conectan uno a continuación de otro, hasta formar una red de control de acceso en forma de bus, logrando conectar de esta forma hasta 31 paneles de control de acceso, como se muestra en la figura 3.3. Para facilitar la configuración y la administración de los mismos, la red de control de acceso debe comenzar en un dispositivo que es la interfaz entre la red de control de acceso y el servidor de administración.

Para poder realizar una interconexión mediante un enlace ethernet al inicio del sistema se debe colocar un convertidor RS-485/ethernet, el mismo que simulará toda la red de control de acceso local como un único dispositivo ethernet.

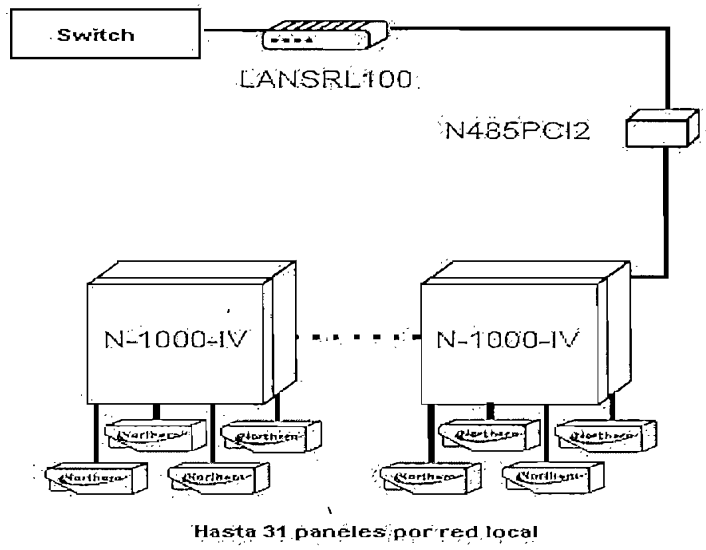


Figura 3.3 Lazo de comunicaciones con un enlace ethernet.

Como se indicó anteriormente cada una de las redes de control de acceso locales se conectarán hacia el punto de concentración que se instalará en el centro de cómputo general; para cumplir con dicho objetivo la salida ethernet, del convertidor RS-485/ethernet se conectará hacia un puerto de un switch ubicado en cada uno de los edificios principales, para poder utilizar los enlaces de fibra óptica de la polired como se muestra en la figura 3.4.

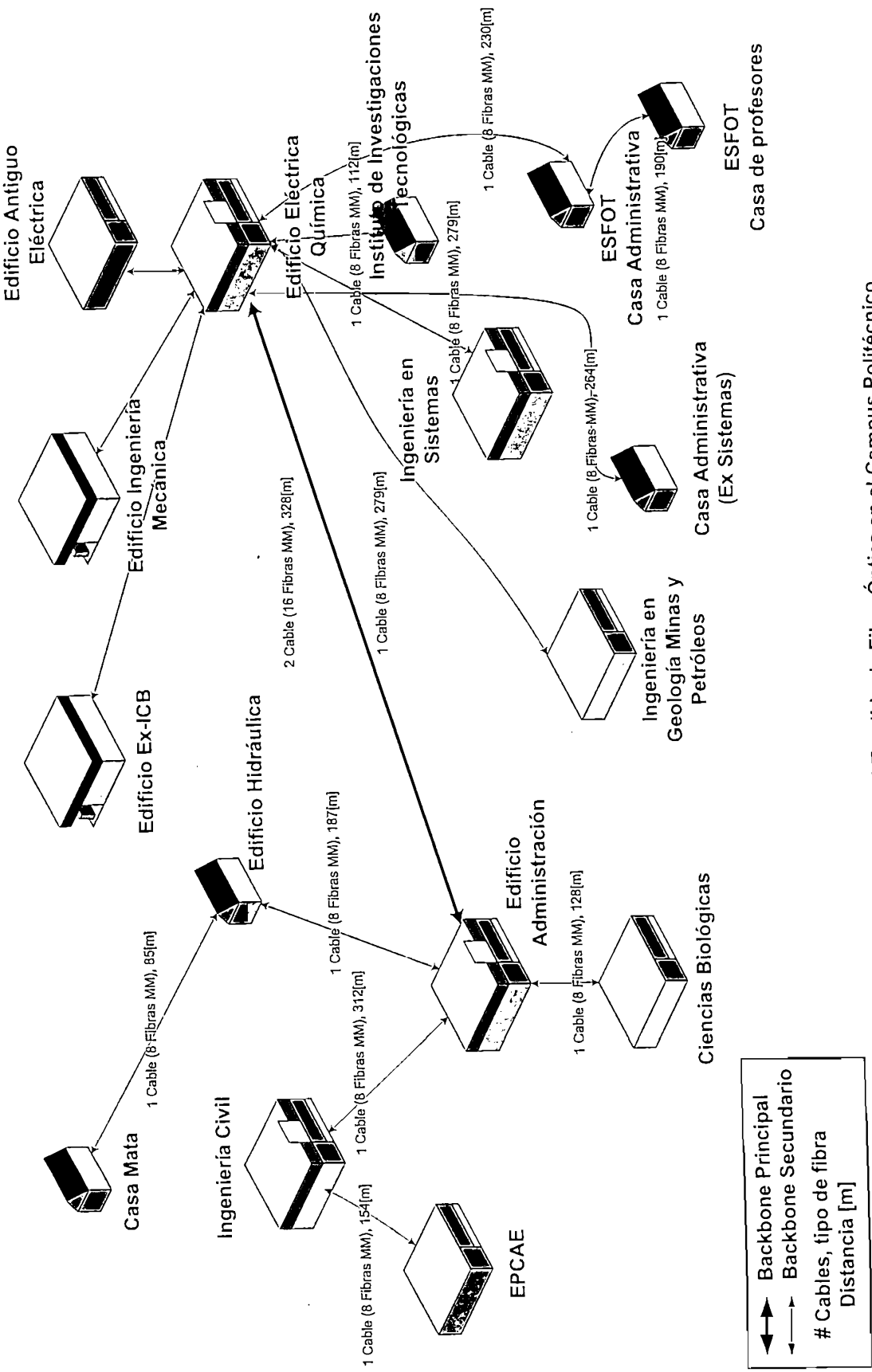


Figura 3.4 Tendido de Fibra Óptica en el Campus Politécnico

Fuente: Plan Estratégico de Internet 2 para la EPN

Dichos enlaces de fibra óptica permiten interconectar a la mayoría de edificios con el centro de cómputo general mediante enlaces de fibra óptica y la información viaja a altas velocidades.

Además se define la utilización de un sistema de respaldo para la transmisión de la información, mediante la utilización de un sistema inalámbrico, para lo cual se recomienda la instalación de una antena direccional en cada uno de los edificios principales pertenecientes a las redes de control de acceso locales y se colocará una antena omnidireccional en la terraza del edificio de administración (punto de concentración).

Para realizar el diseño de seguridad se ha tomado en cuenta las diferentes necesidades de cada uno de los puntos analizados para poder determinar cuales son los puntos más críticos. Mediante la ayuda de la tabla 1.4 y tomando en cuenta la información que se tiene en cada una de las localidades, se ha realizado un análisis costo beneficio de cada uno de los puntos a proteger.

Para poder determinar cuales serán las áreas que necesitaran una mayor protección que otras en este proyecto de titulación como criterios de diseño no tomará en cuenta únicamente el valor de los activos tangibles, por ejemplo el laboratorio de maquinas eléctricas tiene un valor total de los activos mayor que el centro de cómputo general, pero como se mencionó en el capítulo 1 el centro de cómputo general es la parte medular de la Politécnica ya que aquí se almacena información de suma importancia para la institución, motivo por el cual esta área necesita una mayor protección que otras.

En la tabla 1.4, presentada en el capítulo 1, se muestra un resumen de cada una de las áreas a proteger y el total del precio de los activos existentes en cada una de las localidades, se puede definir claramente que todas las localidades tienen activos con un gran valor económico, deduciéndose fácilmente que el costo de implementación de un sistema de control de acceso es relativamente bajo en comparación a los beneficios que se obtendrán con la implementación del mismo, motivo por el cuál se ha decidido proteger cada una de las localidades.

Para proteger cada una de los sitios, se cambiará la puerta de cada una de las entradas principales por una puerta metálica con sensores magnéticos de apertura de puerta, cerradura electromagnética, más una cerradura normal y eventualmente un lector de tarjetas de proximidad o un sensor biométrico basado en la geometría de la mano, para lo cual se utilizarán dos niveles de seguridad:

- **Nivel de seguridad medio**, basado en la utilización de una puerta metálica en la entrada principal a la localidad con sensores magnéticos de apertura de puerta, cerradura electromagnética más cerradura normal y un lector de tarjetas de proximidad para autenticar a los usuarios.

- **Nivel de seguridad alto**, basado en la utilización de una puerta metálica en la entrada principal a la localidad con sensores magnéticos de apertura de puerta, cerradura electromagnética más cerradura normal y un lector biométrico basado en la geometría de la mano para autenticar a los usuarios.

Para definir cuál es nivel de seguridad a implementar en cada una de los sitios no se tomará en cuenta únicamente el valor total de los activos existentes en cada uno, si no qué además se tomará en cuenta la información que se tiene almacenada en cada sitio. Cabe recalcar que la información tiene un valor muy alto, es decir en caso de que la información se pierda o se dañe, es muy difícil o imposible recuperarla, trayendo como consecuencia una pérdida de credibilidad de la institución.

A continuación se presentan ejemplos en los cuales se muestra cómo tomar el criterio para implementar los dos tipos de niveles de seguridad, además se presenta un cuadro resumen con los mecanismos a utilizar para proteger cada una de las localidades.

3.2.2 DISEÑO DEL SISTEMA DE CONTROL DE ACCESO DEL EDIFICIO ANTIGUO DE LA EX FACULTAD DE INGENIERÍA ELÉCTRICA

3.2.2.1 Introducción

Como se mencionó anteriormente se realizará un diseño centralizado, para lo cual cada uno de los edificios formará una red de control de acceso local, por ejemplo el edificio de la ex facultad de Ingeniería Eléctrica, en conjunto con el punto de control de acceso vehicular, formarán una red de control de acceso local, la misma que se interconectará al servidor de administración que se encuentra localizado en el centro de cómputo general a través de un enlace ethernet. Como se mencionó en el capítulo 2 los paneles de control de acceso de Northern Computers permiten interconectar los paneles en forma paralela hasta 31 paneles por cada lazo de seguridad.

En esta propuesta de seguridad se colocarán sensores de apertura de puerta en cada una de las puertas de las entradas principales al edificio antiguo de la ex facultad de Ingeniería Eléctrica, además se colocarán lectores de tarjetas de proximidad en las entradas al edificio, como se muestra en el Anexo 3.

Cabe recalcar que tendrán únicamente tarjetas para abrir cada una de las entradas a los edificios el personal de seguridad. El horario en que se activarán estos lectores de tarjetas de proximidad, los sensores y las cerraduras electromagnéticas será definido por cada uno de los edificios, para el edificio antiguo de la ex facultad de Ingeniería Eléctrica el horario será de lunes a viernes desde las 22h00 hasta las 6h45, el día sábado desde las 18h00 hasta el día lunes a las 6h45, y permanecerán activos durante los días feriados, cabe recalcar qué estos horarios son diferentes para cada uno de los edificios.

Todo esto se puede lograr mediante programación de los paneles de control de acceso, se define este horario para activar el sistema de control de acceso en estas ubicaciones para no interferir con el movimiento estudiantil durante las horas laborables ya que estas puertas de las entradas principales permanecen abiertas durante todo el horario laborable.

Los guardias de seguridad pueden ingresar al edificio autenticándose con el sistema de control de acceso durante la noche para realizar sus jornadas de vigilancia y cuando sean las 6h45 los guardias deberán abrir las puertas para que los estudiantes puedan movilizarse fácilmente. Se mantendrán las puertas de vidrio que actualmente se tienen en el ingreso frontal con sus respectivas cerraduras.

En el Anexo 3 se presentan en forma detallada los planos de cada una de las plantas del edificio antiguo de la ex Facultad de Ingeniería Eléctrica, indicando claramente las ubicaciones a proteger, además se presenta un cuadro con la simbología utilizada con su respectivo significado y un cuadro de distribución de red. En la figura 3.5 se presenta un diagrama vertical de seguridad de la red de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica, en este diagrama se presenta el número de paneles de control de acceso que se localizan en cada una de las plantas del edificio antiguo de la ex facultad de Ingeniería Eléctrica con la identificación del número de lectores que se conectarán en cada uno de los paneles, en el Anexo número 3 se presentan en forma detallada las ubicaciones de cada uno de los paneles de control así como la ubicación de cada uno de los lectores.

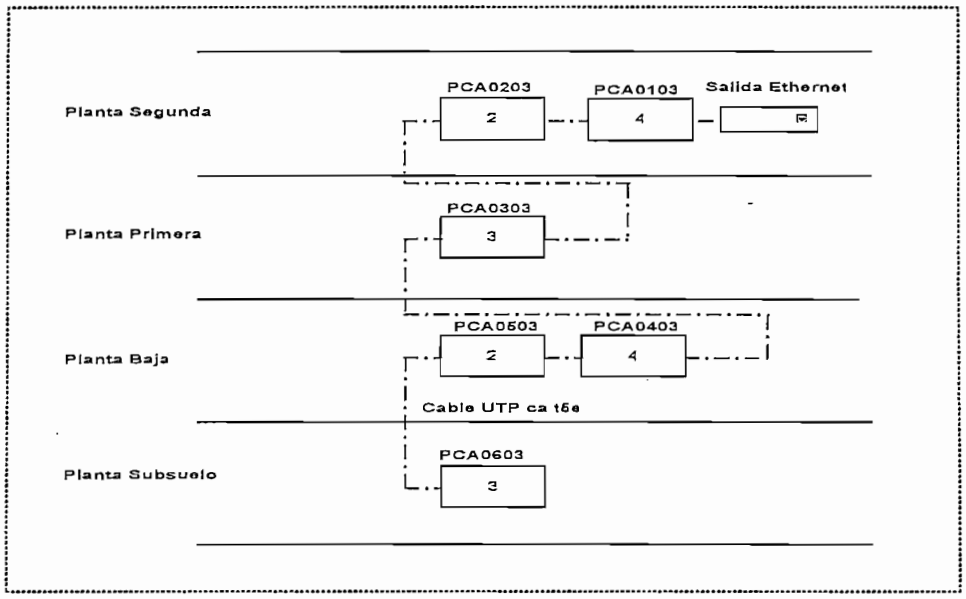


Figura 3.5 Diagrama vertical de seguridad (red de control de acceso edificio antiguo ex facultad Ingeniería Eléctrica)

A continuación se presenta un cuadro con la simbología utilizada en el grafico anterior.

SIMBOLO	DESCRIPCION
PCAxxyy	Panel de control de acceso, donde xx es el número del panel, yy es el identificador de red local
—·—·—·—·—	Cable UTP Cat 5e
#	Número de lectores conectados al panel

A continuación se presentan en forma detallada cuales han sido los motivos primordiales para tomar las decisiones de la utilización de la tecnología en cada una de las ubicaciones a proteger.

3.2.2.2 Laboratorio de Comunicaciones

El laboratorio de comunicaciones se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 205 como se observa en el Anexo 3, Diagrama E1, en esta ubicación funcionan los laboratorios de:

- Comunicación digital
- Teoría de comunicaciones
- Sistemas microprocesados

Como se puede observar en la tabla 1.4 mostrada en el capítulo1, el costo total de los activos que se encuentran en esta ubicación asciende a **12.804,64 USD**, además en esta ubicación funcionan conjuntamente laboratorios y oficinas, la información almacenada en esta ubicación es de suma importancia tanto para los profesores como para los alumnos.

Tomando en cuenta que en años anteriores han existido robos en esta ubicación se ha decidido implementar un **nivel de seguridad medio**.

Es decir se cambiará la puerta principal de madera que actualmente se tiene por una puerta metálica con una cerradura electromagnética más una cerradura

normal, además para poder tener registros de las personas que ingresan al mismo se colocará un lector de tarjetas de proximidad en la entrada a esta ubicación, para que sólo pueda ingresar a esta ubicación personal autorizado y poder tener registros de las personas que ingresan a esta ubicación, además se colocarán sensores magnéticos en la puerta para verificar el estado de la misma. En el Anexo número 3 se presentan los planos con los diseños propuestos para cada una de las localidades.

El sistema de control de acceso permanecerá activo todo el tiempo y permitirá el ingreso de personal autorizado a esta ubicación desde las 6h45 hasta las 22h00, de lunes a viernes y el día sábado desde las 6h45 hasta las 18h00, el día domingo o algún otro día feriado el sistema de control de acceso no permitirá el ingreso de ninguna persona en esta ubicación, a excepción de personal de seguridad autorizado para ingresar en caso de alguna emergencia.

Cabe recalcar que en caso de emergencia existirá una tarjeta con privilegios de administrador para abrir esta localidad por ejemplo en caso de que exista algún incendio.

3.2.2.3 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones se encuentra ubicado en la segunda planta del edificio antiguo de la ex Facultad de Ingeniería Eléctrica en la ubicación EL 218 como se observa en el Anexo 3, Diagrama E1, aquí se encuentra una pequeña red formada por los siguientes servidores:

- Servidor WEB (PIII de 450 MHz)
- Servidor E-Mail (PIII de 670 MHz)
- Servidor de servicios múltiples TELEFIE (PII de 300 MHz)
- Servidor Proxy IBM.

Además aquí se tiene el siguiente equipo activo que sirve para realizar la interconexión de las diferentes computadoras del edificio antiguo de la ex facultad de Ingeniería Eléctrica con el centro de cómputo general:

- Hub Ethernet 10 Base T, 3 Com 12 puertos.
- Switch Ethernet 10 BaseT/ 100 Base TX Autosensig, IBM, 24 Puertos.
- Switch Ethernet con 24 puertos 10 Base T y un puerto 100 Base TX, IBM, 25 Puertos.

Como se puede observar en la tabla 1.4, mostrada en el capítulo 1, el total de los activos que se encuentran en esta ubicación suma **7.284,82 USD**, un valor total de los activos relativamente bajo, pero como se mencionó anteriormente en este proyecto de titulación como criterios de diseño se tomará en cuenta tanto el valor de los activos así como el impacto que trajera a la institución si esta ubicación llegara a ser violentada.

Pensemos qué pasaría si esta ubicación llegaría a ser violentada y se roban los servidores que se encuentran en esta ubicación o que se roben los equipos de interconectividad que permiten conectar al edificio antiguo de eléctrica mediante fibra óptica con el centro de cómputo general, el impacto que tendría en la Politécnica sería muy grande y no podría reponerse fácilmente, por todas estas razones, se ha decidido implementar un **nivel de seguridad Alto**, es decir se cambiará la puerta de madera que actualmente se tiene por una puerta metálica con una cerradura electromagnética más cerradura normal. Para poder tener registros de las personas que ingresan al mismo se colocará un lector biométrico basado en la geometría de la mano en la entrada a esta ubicación, para que sólo pueda ingresar a esta ubicación personal autorizado, además se colocarán sensores magnéticos en la puerta para verificar el estado de la misma.

A continuación se presenta un cuadro en el cual se resume los niveles de seguridad a implementar en cada una de las localidades.

Laboratorio	Nivel de Seguridad	Valores de activos, otros	Elementos seguridad
Lab. Comunicaciones	Medio	El valor de los activos es de $ 12.804,64	Interruptor, lector de tarjetas, sensor magnético de apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.

Laboratorio	Nivel de Seguridad	Valores de activos, otros	Elementos seguridad
Lab. Postgrado	Medio	El valor de los activos es de $ 21.296,27	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Redes	Medio	El valor de los activos es de $ 25.090,00	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Sistemas Digitales	Medio	El valor de los activos es de $ 28.890,75	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Control y Computación	Medio	El valor de los activos es de $ 17.889,04	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Cuarto de Telecomunicaciones	Alto	El valor de los activos es de $ 7.284.82 , cabe recalcar que éste es el punto de conexión con el centro de cómputo general	Interruptor, lector biométrico (geometría de la mano), sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Circuitos Eléctricos	Medio	El valor de los activos es de $ 76.989,98, en esta ubicación no se tiene información que sea de suma importancia para la institución, además en esta localidad existen dos puertas por lo tanto se mantendrá cerrada la una y la otra servirá para realizar el control de acceso.	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica doble cuerpo, cerradura normal.
Lab. Diseño Electrónico	Medio	El valor de los activos es de $ 20.588,48	Interruptor, lector de tarjetas, sensor magnético (apertura puerta), cerradura electromagnética, puerta metálica, cerradura normal.

Laboratorio	Nivel de Seguridad	Valores de activos, otros	Elementos seguridad
Lab. Electrónica	Medio	El valor de los activos es de $ 52.924,13, en esta ubicación se han robado cosas pequeñas cómo multímetros, además en esta localidad existen dos puertas por lo tanto se mantendrá cerrada la una y la otra servirá para realizar el control de acceso.	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica doble cuerpo, cerradura normal.
Lab. Control Industrial	Medio	El valor de los activos es de $ 25.123,98, en esta ubicación existen equipos muy grandes y sería muy difícil que se roben los mismos	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Control Electrónico de Potencia	Medio	El valor de los activos es de $ 73.243,67, en esta ubicación existen equipos muy grandes y sería muy difícil que se roben los mismos, además se protegerán las dos entradas que existen en esta ubicación (EL 027, El 011)	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Taller Eléctrico	Medio	El valor de los activos es de $ 17.877,72	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. SEP	Medio	El valor de los activos es de $ 15.548,96	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica, cerradura normal.
Lab. Máquinas Eléctricas	Medio	El valor de los activos es de $ 91.521,69, en esta ubicación existen equipos muy grandes y sería muy difícil que se roben los mismos, además como se tienen puertas batientes, se mantendrá cerrada la una puerta y la otra se utilizará para realizar el control de acceso	Interruptor, lector de tarjetas, sensor magnético apertura puerta, cerradura electromagnética, puerta metálica doble cuerpo, cerradura normal.
Lab. Alto Voltaje	Medio	El valor de los activos es de $ 38.518,75, en esta ubicación existen equipos muy grandes y sería muy difícil que se roben los mismos, además como se tienen puertas batientes, se mantendrá cerrada la una puerta y la otra se utilizará para realizar el control de acceso	Interruptor, lector de tarjetas, sensor magnético (apertura puerta), cerradura electromagnética, puerta metálica doble cuerpo, cerradura normal.

3.2.3 DISEÑO DEL SISTEMA DE CONTROL DE ACCESO DEL CENTRO DE CÓMPUTO GENERAL

El centro de cómputo general se encuentra ubicado en la planta subsuelo del edificio de administración el mismo que ocupa las áreas AD S01, S05, S06, S07, S08, S09, S10 y S11 como se observa en el Anexo 3, Diagrama A1.

Aquí se tiene la parte medular de la universidad, ya que en esta ubicación se encuentran los siguientes servidores:

- Servidor de correo
- Servidor DNS
- Servidor de Caching Web
- Servidor Web
- Servidor de Matrículas
- Servidor SAE

Este es el punto central al cual se conectan los edificios de las ex Facultades, para por ejemplo salir hacia Internet, realizar el proceso de matrículas, llenar la base de datos del SAE que almacena las calificaciones de los alumnos, etc.

Como se puede observar en la tabla 1.4, mostrada en el capítulo 1, el total de los activos que se encuentran en esta ubicación es de **$ 48.346,22**, un valor relativamente bajo en comparación al total de los activos existentes en otras ubicaciones, pero como se mencionó anteriormente como criterios de diseño se tomarán en cuenta tanto el valor de los activos así como el impacto que trajera a la institución si esta ubicación llegara a ser violentada.

Como se ha mencionado anteriormente la información tiene un valor muy elevado, pensemos qué pasaría si esta ubicación llegara a ser violentada y se robasen los servidores que se encuentran en esta ubicación o si alguien logra tener acceso físico para borrar o modificar las bases de datos del SAE, la Politécnica tendría una pérdida total de la reputación. Cabe indicar que el centro de cómputo general

es la parte central de los sistemas informáticos de la Politécnica, por todas estas razones, se ha decidido implementar un **nivel de seguridad Alto,** es decir se cambiarán las dos puertas principales de madera que se tienen en la entrada principal a esta ubicación por puertas metálicas.

Una puerta permanecerá siempre cerrada y la otra puerta servirá para controlar el acceso de las personas con una cerradura electromagnética.

Además para poder tener registros más precisos de las personas que ingresan al mismo se colocará un lector biométrico basado en la geometría de la mano en la entrada a esta ubicación, para que sólo pueda ingresar personal autorizado y se pueda tener registros de las personas que ingresan. Además se colocarán sensores magnéticos en la puerta para verificar el estado de la misma.

En el Anexo número 3 se presentan los planos con los diseños propuestos para cada una de las localidades.

Además en esta ubicación se tendrá el servidor de administración del sistema de control de acceso, dicho servidor se encontrará junto a los demás servidores, pero el monitor y el teclado estarán ubicados en el área de operadores de modo que un operador del sistema lo pueda administrar sin necesidad de ingresar en el área de servidores.

Una persona de seguridad será la encargada de monitorear el sistema. El software de administración permite tener hasta 5 usuarios simultáneos para poder llenar las bases de datos del sistema de control de acceso, cabe recalcar que se tiene un solo administrador y cinco usuarios.

El sistema de control de acceso permanecerá activo todo el tiempo y permitirá el ingreso de personal autorizado a esta ubicación desde las 6h45 hasta las 18h00, de lunes a viernes y el día sábado desde las 6h45 hasta las 18h00, el día domingo o algún otro día feriado el sistema de control de acceso no permitirá el ingreso de ninguna persona a ésta ubicación.

En caso de emergencia existirá una tarjeta con privilegios de administrador para abrir esta localidad por ejemplo en caso de que exista algún incendio.

3.2.4 DISEÑO DEL SISTEMA DE CONTROL DE ACCESO VEHICULAR AL CAMPUS POLITÉCNICO

3.2.4.1 Introducción

Se puede acceder al Campus Politécnico a través de cinco puntos de acceso vehicular como son:

- Acceso vehicular 1 (Próximo al edificio de Ciencias Biológicas).
- Acceso vehicular 2 (Próximo al edificio de Ciencias Nucleares)
- Acceso vehicular 3 (Próximo al edificio antiguo de Eléctrica)
- Acceso vehicular 4 (Próximo al edificio de metalurgia extractiva, Tecnólogos)
- Acceso vehicular 5 (Próximo al edificio antiguo de Química)

Cada edificio formará una red de control de acceso local y los puntos de acceso vehicular formarán parte de la red de control de acceso más cercano como se muestra en el Anexo número 3, en los diagramas referentes al diseño de control de acceso vehicular.

Como se puede observar en la figura 3.4 existen enlaces de Fibra Óptica en la mayoría de edificios ubicados en el campus Politécnico, para aprovechar la infraestructura existente, los puntos de control de acceso vehicular formarán parte de las redes de control de acceso local más cercana, es decir el control de acceso número 3 formará parte de la red de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica. El control de acceso vehicular número 5 formará parte de la red de control de acceso del edificio antiguo de la ex facultad de Ingeniería Química. El control de acceso vehicular número 4 formará parte de la red de control de acceso del edificio de Metalurgia Extractiva. El control de acceso vehicular número 2 formará parte de la red de control de acceso del edificio de Ciencias Nucleares (Casa Mata). El control de acceso vehicular número 1 formará parte de la red de control de acceso del edificio de Ciencias Biológicas.

De la información obtenida en los edificios de Metalurgia Extractiva y en el edificio antiguo de la facultad de Ingeniería Química no se tienen enlaces de Fibra Óptica pero éstos se conectan a los edificios principales que tienen los enlaces de fibra óptica mediante enlaces de cobre.

En los puntos de control de acceso vehicular se colocará un brazo mecánico en el ingreso al campus, además se colocará un equipo electromagnético denominado "loop" en el suelo. Estos dispositivos nos permiten prevenir que las barreras o portones sigan su proceso de cierre automático estando un vehículo en el área de impacto. En la figura 3.6 se muestra un ejemplo de funcionamiento para estos equipos.

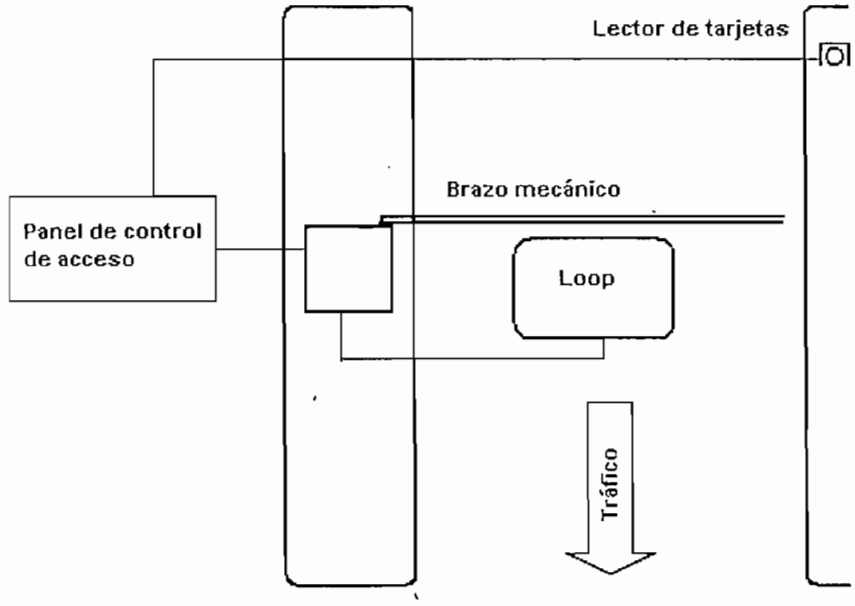


Figura 3.6 Ejemplo de funcionamiento de loop en un solo sentido

La figura 3.6 muestra el funcionamiento del sistema de control de acceso vehicular, cuando una persona desea pasar la barrera, presenta su tarjeta al lector de tarjetas de proximidad, el lector de tarjetas de proximidad envía el código al panel de control de acceso, si el código es válido el panel de control de acceso envía una señal de 12 V al brazo mecánico.

Mientras el auto está pasando por el loop, éste le enviará una señal eléctrica al brazo mecánico para que mantenga levantado el brazo hasta que el auto haya pasado totalmente.

En los sitios de control de acceso vehicular que sean en doble sentido como es el caso del acceso vehicular de eléctrica y el control de acceso vehicular de tecnólogos, se colocarán dos loops, uno en cada sentido (entrada, salida).

En estos sitios se colocará un solo brazo mecánico, tal vez se preguntará como se controlará el tráfico en los dos sentidos, para cumplir con este objetivo, los lectores de tarjetas estarán conectados a los mismos puertos del panel de control de acceso, simulando como si fuera un solo lector de tarjetas, el mismo concepto se utiliza para conectar los loops. La tendencia será a no tener guardias en cada una de las entradas para optimizar recursos.

3.2.4.2 Características técnicas del brazo mecánico de la empresa FACC modelo 620

Este tipo de brazos mecánicos son compatibles con los paneles de control de Northern Computers, ideales para tráfico mediano como es el caso de la EPN.

Requerimientos de energía:

230 [VAC] (+6% -10%), 1 [A]

Potencia absorbida 220 W.

Tiempo de respuesta: menos de 2 segundos.

Temperatura de operación:

-20° C a 55° C

Rango de humedad

0% a 90 % de humedad relativa, sin condensación

Dimensiones de la caja de protección:

Altura	115 cm.
Ancho	56 cm.
Profundidad	47 cm.

Longitud del brazo mecánico: 3 [m]

3.2.4.3 Características técnicas del loop para detección de vehículos de la empresa FAAC modelo DSP – 15

Temperatura de operación:

-75° C a 200° C

Dimensiones:

Altura	2 cm.
Ancho	427 cm.
Profundidad	183 cm.

Este dispositivo se conecta directamente al brazo mecánico y no necesita alimentación eléctrica adicional.

3.3 DISEÑO DEL SISTEMA ELÉCTRICO Y DE REDUNDANCIA DE ENERGÍA DEL SISTEMA DE CONTROL DE ACCESO.

3.3.1 INTRODUCCIÓN

El presente diseño eléctrico toma en cuenta el cálculo de las dimensiones de los cables que alimentarán a cada uno de los tomacorrientes usados para los paneles de control de acceso, los brazos mecánicos, cerraduras electromagnéticas, etc.

Como se mencionó en el capítulo 2, los paneles de control de acceso pueden funcionar sin alimentación eléctrica durante 4 horas pero las cerraduras electromagnéticas y los brazos mecánicos no tienen esta ventaja, motivo por lo

cuál se planteará la solución de redundancia de energía mediante la utilización de un UPS.

Uno de los principales problemas que actualmente se tiene en la parte eléctrica es que en los edificios no existe un sistema de puesta a tierra común para todo el edificio, es decir existen sistemas de puesta a tierra aislados, por ejemplo en el edificio antiguo de la ex facultad de Ingeniería Eléctrica, se tiene una varilla de coperweld para el sistema de puesta a tierra del laboratorio de máquinas eléctricas, etc. Este problema se repite en toda la Politécnica, motivo por lo cual se ha visto la necesidad de realizar el diseño de puesta a tierra para proteger los equipos, cabe recalcar que el sistema de puesta a tierra que se propondrá utilizar para proteger el sistema de control de acceso deberá drenar corrientes moderadas.

A continuación se presenta un análisis detallado de cómo se realiza el diseño de alimentación eléctrica del sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica y el diseño del sistema de puesta a tierra, el mismo que servirá como guía para realizar los diseños de las redes de control de acceso locales de los demás edificios.

3.3.2 DISEÑO DEL SISTEMA ELÉCTRICO Y DE REDUNDANCIA DE ENERGÍA DEL SISTEMA DE CONTROL DE ACCESO DE LA EX FACULTAD DE INGENIERÍA ELÉCTRICA. [4]

3.3.2.1 Cálculo de las dimensiones del conductor de alimentación desde el tablero de distribución regulado hacia cada uno de los tomacorrientes

De la información presentada en el capítulo 2 sobre los paneles de control de acceso de la empresa Northern Computers, se obtiene que éstos necesitan una alimentación de 12 VDC y consumen una corriente continua de 2 A, además las cerraduras electromagnéticas también necesitan una alimentación de 12 VDC y consumen una corriente continua máxima de 1 A, y como en los criterios de diseño se ha decido colocar paneles de control de acceso en cada piso para controlar el acceso a cada una de las ubicaciones de cada piso como se muestra en la figura 3.5, se ha decido colocar una fuente de alimentación DC, para que

alimente a cada una de las cerraduras electromagnéticas y a cada uno de los paneles de control de acceso como se muestra en la figura 3.7.

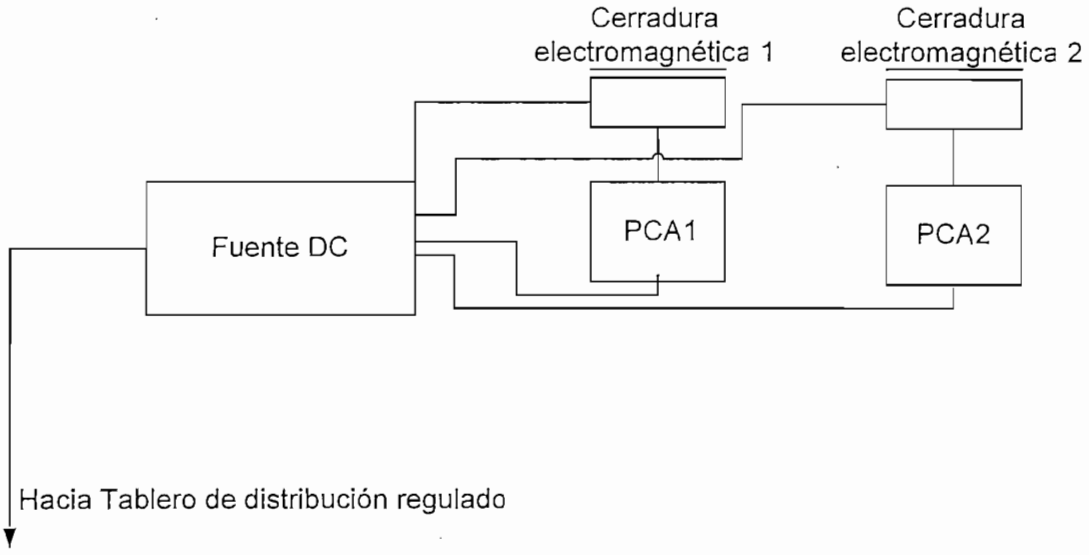


Figura 3.7 Forma de alimentación eléctrica de los paneles de control de acceso y las cerraduras electromagnéticas.

Para poder calcular las dimensiones del cable de alimentación eléctrico que llevará la corriente eléctrica (fase), se considera la ecuación de la potencia eléctrica alterna que dice:

$$P = kIV\cos\varphi \quad \{1\}$$

Dónde:

P= Potencia Eléctrica medida en [W]

I= Corriente Eléctrica medida en [A]

V=Diferencia de potencial eléctrico medida en [V]

φ = Angulo de desfasamiento entre la corriente y el voltaje

K=constante, para el caso de un sistema trifásico con 3 hilos (2 fases, neutro) es $\sqrt{3}$, Voltaje Fase Neutro.

S=P/cos φ = Potencia aparente medida en [VA]

Asumiendo que el ángulo de desfasamiento entre la corriente y el voltaje es cero, se puede deducir fácilmente que la potencia es igual a la potencia aparente como se muestra en la siguiente ecuación:

$$P = S \quad \{2\}$$

Remplazando la ecuación número 2 en la ecuación número 1 se obtiene:

$$I=S/kV \quad \{3\}$$

Antes de realizar el análisis tomaremos en cuenta que se utilizarán dos circuitos (breakers), uno para proteger la alimentación eléctrica del brazo mecánico y el otro para proteger las cerraduras electromagnéticas y los paneles de control de acceso.

Primero se calculará la potencia DC que se necesita debido a la carga DC (paneles de control + cerraduras), luego con esta potencia y asumiendo que el voltaje medido entre fase y neutro a la salida del UPS es de 121 V se obtiene la corriente que necesita el cable de alimentación (fase). Para calcular la corriente máxima que deberá soportar el cable de retorno (neutro) como el conductor de tierra se puede realizar la siguiente aproximación, la corriente que circula por estos conductores es el 70% de la corriente que circula por la fase.

Del análisis realizado anteriormente se ha determinado que en el piso dos se necesitan 2 paneles de control de acceso y 6 cerraduras electromagnéticas, en el piso 1 se necesitan 1 panel de control de acceso y 3 cerraduras electromagnéticas, en la planta baja se necesitan 2 paneles de control de acceso, 4 cerraduras electromagnéticas.

Si consideramos que una cerradura electromagnética necesita 12 VDC y consume una corriente de 1 A y que un panel de control de acceso necesita 12 VDC y consume 2 A, procedemos a calcular la potencia DC consumida en todo la red de control de acceso por los paneles de control de acceso y las cerraduras electromagnéticas de la siguiente manera:

Corriente consumida por las cerraduras = 13 * 1A= 13 A DC
Corriente consumida por los paneles = 7 * 2A= 14 A DC
Corriente total consumida = 27 A DC

Para calcular la potencia consumida por estos elementos en toda la red de control de acceso local, utilizamos una deducción de la ecuación número 1, para calcular

la potencia continua que dice: que la potencia es igual a la corriente DC por el voltaje DC.

P1=I*V=27 *12 =314 W "fórmula para la potencia continua"

De la misma forma procedemos a calcular la potencia consumida por el brazo mecánico recordemos que el brazo mecánico consume una potencia alterna, para lo cual utilizamos la ecuación número 1, considerando que el ángulo de desfasamiento es cero, además debemos recordar que el brazo mecánico necesita una alimentación de 220 V y consume una corriente de 1 A.

$P2=\sqrt{3}\,IV=\sqrt{3}*1*220=381.05$ W

Por lo tanto la potencia total que consumirá el sistema de control de acceso local será igual a la suma de P1+P2=695.05 W y considerando un 20% de crecimiento la potencia total sería de 833.66 W, como consideramos que el ángulo de desfasamiento es cero, la potencia aparente (S) sería de 833.66 VA.

Como P1=312 W considerando que el voltaje entre la fase y neutro es de 121 V y asumiendo que el ángulo de desfasamiento entre la corriente y el voltaje es cero procedemos a calcular la corriente que deberá soportar el circuito número 1, con la ayuda de la ecuación número 1.

$I1=P1/\sqrt{3}\,V=1.48$ A.

Como se puede observar es una corriente muy baja; para evitar caídas de voltaje y como el cable de alimentación para alimentar un tomacorriente debe ser mínimo un cable número 12 AWG el mismo que soporta una corriente máxima de 20 A, se utilizará para la fase un cable flexible número 12 AWG, y para alimentar la tierra y el neutro se utilizará un cable flexible número 14 AWG, además el breaker que protegerá el circuito número 1 debe ser de 20 A.

De la información obtenida podemos apreciar que el brazo mecánico consume una corriente de 1 A por precaución se utilizará cable número 12 AWG, el cable número 12 AWG soporta una corriente máxima de 20 A.

Pero aquí se tiene otro inconveniente, la distancia desde el tablero de distribución al brazo mecánico es de aproximadamente 90 m, debido a esta gran distancia pueden existir caídas de potencial, cabe recalcar que el porcentaje máximo de caída de potencial desde el tablero de distribución regulado hacia la carga (en este caso brazo mecánico) no debe ser mayor del 3%, para poder determinar esto utilizamos la ecuación número 4 que dice:

$$\Delta V = \frac{k1 * L * I * K2}{A} \quad \{4\}$$

Donde:

ΔV = Caída de voltaje [V]

L=longitud del alimentador [m]

I= corriente del circuito [A]

A=Sección transversal del conductor [Circular Mil]

K1= constante que depende del material del conductor, (cu =78.74, Al=118.11)

K2= 0.5 para un sistema trifásico 3 hilos (2 fases+neutro).

Utilizando la ecuación número 4 se calcula la caída de voltaje, con los siguientes datos para un cable de cobre flexible número 12 AWG.

$$\Delta V = \frac{78.74 * 90 * 20 * 0.5}{6530} = 10.85 \text{ V}$$

Expresando porcentualmente será: $\Delta V(\%) = \frac{10.85}{220} * 100\% = 4.93\%$

Utilizando un cable flexible número 8 AWG se logra el objetivo propuesto.

$$\Delta V = \frac{78.74 * 90 * 20 * 0.5}{16510} = 4.29 \text{ V}$$

Expresando porcentualmente será: $\Delta V(\%) = \frac{4.29}{220} * 100\% = 1.95\%$

Por lo tanto para alimentar eléctricamente el brazo mecánico se utilizará cable flexible número 8 AWG para alimentar cada una de las fases y un cable flexible número 10 para alimentar la tierra. Además el breaker que protegerá el circuito número 2 deberá ser de 20 A bifásico.

Ahora calculemos el número de cable que necesitamos para alimentar el tablero regulado desde la salida del UPS.

Como se mencionó anteriormente la carga máxima que debería soportar el tablero de distribución regulado debería ser de 863.66 VA, de esta forma se puede definir la carga que debe soportar el UPS.

Con esta información calculamos la corriente máxima que deberá soportar el cable mediante la ecuación número 1, asumiendo que el ángulo de desfasamiento es cero:

$I_{UPS\text{-}TDR}$= 863.66 / $\sqrt{3}$ *121=4.11 A, aproximadamente 5 [A].

Por lo tanto:

- Para alimentar eléctricamente el brazo mecánico se utilizarán 2 cables flexibles número 8 AWG (fases) + 1 cable flexible número 10 AWG (tierra).

- Para alimentar los tomacorrientes para las fuentes DC que se utilizan para alimentar las cerraduras electromagnéticas y los paneles de control de acceso se utilizará 1 cable flexible número 12 AWG (fase) + 2 cables flexibles número 14 AWG (neutro, tierra).

- Para alimentar eléctricamente el tablero de distribución regulado se puede utilizar cable flexible número 14 pero por seguridad se utilizará cuatro cables flexibles número 10 AWG.

- La carga que debe soportar el UPS es de 1 [KVA] aproximadamente.

3.3.2.2 Diseño del sistema de puesta a tierra del sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica.

Antes de realizar el diseño del sistema de puesta a tierra debemos conocer la resistividad del suelo para lo cual tomaremos como dato el valor de resistividad de suelo investigado para el diseño del sistema de puesta a tierra del laboratorio de Alto Voltaje, propuesto en el proyecto de titulación "DISEÑO DEL SISTEMA DE APANTALLAMIENTO DEL NUEVO LABORATORIO DE ALTA TENSIÓN PARA LA EPN" [6], en el cual se define el valor de la resistividad del suelo del laboratorio de la ex facultad de Ingeniería Eléctrica es aproximadamente 3.000Ω.cm, este valor se puede considerar el mismo para los demás sistemas de puesta a tierra ubicados en cada uno de los puntos de acceso vehicular.

La ecuación número 5 muestra un método de cómo calcular el valor de la resistividad de la puesta a tierra utilizando una varilla, cabe recalcar que este valor debe ser menor a 25 Ω, se recomienda qué este valor se encuentre en el rango de 5 a 10 Ω.

$$R_{1V}=\frac{\rho}{2\Pi L}\ln\left(\frac{4L}{d}\right) \quad \{5\}$$

Donde:

ρ= resistividad del suelo (3.000Ω.cm)

L= longitud de la varilla de coperweld (1,80 m)

d= diámetro de la varilla de coperweld (0,23 cm)

Utilizando la ecuación número 5, podemos determinar que el valor de la resistencia del sistema de puesta a tierra es R1V=21,35 Ω.

Por lo tanto debemos calcular el sistema de puesta a tierra utilizando dos varillas como se muestra en la ecuación número 6.

$$R2V=\frac{\rho}{4\Pi L}\left(1+\frac{L}{D}\right) \quad \{6\}$$

Donde:

ρ= resistividad del suelo (3.000Ω.cm)

L= longitud de la varilla de coperweld (1,80 m)

D= Distancia en línea recta entre las dos varillas (0,50 cm)

Realizando los cálculos correspondientes podemos determinar que el valor de la resistencia R2v=6,1 Ω.

Por lo tanto utilizaremos dos varillas para proteger el sistema de control de acceso en caso de qué existan corrientes indeseables que deban ir al sistema de puesta a tierra, para conectar las dos varillas utilizaremos cable flexible número 10, la corriente máxima que debe soportar el cable que es utilizado para conectar las dos varillas es la misma corriente que se calculó para alimentar los tableros de distribución por precaución se seleccionó un cable flexible número 10 AWG.

Para mantener la resistividad del suelo y proteger la varilla de coperweld de la corrosión se utilizará sulfato de magnesio o sulfato de cobre.

En la figura 3.8 se muestra el diagrama vertical eléctrico del sistema de control de acceso del edificio antiguo de eléctrica.

En la figura 3.9 se muestra el diagrama unifilar eléctrico. Los dos gráficos ayudarán a comprender de una mejor manera el procedimiento antes realizado.

3.3.2.3 Selección del UPS

A continuación se presenta el análisis técnico económico de dos opciones de dos fabricantes de UPS, los mismos que tienen presencia en el mercado ecuatoriano.

Características	POWER WARE 9170 PW6S6K	GAMATRONIC
Alimentación Eléctrica	Voltajes: 208-240 VAC o 200/100, 208/120, 220/110, 240/121VAC. Factor de potencia de entrada 0,98. Frecuencia 50/60 Hz (+-3Hz)	Voltajes: 208-240 VAC o 200/100. Factor de potencia de entrada 0,89. Frecuencia 57-63 Hz
Salida Eléctrica	Voltajes: 208-240 VAC o 200/100, 208/120, 220/110, 240/121VAC. Regulación del voltaje (+-3% del voltaje de entrada). Eficiencia: 88% en operación normal. Regulación de frecuencia= +-3% de la frecuencia de entrada.	Voltajes: 120/208 VAC. Regulación del voltaje (+-2% del voltaje de entrada). Regulación de frecuencia= +-2% de la frecuencia de entrada.
Comunicaciones	Display LCD 4x20 caracteres. Puerto de Comunicaciones RS-232. Soporta SNMP	Display LCD. Puerto de Comunicaciones RS-232. Soporta SNMP
Tiempo de Respaldo	26 minutos a plena carga	12 minutos a plena carga
Temperatura de operación	-20°C a 40°C	-10°C a 40°C
Potencia de Salida	1 KVA expandible a 3 KVA	1 KVA expandible a 4 KVA
Dimensiones	Altura 30 cm. Ancho 25 cm. Profundidad 35 cm.	Altura 30 cm. Ancho 35 cm. Profundidad 40 cm.
Peso	10.8 Kg	10.2 Kg
Reemplazo de baterías	En caliente	En caliente
Costo $	750.65	650.75

Tabla 3.1 Comparación técnica económica de dos marcas de UPS.

En la tabla 3.1 se presenta un resumen sobre las características técnicas y económicas de dos diferentes propuestas de UPS.

Los dos UPS tienen características muy similares, lo que la diferencia principalmente es el tiempo de respuesta. Después realizar una comparación de las características de los dos tipos de UPS se ha decidido utilizar la opción de POWER WARE. El UPS es una propuesta adicional para que funcione de una mejor manera el sistema de control de acceso, como se ha indicado anteriormente, los brazos mecánicos pueden ser abiertos en casos de ausencia de energía por una llave manual, en cambio las cerraduras electromagnéticas en caso de ausencia de energía quedan abiertas. Por está razón las puertas poseen una segunda cerradura normal que da seguridad cuando no hay energía.

Sin embargo el sistema de respaldo de energía otorga sólo 26 minutos de alimentación por cual no sería útil a largo plazo, será utilizado sólo para tomar acciones inmediatas cuando se ha cortado la energía eléctrica, existen en el mercado otras opciones para proteger las ubicaciones en lugar de utilizar las cerraduras electromagnéticas como es el caso de los pestillos magnéticos los mismos que se colocan como la parte hembra de la cerradura normal, no se utilizará esta opción por que solo disminuye la seguridad propuesta. Una mejor opción a la del UPS consiste en alimentar el sistema de control de acceso con el generador que se dispone en el edificio de la ex facultad de Ingeniería Eléctrica.

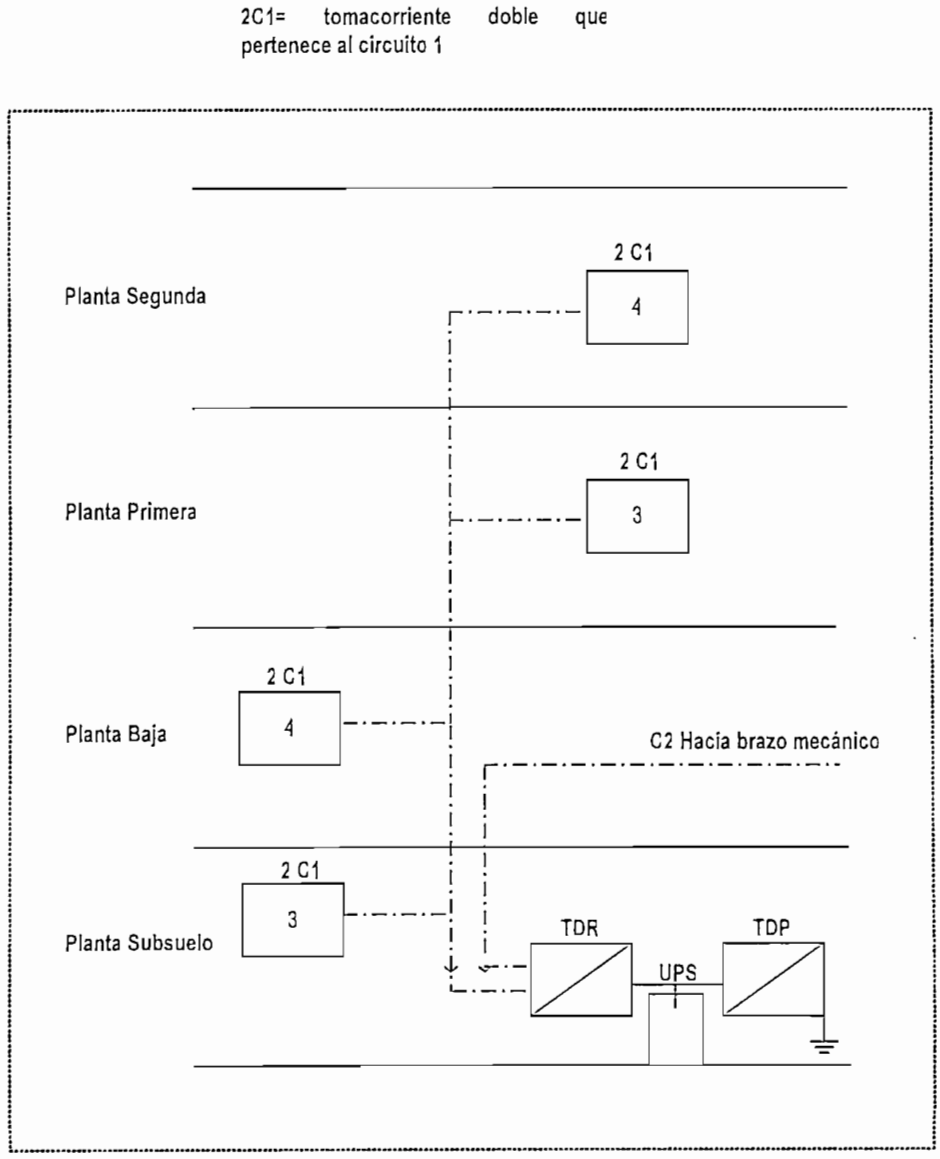


Figura 3.8 Diagrama vertical eléctrico del sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica.

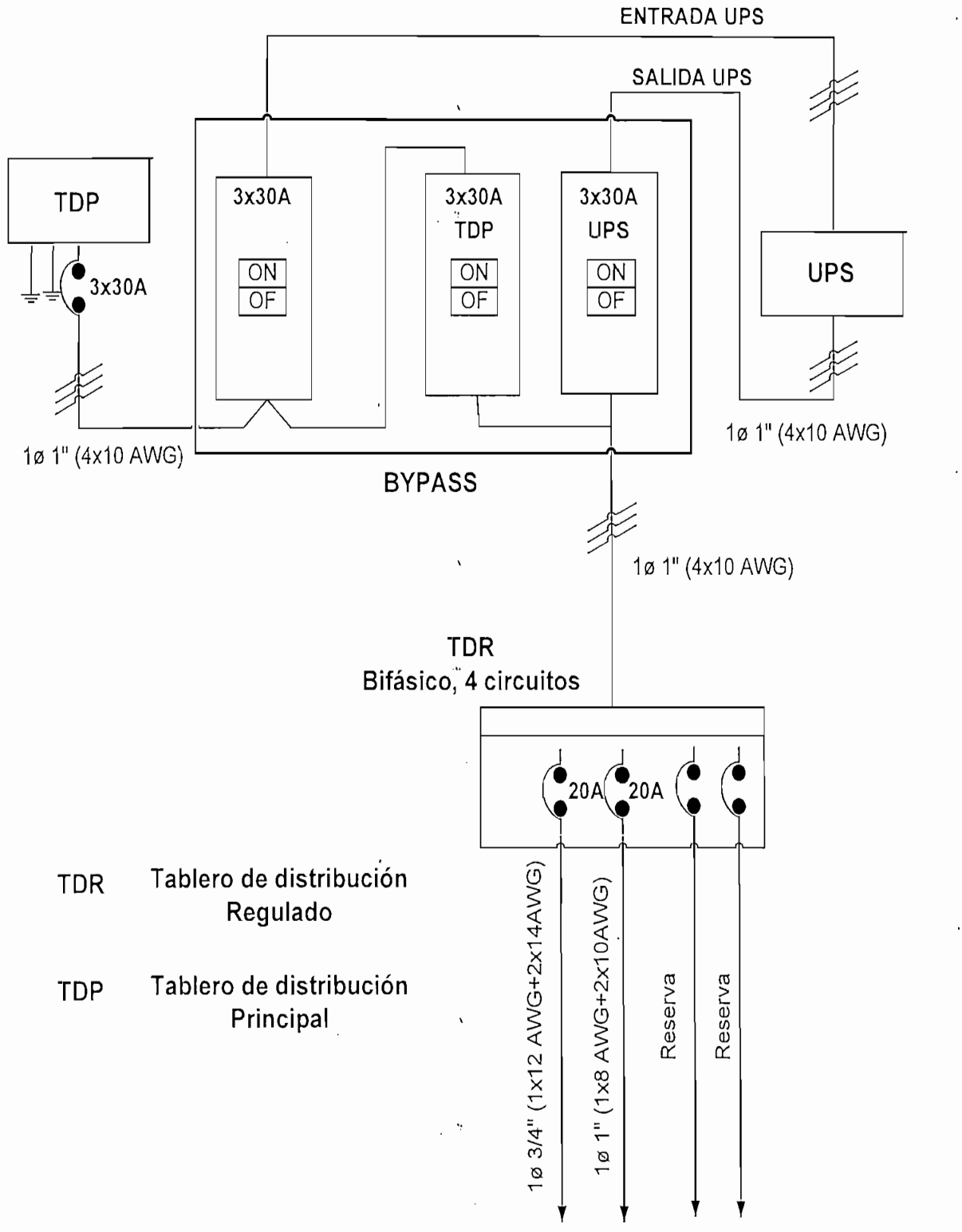


Figura 3.9 Diagrama unifilar eléctrico del sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica.

3.3.3 DISEÑO DEL SISTEMA ELÉCTRICO PARA EL SISTEMA DE CONTROL DE ACCESO VEHICULAR. [4]

3.3.3.1 Introducción

Como se ha mencionado anteriormente cada uno de los puntos de acceso vehicular se conectarán a las redes de control de acceso más cercano, a continuación se presenta el tipo de cable a utilizarse en cada uno de los puntos de control de acceso vehicular.

Como se mencionó anteriormente, en alguno de los edificios principales no existe sistemas de puesta a tierra, motivo por el cual se recomienda realizar el diseño e implementación inmediata de dichos sistemas, los mismos que servirán para proteger todos los dispositivos electrónicos que se tienen en cada una de las ubicaciones.

Para poder diseñar la carga que debe soportar el UPS se debe conocer la carga total que deberá soportar cada una de las redes de control de acceso local, motivo por lo cual sólo se planteará el diseño del UPS para la red de control de acceso del edificio antiguo de la ex Facultad de Ingeniería Eléctrica.

A continuación se presenta un resumen con el tipo de cable a utilizarse en cada uno de los sistemas de control de acceso vehicular, cabe recalcar que sólo se esta realizando el análisis eléctrico para alimentar los brazos mecánicos y un panel de control de acceso. Los criterios de diseño son los mismos utilizados en el ejemplo realizado del edificio antiguo de Ingeniería Eléctrica.

Sistema de control de acceso vehicular	Tipo de cable eléctrico	Observaciones
Acceso número 1 Próximo al edificio de Ciencias Biológicas	Alimentación eléctrica de las fases (cable flexible número 8 AWG), Alimentación eléctrica Tierra (Cable flexible número 10 AWG)	Se utilizarán dos circuitos, un circuito alimentará un brazo y los paneles de control y el otro alimentará el otro brazo. El centro de carga debe ser bifásico de cuatro circuitos para dejar dos circuitos de reserva y cada uno de los breakers debe soportar máximo 20 A. La máxima distancia desde el tablero de breakers al brazo mecánico es aproximadamente 90 m. Se utilizarán 2 varillas coperweld para realizar el sistema de puesta a tierra.

Acceso número 2 Próximo al edificio de Ciencias Nucleares.	Alimentación eléctrica de las fases (cable flexible número 8 AWG), Alimentación eléctrica Tierra (Cable flexible número 10 AWG)	Se utilizarán dos circuitos, un circuito alimentará un brazo y los paneles de control y el otro alimentará el otro brazo mecánico. El centro de carga debe ser bifásico de cuatro circuitos para dejar dos circuitos de reserva y cada uno de los breakers debe soportar máximo 20 A. La máxima distancia desde el tablero de breakers al brazo mecánico es aproximadamente 90 m. Se utilizarán 2 varillas coperweld para realizar el sistema de puesta a tierra.
Acceso número 3 Próximo al edificio Antiguo de la ex Facultad de Ingeniería Eléctrica	Alimentación eléctrica de las fases (cable flexible número 8 AWG), Alimentación eléctrica Tierra (Cable flexible número 10 AWG)	Se utilizarán dos circuitos, uno para alimentar el brazo mecánico y el otro para alimentar los paneles de control de acceso, con el objetivo de balancear la carga. El centro de carga debe ser bifásico de cuatro circuitos para dejar dos circuitos de reserva y cada uno de los breakers debe soportar máximo 20 A. La máxima distancia desde el tablero de breakers al brazo mecánico es aproximadamente 90 m. Se utilizarán 2 varillas coperweld para realizar el sistema de puesta a tierra.
Acceso número 4 Próximo al edificio de Metalurgia Extractiva Tecnólogos	Alimentación eléctrica de las fases (cable flexible número 8 AWG), Alimentación eléctrica Tierra (Cable flexible número 10 AWG)	Se utilizará dos circuitos uno para alimentar el brazo mecánico y el otro para alimentar los paneles de control con el objetivo de balancear la carga. El centro de carga debe ser bifásico de cuatro circuitos para dejar dos circuitos de reserva y el breaker debe soportar máximo 20 A. La máxima distancia desde el tablero de breakers al brazo mecánico es aproximadamente 100 m. Cabe recalcar que en esta ubicación se tiene un solo brazo mecánico. Se utilizarán 2 varillas coperweld para realizar el sistema de puesta a tierra.
Acceso número 5 Próximo al edificio antiguo de Ingeniería Química	Alimentación eléctrica de las fases (cable flexible número 10 AWG), Alimentación eléctrica Tierra (Cable flexible número 12 AWG)	Se utilizarán dos circuitos uno para alimentar un brazo mecánico y los paneles de control y el otro para alimentar el otro brazo, con el objetivo de balancear la carga. El centro de carga debe ser bifásico de cuatro circuitos para dejar dos circuitos de reserva y cada uno de los breakers debe soportar máximo 20 A. La máxima distancia desde el tablero de breakers al brazo mecánico es aproximadamente 40 m. Se utilizarán 2 varillas coperweld para realizar el sistema de puesta a tierra.

3.4 DISEÑO DEL SISTEMA DE REDUNDANCIA PARA TRANSMISIÓN DE DATOS DEL SISTEMA DE CONTROL DE ACCESO.

3.4.1 INTRODUCCIÓN

Como se ha mencionado anteriormente este proyecto de titulación planteará un sistema de respaldo de transmisión de datos para garantizar la comunicación con el servidor de administración. Para cumplir con este objetivo se planteará un sistema de transmisión de información inalámbrico, el mismo que se utilizará en caso de que exista alguna falla en la transmisión de datos, a través del backbone de fibra óptica que actualmente existe en la Politécnica. El sistema de respaldo inalámbrico tendrá su punto de concentración en el edificio de administración mediante la utilización de una antena omnidireccional y se colocarán antenas direccionales en cada uno de los edificios principales en donde se tendrán las redes de control de acceso locales.

Para cumplir con el objetivo de este proyecto de titulación en el cual se planteaba proteger los cinco puntos de acceso vehicular, el centro de cómputo general y el edificio antiguo de Ingeniería Eléctrica se colocarán las antenas en los edificios principales como se muestra en la figura 3.10.

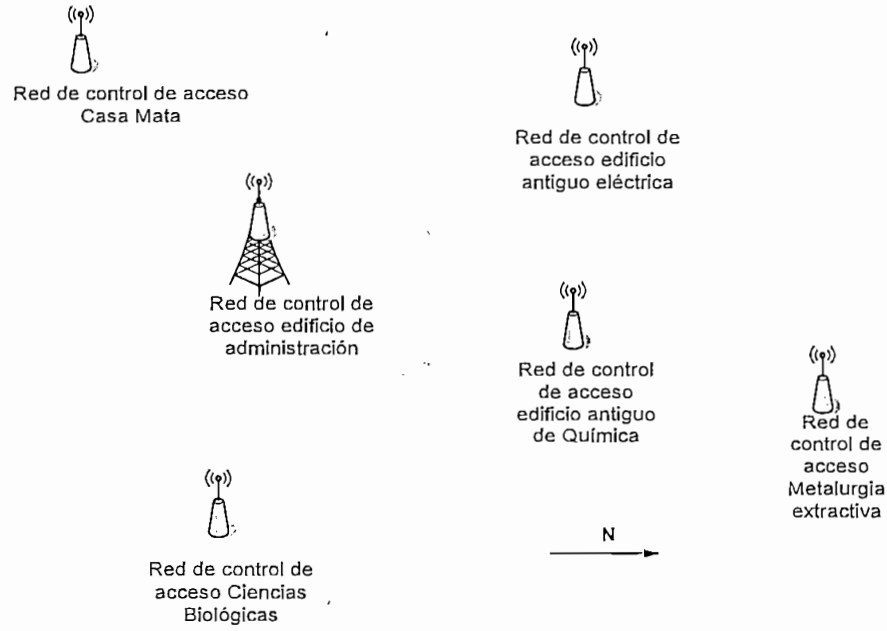


Figura 3.10 Sistema inalámbrico de respaldo de transmisión de datos del sistema de control de acceso.

En la actualidad existen muchas empresas que se dedican a producir equipo para cumplir con los desafíos inalámbricos, llegando a alcanzar enormes distancias a grandes velocidades de transmisión, a continuación se presenta el análisis técnico económico de dos propuestas para cumplir con el objetivo propuesto, la una propuesta esta a cargo de la empresa TERABEAM con su producto Marquee Point to Multipoint, y la otra propuesta esta a cargo de 3 Com con su producto building to building Bridge.

Características	TERABEAM MARQUEE POINT TO MULTIPOINT	3 COM BUILDING TO BUILDING BRIDGE
Dimensiones	Altura: 38,9 cm. Ancho: 38,9 cm. Profundidad: 2 cm	Altura: 35 cm. Ancho: 38 cm. Profundidad: 7 cm
Peso	1,32 [Kg]	2,54 [Kg]
Alimentación de energía	110/220 VAC 50/60Hz	110/220 VAC 50/60Hz
Longitud máxima del cable desde la antena hasta el bridge	390 [m]	200 [m]
Velocidad de transmisión	Hasta 54 Mbps	Hasta 11 Mbps
Puerto de Comunicaciones	RJ-45	RJ-45, 10 BaseT/100 Base Tx
Temperatura de operación	-30°C a 60°C	-33°C a 50°C
Corriente máxima consumida	0,5 [A]	0,5 [A]
Potencia máxima consumida	16 [W]	20 [W]
Frecuencia de operación	5.725 a 5,8 GHz	2,4-2 a 48GHz
Pérdida de retorno	12 dbi mínimo	8 dbi mínimo
Ganancia	23 dbi antena direccional, 16 dbi antena omnidireccional	13 dbi antena direccional, 8 dbi antena omnidireccional
Especificaciones de red	Soporta MAC (Media Access control), Soporta autenticación Radius, Soporta Rip II, Soporta Spanning Tree, Encripcion DES, Servidor DHCP, Soporta NAT, Soporta SNMP	Soporta MAC (Media Access control), Soporta Spanning Tree, Encripcion DES, Servidor DHCP, Soporta NAT, Soporta SNMP
Alcance	2 [Km]	1.471 [m]
Esquema de modulación	OFDM-QPSK	DSSS
Costo $	Bridge más antena direccional (Cliente)=$ 519 Bridge más antena omnidireccional (Base)=$ 1.599	Bridge más antena direccional (Cliente)=$ 890 Bridge más antena omnidireccional (Base)=$ 890

Tabla 3.2 Comparación técnica económica de dos productos de acceso inalámbrico

Del análisis técnico económico realizado anteriormente y tomando en cuenta que se necesitan 5 equipos clientes y un equipo base, se puede apreciar que la solución propuesta por la empresa TERABEAM es la mejor de las dos opciones.

3.5 NORMAS DE ADMINISTRACIÓN PARA EL SISTEMA DE CONTROL DE ACCESO [5]

Para facilitar la administración del sistema de control de acceso se define a continuación cómo se etiquetarán los extremos de los cables que conectan las cerraduras electromagnéticas con los paneles de control de acceso, los extremos de los cables que conectan los lectores (tarjetas o biométricos) con el panel de control de acceso, además se definirán los cuadros de distribución de seguridad.

Se etiquetarán con etiquetas de sujeción los extremos de los cables que conectan los dispositivos de control de acceso hacia cada uno de los paneles de control de acceso, la misma etiqueta se utilizará en los dos extremos del cable, para cumplir con este objetivo se utilizará la siguiente nomenclatura:

¥#-NN-IP-IE

Donde:

¥: Identificación del dispositivo que se encuentra conectado al panel de control de acceso, para lo cual se utilizará la siguiente simbología:

C= Cerradura Electromagnética

P= Lector de Tarjetas de proximidad

B= Lector biométrico basado en la geometría de la mano

M= Brazo mecánico

I = Interruptor

#: Es el número del puerto al cual se encuentra conectado el dispositivo en el panel de control de acceso, recordemos que cada panel de control puede controlar máximo 4 lectoras, con sus respectivas cerraduras electromagnéticas.

NN: Es el número de panel de control de acceso este tiene un rango de 01 a 31.

IP: Es la identificación del piso en donde se encuentra ubicado el panel de control de acceso, los dispositivos estarán ubicados en el mismo piso de los paneles de control de acceso a los cuales se encuentran conectados, a excepción de los brazos mecánicos, para lo cual se utilizará la siguiente nomenclatura:

01: Planta Subsuelo
02: Planta Baja
03: Planta Primera
04: Planta Segunda

IE: Es la identificación del edificio al cual corresponde la red de control de acceso local, para lo cual se tomará la siguiente nomenclatura para identificar a los edificios.

01 = Edificio Ciencias Biológicas
02 = Edificio Casa Mata
03 = Edificio antiguo de Eléctrica
04 = Edificio Metalurgia Extractiva
05 = Edificio antiguo de Química
06 = Edificio de administración

Por ejemplo:

C1-04-01-03

Significa:

La cerradura electromagnética se encuentra conectada al relé número 1 del panel de control de acceso número 4, que se encuentra ubicado en la planta subsuelo del Edificio antiguo de Eléctrica.

B1-05-02-03

Significa:

El brazo mecánico se encuentra conectado al relé número 1 del panel de control de acceso número 5, el panel de control de acceso se encuentra ubicado en la planta baja del Edificio antiguo de Eléctrica.

3.6 ANÁLISIS DE COSTOS DEL SISTEMA DE CONTROL DE ACCESO.

3.6.1 INTRODUCCIÓN [4][5]

En el Anexo número 4 se presenta la información detallada acerca del cómputo de materiales del sistema de control de acceso del edificio antiguo de la ex facultad de Ingeniería Eléctrica, del sistema de control de acceso vehicular de cada uno de los puntos que cumplen con dicho objetivo y del sistema de control de acceso del centro de cómputo general, a continuación se presentan los criterios tomados para determinar la cantidad de material a utilizar.

Cálculo del cableado horizontal

Para realizar este cálculo se debe tomar en cuenta los siguientes datos:

DMin =Distancia al punto más cercano desde el Panel de control hasta el lector.

DMax =Distancia al punto más lejano desde el Panel de control hasta el lector.

Con estos valores se obtiene el promedio de la longitud del cable a utilizar.

DP= (DMax+DMin)/2

Para obtener la cantidad de cable UTP a utilizar en cada piso se procede a multiplicar el valor promedio por el número de lectoras y se obtiene la longitud del cable a utilizar cabe recalcar que se debe dejar una holgura del 10% + 2.5 m.

Para calcular la cantidad de cable 2x22 AWG a utilizar por piso se procede a multiplicar la cantidad de cable UTP por dos, recordemos que se utilizará un cable

2x22 AWG para conectar la cerradura electromagnética y otro cable 2x22 AWG para conectar el interruptor.

Dimensiones de la tubería a utilizar

Para poder determinar el diámetro de la tubería metálica a utilizar para poder transportar cada uno de los tipos de cables se utilizó las siguientes tablas:

Conduit		Número de Cables 24 AWG (UTP)
Diámetro interno (mm)	Medida (pulg)	
15.8	1/2	0
20.9	3/4	3
26.6	1	6
35.1	1 ¼	10
40.9	1 ½	15
52.5	2	20
62.7	2 ½	30
77.9	3	40

Tabla 3.3 Número máximo de cables UTP por tubería Conduit.

Tamaño AWG MCM	Número máximo de conductores TW, THW en tubería conduit							
	½	¾	1	1 ¼	1 ½	2	2 ½	3
	Pulg	Pulg	Pulg	Pulg	Pulg	Pulg	Pulg	Pulg
18	7	12	20	35	49	80	115	176
16	6	10	17	30	41	68	98	150
14	4	6	10	18	25	41	58	90
12	3	5	8	15	24	34	50	76
10	1	4	7	13	17	29	41	64
8	1	3	4	7	10	17	25	38
6	1	1	3	4	6	10	15	23
4		1	1	3	4	7	10	16

Tabla 3.4 Número máximo de conductores TW, THW (Eléctricos) en tubería Conduit.

Una vez definido el tipo de tubería a utilizar se debe tomar en cuenta que deben existir cajas de paso, para poder pescar los cables, no se deben hacer empalmes en las cajas de paso. Para poder determinar el número de cajas de paso se debe tomar en consideración que éstas deben estar cada 2 tubos de 3 m de longitud si la trayectoria es recta, caso contrario se debe colocar una caja de paso en cada una de las esquinas.

Además se debe considerar que deben existir conectores y abrazaderas para realizar la instalación de estos materiales para lo cual se considera los siguientes criterios:

Número de abrazaderas= 3xnúmero de tubos
Número de conectores = 2xnúmero de cajas.
Número de uniones = número de tubos.

Existen muchos otros elementos que se deben considerar en el diseño como se muestra en el Anexo número 4 pero el objetivo de este proyecto de titulación no es el de definir cómo realizar el cómputo de materiales, motivo por el cual en el Anexo número 4 se presenta el tipo de materiales a utilizar y las cantidades computadas para este proyecto.

A continuación se presenta un resumen del análisis de costos, considerando por separado el análisis de costos del sistema de control de acceso vehicular, análisis de costos del sistema de control de acceso del edificio antiguo de Ingeniería Eléctrica y el análisis de costos del sistema de control de acceso del centro de cómputo general, la idea es que las autoridades de la EPN comiencen por implementar el sistema de control de acceso vehicular y el sistema de control de acceso del centro de cómputo general para lo cual se presentan en cada una de las propuestas dos escenarios en los cuales se consideran todos los requerimientos para que funcionen cada una de las propuestas y el otro con los requerimientos mínimos necesarios para que funcionen cada una de las propuestas referentes al control de acceso físico, además se realiza un análisis de cómo financiar dichas soluciones.

3.6.2 ANÁLISIS DE COSTOS DEL SISTEMA DE CONTROL DE ACCESO VEHICULAR DE LA EPN.

ITEM	Descripción	Unidad Medida	Cantidad	Precio Unitario	Total
	COSTO TOTAL DEL PROYECTO				**42.722,43**
	1 Total Sistema de Control de Acceso				**35.013,15**
	1.1 Equipos Control Acceso				**32.207,74**
101	FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	5	150,00	750,00
102	CONVERTIDORES RS-485 ETHERNET	u	5	299,00	1.495,00
103	SERVIDOR DE ADMINISTRACION HP PROLIANT ML350 G4	u	1	3.693,00	3.693,00
104	IMPRESORA PARA TARJETAS	u	1	4125,40	4.125,40
105	SOFTWARE DE ADMINISTRACION	u	1	825,44	825,44
106	CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	5	2,32	11,60
107	PC ACCESO N-1000-III	u	5	1.500,00	7.500,00
108	LECTOR DE PROXIMIDAD	u	10	170,73	1.707,30
109	LOOP	u	10	250,00	2.500,00
110	BRAZO MECANICO	u	8	1.200,00	9.600,00
	1.2 Elementos Cableado				**2.011,70**
111	CABLE UTP 04 PAR C5E	m	890	0,19	169,10
112	CABLE SPT 2X22 AWG	m	980	0,22	215,60
113	TUBO EMT 3/4" X3M	u	445	3,60	1.602,00
114	CANALETA PVC 20X12X2M LISA	u	25	1,00	25,00
	1.3 Consumibles Cableado				**40,66**
115	AMARRAS PLASTICAS 20CM	u	150	0,02	3,00
116	TACO F-6	u	595	0,01	5,95
117	TORNILLO COLEPATO 1X8	u	595	0,01	5,95
118	TORNILLO COLEPATO 1/2X8	u	200	0,01	2,00
119	SILICONA	u	2	0,63	1,26
120	SIERRAS	u	10	2,25	22,50
	1.4 Consumibles canaleta				**18**
121	UNIONES20X12	u	36	0,50	18
	1.5 Consumibles Tubería				**735,05**
122	CAJA EMT 12X12CM	u	90	0,75	67,50
123	TAPA CAJA EMT 12X12CM	u	90	0,27	24,30
124	CONECTOR EMT 3/4"	u	1000	0,32	320,00
125	UNION EMT 3/4"	u	505	0,32	161,60
126	ABRAZADERA EMT ¾"	u	1500	0,08	120,00
127	ALAMBRE GALVANIZADO N°, 18	Kg	5	1,13	5,65
128	CODO EMT 3/4"	u	60	0,60	36,00
	2 TOTAL SISTEMA DE ALIMENTACION ELECTRICO				**1.304,28**
	2.1 Sistema de Alimentación Eléctrico				**1.287,40**
201	CABLE TW 08 AWG, MULTIFILAR	m	800	0,47	376,00
202	CABLE TW 10 AWG, MULTIFILAR	m	2000	0,35	700,00
203	CABLE TW 12 AWG, MULTIFILAR	m	170	0,22	37,40
205	BREAKER 1X20A	u	10	3,90	39,00
207	CENTRO DE CARGA BIFASICO 4 CIRCUITOS	u	5	19,00	95,00
208	VARILLA COPERWELD DE HIERRO BAÑADA DE COBRE	u	10	4,40	44,00
210	GEL DE SULFATO DE COBRE	Q	1	19,00	19,00
	2.2 Consumibles Eléctrico				**12,88**
208	CINTA AISLANTE 20 YD	u	5	0,70	3,50
209	ETIQUETA CABLE C.VERDE	u	50	0,10	5,00

210	MASKING	u	5	0,88	4,38
	3 TOTAL SISTEMA DE REDUNDANCIA DE TRANSMISION DE DATOS				**4.405**
	3.1 Sistema de Redundancia de transmisión de datos				**4.405**
106	SISTEMA ANTENA BASE	u	1	1.600,00	1.600,00
107	SISTEMA ANTENA CLIENTE	u	5	519,00	2.595,00
109	SOPORTE PARA ANTENAS 2m C/BASE METALICA	u	6	35,00	210,00
	4 MANO DE OBRA Y CONFIGURACION DEL SISTEMA				**2.000,00**

Del análisis económico realizado se puede concluir que el costo total para implementar el sistema de control de acceso vehicular en la EPN con un sistema de redundancia de transmisión de datos es de **$ 42.722,43**.

Se puede implementar el sistema de control de acceso vehicular quitando el sistema de redundancia de transmisión de datos, con lo cual el costo de la implementación es de **$ 38.317,43,** obteniéndose un ahorro de **$4405**.

Este proyecto de titulación propone que se realice la instalación del sistema de control de acceso vehicular con las especificaciones mínimas necesarias, es decir sin la implementación del sistema de redundancia de transmisión de datos el mismo que puede ser instalado posteriormente.

De la información presentada en el capítulo 1 se puede apreciar que en el semestre Abril/Agosto se vendieron únicamente 80 adhesivos a los estudiantes y se obsequiaron 1.200 adhesivos a los profesores, para financiar la inversión inicial se propone cobrar 30 $ el primer semestre a cada uno de los profesores, estudiantes y trabajadores que deseen ingresar con su vehiculo al campus Politécnico, de éstos 30 $ se destinarán 15 $ para la realización de la tarjeta de identificación, de éstos 15 $ se utilizarán 8 $ para la realización de la tarjeta de autenticación con lo cual se tendrá un margen de recuperación de 7$ por cada tarjeta, por lo tanto se podría obtener $ 8.960 por semestre, con este dinero se puede financiar la inversión inicial del sistema de control de acceso vehicular de la Escuela Politécnica Nacional en 4 semestres aproximadamente.

3.6.3 ANÁLISIS DE COSTOS DEL SISTEMA DE CONTROL DE ACCESO EDIFICIO ANTIGUO DE ELÉCTRICA.

ITEM	Descripción	Unidad Medida	Cantidad	Precio Unitario	Total
	COSTO TOTAL PROYECTO				**25.670,90**
	1 Total Sistema de Control de Acceso				**24.617,93**
	1.1 Equipos Control Acceso				**23.654,41**
101	PUERTAS METALICAS 0.90x2m, C/CERRADURA DE POMO KWIIKSET	u	12	280,00	3.360,00
102	PUERTAS METALICAS BATIENTES 1,50x2, C/CERRADURA DE POMO KWIKSET	u	4	360,00	1.440,00
103	FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	4	150,00	600,00
104	CONTACTOS MAGNETICOS	u	18	2,80	50,40
105	CONVERTIDORES RS-485 ETHERNET	u	1	299,00	299,00
106	BRAZOS PEQUEÑOS PARA CERRAR PUERTA	u	18	8,75	157,50
107	LECTOR DE PROX	u	19	170,73	3.243,87
108	CERRADURA ELECTROMAGNETICA	u	18	138,00	2.484,00
109	HAND PUNCH	u	1	1.832,44	1.832,44
110	PC ACCESO N-1000-IV	u	5	2.037,44	10.187.64
	1.2 Elementos Cableado				**718,54**
111	CABLE UTP 04 PAR C5E	m	630	0,19	119,70
112	CABLE SPT 2X22 AWG	m	660	0,22	145,20
113	TUBO EMT 3/4" X3M	u	70	3,60	252,00
114	TUBO EMT 1" X3M	u	20	5,58	111,60
115	CANALETA PVC 20X12X2M LISA	u	40	1,00	40,00
116	INTERRUPTOR SIMPLE C/TAPA	u	18	1,40	25,20
117	CAJA PVC 10X5X4CM C. ALMENDRA	u	18	1,38	24,84
	1.3 Consumibles Cableado				**40,55**
118	AMARRAS PLASTICAS 20CM	u	120	0,02	2,40
119	TACO F-6	u	246	0,01	2,46
120	TORNILLO COLEPATO 1X8	u	246	0,01	2,46
121	TORNILLO COLEPATO 1/2X8	u	120	0,01	1,20
122	SILICONA	u	20	0,63	12,60
123	SIERRAS	u	8	2,25	18,00
	1.4 Consumibles Canaleta				**9,00**
124	UNION 20X12	u	20	0,45	9,00
	1.5 Consumibles Tubería				**195,43**
125	CAJA EMT 12X12CM	u	60	0,75	45,00
126	TAPA CAJA EMT 12X12CM	u	60	0,27	16,20
127	CONECTOR EMT 3/4"	u	140	0,32	44,80
128	CONECTOR EMT 1"	u	40	0,50	20,00
129	UNION EMT 3/4"	u	74	0,32	23,68
130	UNION EMT 1"	u	24	0,50	12,00
131	ABRAZADERA EMT 3/4"	u	210	0,08	15,75
132	ABRAZADERA EMT 1"	u	60	0,13	7,50
133	ALAMBRE GALVANIZADO Nº, 18	Kg	4	1,13	4,50
134	CODO EMT 3/4"	u	8	0,75	6,00
	2 TOTAL SISTEMA DE ALIMENTACION ELECTRICO				**1.052,97**
	2.1 Sistema de Alimentación Eléctrico				**1.045,67**
201	CABLE TW 12 AWG, MULTIFILAR	m	38	0,22	8.36
202	CABLE TW 14 AWG, MULTIFILAR	m	74	0,19	14,06

203	TOMACORRIENTE TRIPOLAR DOBLE C/PLACA	u	4	3,90	15,60
204	CAJA PVC 10X5X4CM C. ALMENDRA	u	4	1,73	6,90
206	UPS	u	1	750,65	750,65
207	GABINETE BYPASS 30ª	u	1	231,14	231,14
208	CENTRO CARGA 04P BIFASE	u	1	18,96	18,96
	2.2 Consumibles Eléctrico				**7,30**
209	CINTA AISLANTE 20 YD	u	4	0,70	2,80
210	ETIQUETA CABLE C.VERDE	u	8	0,10	0,80
211	MASKING	u	4	0,88	3,50
212	TACO F-6	u	8	0,01	0,10
213	TORNILLO COLEPATO 1X8	u	8	0,01	0,10
	3 MANO DE OBRA Y CONFIGURACION DEL SISTEMA				**1.800**

Del análisis económico realizado se puede concluir que el costo total para implementar el sistema de control de acceso físico en el antiguo edificio de Ingeniería Eléctrica es de **$ 25.670,99**, el mismo que incluye el sistema de alimentación eléctrica y de redundancia de energía.

Se puede implementar el sistema de control físico en el edificio antiguo de la ex facultad de Ingeniería Eléctrica sin implementar el sistema de alimentación eléctrica y de redundancia de energía, asumiendo que en cada una de las localidades donde se colocarán los paneles de control de acceso existen tomacorrientes, con lo cual el costo de la implementación es de **$ 24.618,02.**

Este proyecto de titulación propone que se realice la instalación del sistema de control de acceso físico en el edificio antiguo de la ex facultad de Ingeniería Eléctrica sin considerar el sistema de alimentación eléctrico y de respaldo de energía, se realiza esta consideración ya que en caso de ausencia de energía, las cerraduras electromagnéticas quedan abiertas automáticamente.

Para poder financiar la inversión inicial se propone cobrar 15 $ el primer semestre y los siguientes semestres se cobrará 7 $ a cada uno de los estudiantes de la ex facultad de Ingeniería Eléctrica si éstos no han perdido la tarjeta de identificación, caso contrario se cobrará 15 $, de estos 15 $ se destinara 8 $ para la realización de la tarjeta de identificación con lo cual se tendrá un margen de recuperación de 7 $ por cada tarjeta.

En la ex facultad de Ingeniería Eléctrica en el período Abril/Agosto 2005 se matricularon aproximadamente 2.090 estudiantes, por lo tanto cada semestre se podría obtener $ 14.630, con este dinero se puede financiar la inversión inicial del sistema de control de acceso físico de la ex facultad de Ingeniería Eléctrica en aproximadamente 2 semestres.

3.6.4 ANÁLISIS DE COSTOS DEL SISTEMA DE CONTROL DE ACCESO CENTRO DE CÓMPUTO GENERAL.

ITEM	Descripción	Unidad Medida	Cantidad	Precio Unitario	Total
	COSTO TOTAL DEL PROYECTO				**5.461,80**
	1 Total Sistema de Control de Acceso				**5.198,80**
	1.1 Equipos Control Acceso				**5.062,66**
101	PUERTAS METALICAS BATIENTES 1,50x2, C/CERRADURA DE POMO KWIKSET	u	1	360,00	360,00
102	FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	1	150,00	150,00
103	CONTACTOS MAGNETICOS	u	3	2,80	8,40
104	CONVERTIDORES RS-485 ETHERNET	u	1	299,00	299,00
105	BRAZOS PEQUEÑOS PARA CERRAR PUERTA	u	2	8,75	17,50
106	PC ACCESO N-1000-III	u	1	1.500,44	1.500,0
107	CERRADURA ELECTROMAGNETICA	u	2	172,66	345,32
108	HAND PUNCH	u	1	1.832,44	1.832,44
109	LECTOR DE PROX	u	2	275,00	550,00
	1.2 Elementos Cableado				**95,62**
109	CABLE SPT 2X22 AWG	m	35	0,28	9,63
110	TUBO EMT ¾" X3M	u	15	4,50	67,50
111	CANALETA PVC 20X12X2M LISA	u	4	1,25	5,00
112	INTERRUPTOR SIMPLE C/TAPA	u	2	1,69	3,38
113	CAJA PVC 10X5X4CM C. ALMENDRA	u	2	1,73	3,46
114	CABLE UTP 04 PAR C5E	m	35	0,19	6,65
	1.3 Consumibles Cableado				**4,78**
114	AMARRAS PLASTICAS 20CM	u	30	0,03	0,75
115	TACO F-6	u	16	0,01	0,20
116	TORNILLO COLEPATO 1X8	u	16	0,01	0,20
117	TORNILLO COLEPATO 1/2X8	u	10	0,01	0,13
118	SILICONA	u	2	0,63	1,25
119	SIERRAS	u	1	2,25	2,25
	1.4 Consumibles Canaleta				**0,90**
120	UNION 20X12	u	2	0,45	0,90
	1.5 Consumibles Tubería				**25,84**
121	CAJA EMT 12X12CM	u	5	0,93	4,63
122	TAPA CAJA EMT 12X12CM	u	5	0,34	1,69
123	CONECTOR EMT 3/4"	u	20	0,40	8,00
124	UNION EMT 3/4"	u	11	0,40	4,40
125	ABRAZADERA EMT 3/4"	u	30	0,08	2,25
126	ALAMBRE GALVANIZADO Nº, 18	Kg	1	1,13	1,13
127	CODO EMT ¾"	u	5	0,75	3,75
	3 MANO DE OBRA Y CONFIGURACION DEL SISTEMA				**272**

Del análisis económico realizado se puede concluir que el costo total para implementar el sistema de control físico del centro de cómputo general es de **$ 5.461,80**.

No se considera la recuperación de esta inversión, motivo por el cual se propone que la Politécnica asuma los costos de implementación de este sistema de control de acceso físico.

Nota.- Las proformas presentadas anteriormente no incluyen el 12% del impuesto al valor agregado (IVA), además la forma de pago es el 70 % a la aceptación de la oferta y 30% contra entrega.

REFERENCIAS DEL CAPITULO III

[1] LAWRENCE J. Fenelly, Effective Physical Security, Tercera Edición, Elsevier, United States of America, 2004. Páginas 101-115, 125-167, 195-203.

[2] SUDHANSHU kairab, A Practical Guide to Security Assessments, Segunda Edición, Auerbach, United States of America, 2004. Páginas 193-205.

[3] GARCIA M. Lynn, The Design and Evaluation of Physical Protection Systems, primera Edición, Elsevier, United States of America. 2001. Páginas 173-199.

[4] AVILES Fausto, "Folleto, Instalaciones Eléctricas", Quito Ecuador.

[5] HIDALGO Pablo, "Folleto, Sistemas de Cableado Estructurado", Quito Ecuador.

[6] PAEZ V. Jorge, "Diseño de un sistema de apantallamiento y puesta a tierra del nuevo laboratorio de Alta Tensión de la EPN", Quito Ecuador, 1976, páginas 12-54.

4 POLÍTICAS DE SEGURIDAD PARA LA EPN

4.1 INTRODUCCIÓN [6][7]

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de Internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierten en retos para delincuentes informáticos universales conocidos como Crakers, es decir transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país existen pocas instituciones que no se han visto sujetas a los ataques en sus instalaciones, tanto desde el interior como del exterior.

Uno de los principales problemas que se tienen en la EPN es que existen muchos activos dispersos en laboratorios o en oficinas como por ejemplo laptops que no se encuentran en inventarios. Las cosas entran y salen de la EPN de una manera muy sencilla sin que exista mayor control.

Los escasos recursos humanos involucrados en seguridad, la poca concientización, la falta de visión y las limitantes económicas han retrasado muchos de los esfuerzos que se han realizado individualmente por parte de ciertos grupos para disminuir este riesgo.

Del análisis realizado en cuanto a los activos que existen en cada uno de los laboratorios de la ex facultad de Ingeniería Eléctrica, el centro de cómputo general y en sí en toda la Politécnica, se demanda que estos recursos estén disponibles todo el tiempo. Del estudio realizado en este proyecto de titulación se ha visto la necesidad de implementar un sistema de control de acceso como se ha descrito

en el capítulo 3. Es necesario recalcar que un sistema de seguridad o cualquier sistema, no sirve de nada si las personas que interactúan con el mismo no entienden los beneficios del sistema a implementarse y la necesidad que se tiene de que las personas ayuden a mejorarlo cada día más.

La seguridad de las instituciones en muchos países se ha convertido en cuestión de prioridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe plasmar mecanismos confiables para proteger los activos de la institución.

Aunque no hay un sistema de control de acceso físico que sea impenetrable en un 100 por ciento, un sistema de control de acceso como se ha presentado en el capítulo 3, respaldado por políticas integrales de seguridad de control de acceso, puede reducir de manera importante el riesgo de ataques al incrementar la dificultad que necesita vencer el atacante para penetrar en cada una de las ubicaciones.

4.2 LOS RIESGOS DE LA GUERRA INFORMÁTICA

La guerra Informática consiste en identificar la información y las funciones de la información del adversario con el fin de degradar la voluntad o capacidad de lucha del oponente. Si la misión final consiste en ganar una ventaja económica, política, militar o personal, los intrusos constantemente están buscando la manera de comprometer y atacar la información que poseen otras organizaciones.

Nuestra universidad no se encuentra ausente de este tipo de ataques. La protección constante y diligente de la información y la infraestructura es necesaria en todo momento.

4.3 CONSTRUCCIÓN DE CAPAS DE SEGURIDAD

Las mejores prácticas de la industria se centran en el concepto de seguridad total.

La seguridad en capas es una práctica que combina diferentes componentes de seguridad, como el sistema de control de acceso, circuitos cerrados de televisión, sistemas de detección de incendios y herramientas de evaluación de vulnerabilidades para crear una completa barrera defensiva mucho más fuerte que sus partes individuales por separado.

La seguridad en capas aumenta de manera extraordinaria el costo y dificultad de penetración de un atacante, por lo cual se disminuye la posibilidad que los atacantes se tomen el trabajo de asediar a una institución.

4.3.1 COMPROMISO CON LA SEGURIDAD

Mantener la protección de la empresa o institución exige un compromiso firme, puesto que las amenazas, las vulnerabilidades y los requerimientos de la empresa cambian, **las políticas de seguridad y los mecanismos adoptados deben ser reevaluados periódica y habitualmente para brindar protección total.**

Además, la seguridad informática debe cumplir principalmente las siguientes propiedades:

Privacidad.- La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la privacidad es la divulgación de información confidencial.

Integridad.- La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la integridad es la modificación no autorizada de los datos en la base de datos del SAE de la EPN, el sistema de control de acceso físico no protege toda la información pero es un primer componente del sistema de protección.

Disponibilidad.- La información debe estar en el momento que el usuario requiera de ella.

4.3.2 POLÍTICAS DE SEGURIDAD [1][2][3][4][5][6][7]

Las políticas, estándares y procedimientos para la seguridad de la Información son una serie de múltiples documentos interrelacionados que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones actuales y futuras. Desafortunadamente, las discusiones acerca de las "políticas", "estándares" y "procedimientos" para la seguridad de la información son con frecuencia confusas; están llenas de malos entendidos, información errada y definiciones contradictorias.

Desde la perspectiva de seguridad de la información, estos términos no están claramente definidos en español y no se traducen fácilmente a otros idiomas. Teniendo en cuenta lo anterior, es importante primero definir los términos prácticos para que puedan ser fácilmente entendidos por cualquier persona en cualquier idioma.

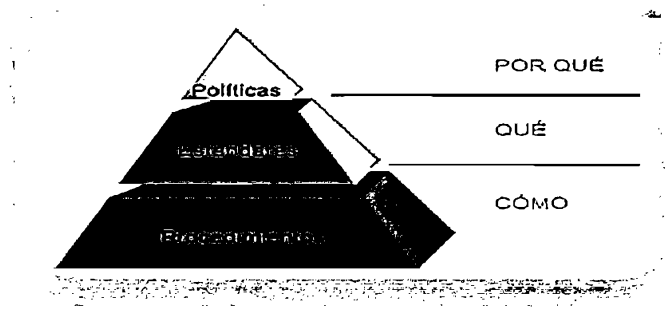


Figura 4.1 Pirámide explicativa sobre las políticas, estándares y procedimientos.

- Una política de seguridad explica con documentación el **por qué** una organización protege su información.
- Los estándares de la organización explican con documentación lo **que** la organización quiere hacer para implementar y administrar la seguridad de su información.
- Los procedimientos explican con documentación exactamente **cómo** la organización obtendrá los requerimientos ordenados por estándares y políticas de nivel superior.

4.3.3 DOCUMENTO DE LA POLÍTICA DE SEGURIDAD

Es importante anotar que la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentación el enfoque del medio ambiente, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

4.3.4 ESTÁNDARES

Los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y lógicos (técnicos) que están diseñados para proteger la información. Uno de los documentos de estándares define el contenido y presentación de toda la documentación de seguridad de la compañía de manera que muchas organizaciones contarán con docenas de documentos de los estándares para la seguridad de la información.

4.3.5 PROCEDIMIENTOS

Los procedimientos de seguridad de la información establecen de manera detallada las operaciones que necesitan realizarse para satisfacer los requerimientos especificados en el estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información.

Los beneficios que se presentan en la aplicación de estándares y procedimientos son:

- Control de actividades de procesamiento.
- Control de calidad de procesamiento.
- Control de tiempo, costos y recursos.
- Mejoras de la moral del personal.

4.3.5.1 Tipos de estándares y procedimientos

Los estándares y procedimientos han sido definidos como dos tipos de estándares los cuales son:

- **Estándares de métodos**. Se utilizan como guías, los estándares son utilizados para establecer prácticas uniformes y técnicas comunes.

- **Estándares de desempeño.** Son utilizadas como normas, los estándares son utilizados para medir el desempeño de la función del procesamiento de datos.

4.3.5.2 Otra Clasificación

- **Estándares de compra:** Se establecerán todas las reglas para la realización de todas las compras dentro de un centro de cómputo.

- **Estándares de productividad:** Se establecerán procedimientos para medir y obtener la mayor productividad posible.

- **Estándares de comunicación:** Se establecerán formas para que los directivos puedan visualizar el potencial real del centro de cómputo y no pidan imposibles.

- **Estándares de trabajo:** Se establecerán las reglas para el trabajo dentro del centro de cómputo.

- **Estándares de programación:** Menciona los estándares a seguir en la programación y la operación de sistemas, para aumentar la seguridad de éstos.

4.3.6 DIVISIÓN DE LAS ÁREAS DE ADMINISTRACIÓN DE LA SEGURIDAD

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes grupos. Estos son:

- Autenticación: se refiere a establecer las entidades que puedan tener acceso al universo de recursos que cierto ambiente puede ofrecer.

- Autorización: es el hecho de que las entidades autorizadas a tener acceso a los recursos, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

- Auditoría: se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este rubro el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

4.4 POLÍTICAS DE SEGURIDAD FRENTE AL CONTROL DE ACCESO FÍSICO PARA LA EPN. [4][5][6][8][9]

4.4.1 INTRODUCCIÓN

Como se ha mencionado anteriormente, las políticas de seguridad son una parte fundamental dentro de cualquier sistema de seguridad, a continuación se presentan las posibles políticas de seguridad física que se podrían utilizar en la EPN para cumplir con el objetivo propuesto en este proyecto de Titulación el mismo que es el de proponer un sistema de control de acceso físico para la EPN, además se definirán algunos procedimientos que se consideran fundamentales. Cabe recalcar que las políticas de seguridad propuestas a continuación deben seguir un proceso de afinamiento continuo. La información que se presenta a continuación ha sido adecuada a la información que se puede observar en las

encuestas realizadas a ciertos jefes de departamento y profesores expertos en seguridad, dichas encuestas se pueden observar en el Anexo número 1.

Antes de entrar en detalle sobre las políticas de seguridad, es necesario definir quién estará a cargo de definir las políticas de seguridad, para lo cual se procede a explicar cómo funciona en la actualidad el control de seguridad física, esto se muestra en la figura 4.2.

Como máximo organismo de la estructura presentada se tiene al Consejo Politécnico, debajo de este organismo se encuentra el rectorado, el centro de seguridad física se encuentra debajo del departamento de servicios generales, dicho centro es dirigido por el jefe del departamento de servicios generales, por ejemplo si un estudiante necesita realizar algún experimento el día domingo, este debe solicitar un salvoconducto al Director de Administración el mismo que analiza la situación, si observa que se debe proceder con el salvoconducto, envía la solicitud al departamento de servicios generales quien se encarga de dar cumplimiento con los permisos mediante la ayuda del jefe de departamento de servicios generales.

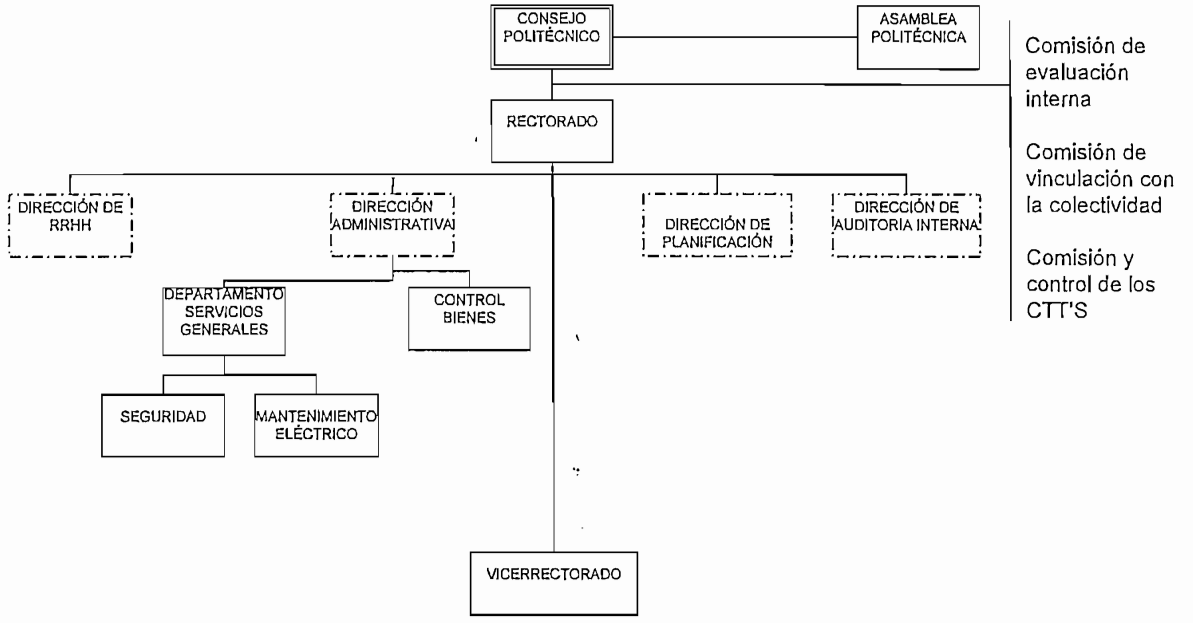


Figura 4.2 Organigrama estructural general de la EPN.

Este proyecto de titulación propone la creación de un comité de seguridad, el mismo que será únicamente consultivo, es decir que se encargará de definir las políticas de seguridad y modificar las mismas. Se propone que este comité de seguridad esté conformado por el director de recursos humanos o un delegado del mismo, el director de la dirección administrativa o delegado del mismo, dos docentes expertos en seguridad, los mismos que serán elegidos por Consejo Politécnico, y el encargado de seguridad.

A continuación se presenta la estructura propuesta, la misma que mantendrá la estructura actual de la EPN, el comité de seguridad se encontrará debajo de la dirección administrativa. La figura 4.3 muestra el esquema propuesto.

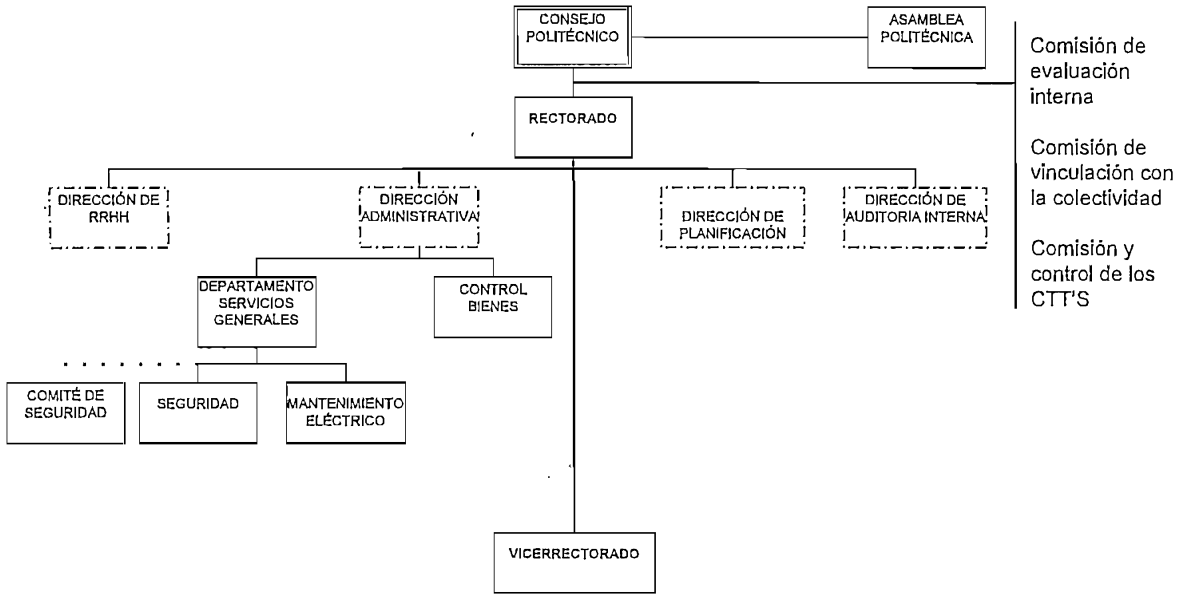


Figura 4.3 Organigrama propuesto para implementar las políticas de seguridad.

En la figura 4.3 se presenta el organigrama donde se presenta la ubicación del comité de seguridad el mismo que se encargará de definir las políticas de seguridad, para implementar dichas políticas, se propone mantener la actual organización de seguridad.

A continuación se presenta una propuesta de las políticas de seguridad frente al control de acceso y algunos procedimientos que se han visto necesarios de definir.

4.4.2 POLÍTICA DE LA IDENTIFICACIÓN Y CONTROL

Objetivos:

Identificar a cada una de las personas que ingresan a las áreas restringidas de la Politécnica para poder tener registros y control de las personas. Controlar el ingreso o salida de los objetos de cada una de las ubicaciones para poder disminuir el número de robos que han existido en años anteriores.

1. Todas las personas que estudian o trabajan en la EPN deberán portar la respectiva tarjeta de identificación para poder ingresar en áreas restringidas dentro de la Politécnica.

2. Todas las personas ajenas a la institución deberán portar una tarjeta de identificación de visitante para poder ingresar en áreas restringidas dentro de la Politécnica.

3. Todo material o equipo que trate de ingresar o salir de cada uno de los laboratorios deberá ser registrado por parte del encargado de cada uno de los laboratorios.

4. Cada uno de los laboratorios deberá quedar con seguro cuando no se encuentre ninguna persona en dicha localidad.

5. Estudiantes, trabajadores, profesores y visitantes, deberán acogerse a los horarios de ingreso y salida de la institución.

4.4.3 POLÍTICA SOBRE EL EQUIPO DE LABORATORIO.

Objetivo:

Llevar registros de todos los equipos que se encuentran actualmente en cada una de las ubicaciones para tener inventarios completos de los mismos.

1. Los responsables de cada uno de los laboratorios y del centro de cómputo general deberán en conjunción con el departamento de control de bienes dar cabal cumplimiento con notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación de todos los equipos que se encuentran en cada una de los laboratorios.

4.4.4 POLÍTICA SOBRE EL MANTENIMIENTO Y ACTUALIZACIÓN DE LOS EQUIPOS UTILIZADOS PARA REALIZAR EL CONTROL DE ACCESO.

Objetivo:

Mantener e incrementar el nivel de funcionalidad de cada uno de los equipos involucrados en el control de acceso físico.

1. Se debe verificar el correcto funcionamiento de cada uno de los equipos utilizados para realizar el control de acceso, que son propiedad de la EPN, procurando conservar e incrementar la calidad del servicio que prestan, mediante la mejora sustantiva de su desempeño.

4.4.5 PLANES DE CONTINGENCIA

Objetivo:

Proporcionar una convicción razonable de que la institución se podrá recuperar ante un desastre.

1. Cada uno de los departamentos deberá emitir los planes de contingencia anuales que correspondan a las actividades críticas que realicen.

4.4.6 SANCIONES.

Objetivo:

Tratar que las personas cumplan con las políticas definidas.

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por el Comité de Seguridad y aprobado por Consejo Politécnico.

2. Las sanciones pueden ser desde una llamada de atención al usuario, hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

3. Corresponderá a Consejo Politécnico hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de seguridad de la institución.

4. Todas las acciones en las que se comprometa la seguridad de la EPN y que no estén previstas en esta política, deberán ser revisadas por el Comité de Seguridad para dictar una resolución sujetándose al estado de derecho.

Notas

1. Estas políticas de seguridad deberán seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura, desarrollo de nuevos servicios, entre otros.

2. El documento que contiene la política de seguridad deber ser difundido a todo el personal docente, estudiantes y trabajadores.

3. En concordancia con la política de la institución y en las áreas restringidas se llevará un registro permanente del tráfico de personal, sin excepción.

4.5 PROCEDIMIENTOS DE SEGURIDAD FRENTE AL CONTROL DE ACCESO PARA LA EPN

4.5.1 PROCEDIMIENTO DE LA IDENTIFICACIÓN Y CONTROL

1. Si un estudiante o un trabajador se encuentra en un área restringida y es solicitado de identificarse, éste debe presentar su tarjeta de identificación caso contrario será obligado a salir del área restringida.

2. Las personas ajenas a la institución que deseen ingresar a alguna área crítica, deberán registrarse con el encargado de esa área o el personal de seguridad, para que éste les provea de una tarjeta de identificación de visitante, cabe recalcar que las personas que visiten la Universidad deberán estar sujetas a las políticas de seguridad de la Politécnica.

3. El Comité de Seguridad estará encargado de definir las áreas a las cuales cada una de las personas que estudian o trabajan en la EPN podrán acceder. Para implementar esta normativa el encargado de seguridad deberá tener acceso a una base de datos con los nombres de las personas y las áreas a las cuales podrán acceder. En caso de que un estudiante o trabajador desee ingresar a otra localidad será responsabilidad del encargado de cada uno de los laboratorios o del centro de cómputo general el autorizar su ingreso.

4. El Comité de Seguridad estará encargado de definir las áreas a las cuales podrán acceder los visitantes de la Universidad.

5. Cada uno de los encargados de los laboratorios deberá asegurar las localidades, cuando éstos dejen las instalaciones.

6. El departamento de control de bienes de la Escuela Politécnica Nacional deberá tener un registro de todos los equipos pertenecientes a la institución que en la actualidad se encuentran en cada uno de los laboratorios. De los

equipos que no pertenecen a la Politécnica lo debe hacer el encargado de cada uno de los laboratorios.

7. Bajo condiciones de emergencia o de situaciones de urgencia, el acceso a las áreas críticas estará sujeto a las disposiciones que especifiquen las autoridades superiores de la institución.

8. Las áreas de cada uno de los departamentos donde se encuentre equipo cuyo propósito reúna características imprescindibles y de misión crítica, deberán sujetarse también a las normas que establezca el comité de seguridad.

9. El comité de seguridad deberá normar los mecanismos utilizados para sacar los respaldos de la información de seguridad.

4.5.2 PROCEDIMIENTO SOBRE EL MANTENIMIENTO Y ACTUALIZACIÓN DE LOS EQUIPOS UTILIZADOS PARA REALIZAR EL CONTROL DE ACCESO.

1. El departamento de servicios generales deberá definir las normas y procedimientos respectivos para la realización del mantenimiento preventivo y correctivo de los equipos, el mismo que deberá ser efectuado al menos una vez al año.

2. El personal técnico de apoyo interno de los departamentos académicos se apegará a los requerimientos establecidos en las normas y procedimientos que el departamento de servicios generales emita.

4.5.3 PROCEDIMIENTOS DE LA AUDITORÍA DEL SISTEMA DE CONTROL DE ACCESO.

1. El departamento de auditoría interna deberá designar un grupo para realizar la auditoría al sistema de seguridad al menos una vez al año.

4.5.4 PROCEDIMIENTO DE LA DIFUSIÓN DE LAS POLÍTICAS DE SEGURIDAD

1. Los encargados de seguridad deberán difundir periódicamente las políticas de seguridad que norman a la institución mediante volantes, conferencias, la página web de la institución, etc. Además los encargados de seguridad estarán en la obligación de despejar las dudas de las personas que lo requieran.

4.5.5 PROCEDIMIENTO DE LOS RECONOCIMIENTOS

1. El Comité de Seguridad establecerá los reconocimientos necesarios a las personas que alimenten con nuevas ideas para mejorar las políticas de seguridad que normarán a la Escuela Politécnica Nacional.

REFERENCIAS DEL CAPITULO IV

[1] LAWRENCE J. Fenelly, Effective Physical Security, Tercera Edición, Elsevier, United States of America, 2004. Páginas 9-13, 101-115.

[2] SUDHANSHU kairab, A Practical Guide to Security Assessments, Segunda Edición, Auerbach, United States of America, 2004. Páginas 45-65.

[3] GARCIA M. Lynn, The Design and Evaluation of Physical Protection Systems, primera Edición, Elsevier, United States of America. 2001. Páginas 173-199.

[4] GALLEGOS Frederick, SENFT Sandra, MANSON Daniel, GONZALES Carol, Information Technology Control and audit, segunda edición, Auerbach, United States of America, 2004, Páginas 29-57.

[5] Headquarters, Department of the Army, Physical Security, United States of America, ISBN 1-931828-59-8, Physical Security Plan.

[6] AVILA Nelson., "Folleto, Seguridad en redes", Quito Ecuador. Capítulo 10.

[7] SIMANTEC
http://www.symantec.com/region/mx/enterprisesecurity/content/security_articles.ht

[8] GABRIELSON Bruce, Information Security Program Development, Center for Information Security Technology Columbia, Maryland
www.InformationSecurityProgram.http

[9] WALT Charl, Introduction to Security Policies a sample Policy
http://www.securityfocus.com/

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Los accesos no autorizados de personas y objetos traen consigo consecuencias muy graves para la institución, por ejemplo ingresan personas de dudosa procedencia que pueden realizar robos, traficar droga, etc.

- Antes de realizar cualquier diseño de seguridad física se deben tomar en cuenta las amenazas de las que nos queremos proteger, medir la probabilidad de ocurrencia de las mismas, y entonces definir la forma de cumplir los objetivos del proyecto.

- Un adecuado análisis de riesgos nos permite definir claramente los problemas de los que nos queremos proteger y los objetivos para alcanzar dicho propósito.

- En el análisis costo beneficio, muchas veces no tomamos en cuenta otro tipo de activos como la información, la misma que en caso de perderse o alterarse sería muy difícil o casi imposible de recuperar.

- Un sistema de control de acceso debe tomar en cuenta tanto las características físicas, técnicas como el reconocimiento de las personas, ya que de nada serviría un sistema de control de acceso implementado con la última tecnología si las personas que interactúan con el mismo no comprenden la necesidad de su utilización y lo dañan o lo burlan.

- Los sistemas de control de acceso tratan de autenticar a las personas que intentan acceder a sitios protegidos, permitiendo el ingreso de personas autorizadas que pueden utilizar mecanismos tan simples como una contraseña o tan complejos como un sistema biométrico para autenticar a las personas.

- Existen muchos mecanismos para autenticar a las personas uno de estos métodos y el más aceptado es el de las tarjetas de proximidad, el cual incorpora hardware de alta seguridad tanto para almacenar datos, cómo para realizar funciones de encripción.

- Las tarjetas de proximidad, son utilizadas para disminuir los tiempos necesarios para realizar la autenticación, pues una persona que desea autenticarse no necesita sacar la tarjeta de su cartera, el lector la detectará automáticamente cuando ésta se encuentre a una determinada distancia del lector de la misma, esto es muy necesario para definir la solución de acceso vehicular.

- Las tarjetas de banda magnética son un medio económico para realizar la autenticación de las personas, pero éstas tienen una baja capacidad de almacenamiento de información, motivo por el cual han sido remplazadas por las tarjetas inteligentes de proximidad las mismas que brindan una mayor seguridad.

- Los sistemas biométricos autentican a las personas tomando en cuenta alguna característica física de las personas, existen muchos sistemas de autenticación biométricos pero uno de los más aceptados es el sistema de autenticación biométrico basado en la geometría de la mano.

- Antes de seleccionar el tipo de tecnología a utilizar se debe tomar en cuenta las características técnicas del producto, el precio y además se debe verificar si la tecnología es aceptada por las personas que interactúan con la misma.

- Mediante la implementación del sistema de control de acceso vehicular la Politécnica podrá evitar en un gran porcentaje el número de fraudes que en la actualidad se tiene con la utilización del sticker cómo método de autenticación vehicular.

- La efectividad de los guardias de estacionamientos puede reforzarse enormemente si en la universidad se instalan detectores electrónicos con alarmas u otros indicadores de advertencia que terminan en la estación del guardia.

- No es suficiente con implementar un sistema de control de acceso físico, si los laboratorios de la Politécnica no cumplen primero con las normas físicas necesarias para que funcionen como tales, por ejemplo hacen falta sistemas de detección contra incendios.

- Los mecanismos de redundancia de energía basados en UPS no son indispensables para que funcione adecuadamente el sistema de control de acceso planteado como solución ya que éstos permiten que el sistema funcione durante 26 minutos aproximadamente a plena carga, por lo cual esta solución no seria útil a largo plazo, ésta serviría solamente para tomar decisiones inmediatas.

- El mecanismo inalámbrico de redundancia de transmisión de datos puede trabajar adecuadamente en grandes distancias, además estos mecanismos permiten tener acceso a lugares difíciles con costos relativamente bajos y a grandes velocidades, ofreciendo mecanismos de encripción para que la información viaje de una manera segura a través del interfaz de aire.

- El mecanismo de redundancia de transmisión de datos propuesto, no puede funcionar automáticamente cuando el enlace principal sufra algún daño debido a las limitaciones de hardware de los switches existentes en cada uno de los edificios principales, los mismos que no presentan opciones de balanceo de carga u otro mecanismo para actuar de una manera inmediata. Es decir si el enlace principal cae se deberá conectar el mecanismo de redundancia de transmisión de datos manualmente. Se toma ésta decisión para evitar lazos de transmisión de datos entre los enlaces principales y el enlace de respaldo.

- Los mecanismos de comunicaciones son parte fundamental de los sistemas de control de acceso, los mismos que pueden ayudar a detectar y neutralizar una amenaza de una manera más óptima.

- Las normas de administración deben proveer un esquema de administración uniforme y de fácil entendimiento para las personas que están encargadas de la administración de los sistemas, para cumplir con dicho objetivo se utilizan mecanismos como: planos, etiquetas, registros, reportes, etc.

- Se puede afirmar que la Escuela Politécnica Nacional reclama que los mecanismos administrativos de la organización estén claramente establecidos, a fin de tener seguridad para cada uno de los activos, y poder seguir estándares y procedimientos, y cuando se de el caso poder salir avante recuperando todo lo posible en caso de un desastre.

- Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, lo que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

- La seguridad de las instituciones en muchos países se ha convertido en cuestión de prioridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y debe plasmar mecanismos confiables para proteger los activos de la institución.

- Las políticas y procedimientos son importantes en el establecimiento de un programa eficaz de seguridad física, deben reflejar las políticas generales de la organización como protección de la información y recursos. Deben cubrir el uso de recursos y deben marcar la información sensible, movimiento de recursos, introducción de equipo y medios de comunicación, disposición de la información sensible ante una pérdida. La puesta en

práctica de estas políticas es esencial para la efectividad de los sistemas de seguridad informática.

- Las políticas de seguridad, estándares y procedimientos deben provenir desde las autoridades superiores, para que las mismas sean aplicables en cada uno de los estamentos de la Politécnica.

- Se deben difundir periódicamente las políticas de seguridad que norman a la institución, además los encargados de seguridad deben despejar las dudas de las personas que lo requieran.

- Para poder mejorar continuamente las políticas de seguridad es necesario la participación continua de toda la comunidad politécnica. Para cumplir con dicho objetivo es recomendable premiar a cada una de las personas que alimenten con nuevas ideas para mejorar las políticas de seguridad que normarán a la Escuela Politécnica Nacional.

- Como se ha mencionado a lo largo de este proyecto de titulación no existe un mecanismo de seguridad 100% seguro, un problema que se puede dar con la utilización de la solución propuesta para controlar el acceso vehicular, es que un auto puede ingresar mientras otro está saliendo, para solucionar este problema se puede usar dos lectoras, una para entrada y otra para salida.

- El conocimiento de seguridad y el entrenamiento es una medida preventiva que ayuda a que los usuarios entiendan los beneficios de las prácticas de seguridad. Si los empleados no entienden la necesidad por los controles de seguridad, ellos pueden burlar los controles en el futuro y por eso pueden debilitar el programa de seguridad o pueden hacerlo inútil.

- Los entrenamientos técnicos pueden ayudar a los usuarios a prevenir el problema de seguridad más común "errores y omisiones".

- Para facilitar la administración del sistema de control de acceso se ha decidido realizar un sistema de control de acceso en profundidad y además centralizado, es decir cada uno de los edificios conformará una red de control de acceso local, la misma que se interconectará con un punto central en el centro de cómputo general, formando una red de control de acceso de campus.

- Un aspecto fundamental que se debe tomar en cuenta en el diseño e implementación del sistema de control de acceso es que todos los cables deben estar protegidos, un mecanismo a utilizarse para solucionar éste problema es utilizar tubería conduit EMT metálica.

- El presente proyecto de titulación puede ser expandido para controlar el horario de entrada salida de cada una de las personas que trabajan en la Politécnica.

- Mediante la implementación del sistema de control de acceso planteado, tanto en el acceso vehicular como en el acceso a áreas críticas, se puede permitir a los profesores ingresar a la Universidad en días no laborables, evitándose todo el papeleo que en la actualidad se tiene que hacer para obtener un salvoconducto, cabe recalcar que el sistema permite tener registros de las personas que ingresan en las diferentes ubicaciones.

- Existen otro tipo de lectoras de proximidad las mismas que pueden detectar una tarjeta a mayores distancias, este tipo de lectoras se puede colocar en los accesos vehiculares.

- Las tarjetas hibridas propuestas, permiten controlar el acceso de las personas hacia cada una de las localidades, además pueden almacenar otro tipo de información que puede ser utilizada en otras aplicaciones, cabe recalcar que se necesita otra lectora para poder realizar otras aplicaciones diferentes a las del control de acceso.

5.2 RECOMENDACIONES

- La EPN es una universidad pública motivo por el cual muchos de los estudios que se han realizado para solucionar los problemas que actualmente agobian a la misma, se han quedado en papel, es por esto que se recomienda implementar la primera fase de este proyecto de titulación, el cual se trata de la implementación del sistema de control de acceso vehicular, luego de lo cual se pueden ir implementando los sistemas de control de acceso físico de cada uno de los edificios, para financiar este proyecto se recomienda realizar el cobro de una cuota a cada una de las personas que deseen ocupar el campus politécnico para dejar sus automóviles.

- En este proyecto de titulación se propone la utilización del sistema de control de acceso del fabricante Northern Computers, sin embargo se podría mejorar la propuesta de sistemas de control de acceso basados en PLC's desarrollando aún más el software de administración y realizando pruebas para hacer emular un lector biométrico como un lector de tarjetas, pudiendo llegar a ser esta propuesta mejor que la opción de Northern Computers en costo y en calidad.

- En los ingresos a áreas críticas se debe tener letreros grandes de identificación para que las personas sepan que esta área es de acceso restringido.

- En caso de ausencia de energía eléctrica en el sistema de control de acceso del edificio antiguo de Ingeniería Eléctrica, se recomienda alimentar el sistema de control de acceso con el generador que actualmente se dispone en el edificio.

- Se debe colocar los tipos apropiados de extintores de incendios los mismos que deben ser de un fácil acceso en las áreas críticas como el centro de cómputo general.

- Se debe capacitar a los empleados en el uso apropiado de extintores de incendios y en los procedimientos que deben seguir en caso de un incendio, los mecanismos de señalización deben ser adecuados para que en casos de emergencia las personas puedan localizar fácilmente el extintor.

- Se recomienda utilizar en cada una de las áreas críticas extintores de incendios que inundan el área con INERGEN que normalmente no causa daños al equipo y es menos peligroso para las personas que el dióxido del carbono.

- Se recomienda utilizar mecanismos adecuados de verificación de alarmas como los circuitos cerrados de televisión.

- Como medida preventiva se recomienda utilizar en el centro de cómputo general y en áreas críticas mecanismos que mantengan la temperatura entre 20 a 23 °C la humedad promedio entre 45 a 55%.

- El principal problema que se tiene en la parte eléctrica en toda la Politécnica es que no existen sistemas adecuados de puesta a tierra, motivo por lo cual se debe realizar implementaciones de sistemas de puesta a tierra adecuados en cada uno de los edificios, mediante un estudio adecuado de la resistividad del suelo, de esta manera se garantizara que en todo el edificio no existan variaciones de potencial respecto a tierra.

- Otro aspecto de suma importancia que se debe tomar en cuenta en los mecanismos de seguridad son las auditorias que se deben realizar continuamente al sistema de còntrol de acceso y a los encargados de administrar el mismo.

- Se deben realizar auditorias continuas del sistema para poder mejorar continuamente el sistema de control de acceso físico.

- Los informes de violación frecuentemente y regularmente deben ser examinados por funcionarios de seguridad y se deben identificar los accesos desautorizados exitosos o infructuosos.

- Se debe separar regularmente las asignaciones de trabajo para asegurar que se mantiene una separación apropiada de deberes, los trabajos críticos o sensibles deben ser rotados periódicamente entre personal calificado con lo cual se impide a un individuo obtener el control entero de un proceso.

- La Politécnica debe definir planes de recuperación ante un desastre, este plan debe ser un documento que contenga procedimientos como respuesta ante una emergencia. El objetivo primario de este plan, usado junto con los planes de contingencia, es proporcionar una convicción razonable para que la institución pueda recuperarse de los desastres, continúe operando sus aplicaciones críticas aunque en un modo degradado y las devuelva a un modo normal de funcionamiento dentro de un tiempo razonable.

- El documento que contiene la política de seguridad deber ser difundido a toda la comunidad politécnica.

- Los respaldos de la información deben tener el mismo nivel de protección que los archivos originales; es insensato mantener una seguridad firme para los datos en el sistema, pero una floja seguridad para los mismos datos en una situación de respaldo.

- Las Políticas de seguridad no deben ser estáticas, es decir éstas deben ser revisadas continuamente, recordemos que la seguridad física es responsabilidad de todos, las políticas de seguridad, procedimientos y estándares deberían ser dictadas por empresas especializadas, dichas empresas deberían decir a las empresas instaladoras que se debe realizar.

- Se debe identificar claramente cada uno de las ubicaciones que son de acceso restringido, para que las personas sepan cuáles son los lugares restringidos y tengan precaución de ingresar en los mismos.

- En cada una de las entradas principales se deben colocar letreros de identificación que indiquen que éste es un punto de control de acceso, para que las personas tomen precauciones.

- Los guardias y encargados de seguridad deberán contar con mecanismos adecuados de sistemas de comunicaciones (radios de comunicación), para que en caso de que ocurra alguna emergencia, éstos puedan disminuir los tiempos para controlar dicha emergencia.

- Se recomienda tener los planos arquitectónicos: eléctricos, de datos y de seguridad de cada uno de los edificios a escala y en medio electrónico y con una nomenclatura adecuada para poder identificar claramente cada uno de los elementos existentes y poder asegurarlos.

- Se debería rediseñar el tránsito vehicular dentro de la EPN con el objetivo de disminuir el número de accesos vehiculares que en la actualidad se tienen en el Campus Politénico.

- Se recomienda mantener un registro de todos los equipos existentes en la universidad, además se debería tener un seguro de todos los equipos importantes.
- Se deben realizar campañas de concientización y de identidad con la Politécnica.

REFERENCIAS BIBLIOGRÁFICAS

- AVILA Nelson., "Folleto, Seguridad en redes", Quito Ecuador.
- AVILES Fausto, "Folleto, Instalaciones Eléctricas", Quito Ecuador.
- GALLEGOS Frederick, SENFT Sandra, MANSON Daniel, GONZALES Carol, Information Technology Control and audit, segunda edición, Auerbach, United States of America, 2004.
- GARCIA M. Lynn, The Design and Evaluation of Physical Protection Systems, primera Edición, Elsevier, United States of America. 2001.
- Headquarters, Department of the Army, Physical Security, United States of America, ISBN 1-931828-59-8, Physical-Security Plan.
- HIDALGO Pablo, "Folleto, Sistemas de Cableado Estructurado", Quito Ecuador.
- Information Security Management Handbook, Auerbach, United States of America, 2003.
- LAWRENCE J. Fenelly, Effective Physical Security, Tercera Edición, Elsevier, United States of America, 2004.
- PAEZ V. Jorge, "Diseño de un sistema de apantallamiento y puesta a tierra del nuevo laboratorio de Alto Tensión de la EPN", Quito Ecuador. 1976.
- STALLINGS William, Comunicaciones y Redes de Computadores, Sexta Edición, Madrid España, 2000.
- SUDHANSHU kairab, A Practical Guide to Security Assessments, Segunda Edición, Auerbach, United States of America, 2004.
- VILLALÓN Antonio, Seguridad en Unix y Redes, Versión 2.1, Valencia España.

ARTICULOS Y MANUALES

- ALMEIDA Rosario, LUCERNA Pàblo, Reconocimiento del iris.
- BECERRA Nestor, VILLAR Miguel, Verificación de identidad de individuos mediante la voz.
- GARCÍA ORTEGA, Sistema de reconocimiento de huellas dactilares para el control de acceso a recintos, México, 2001.
- LIONEL Martin, Person identification technique using human iris recognition, Francia. 2001.
- RODRÍGUEZ Fernando, SUAREZ francisco, Identificación dactilar basada en filtros Galvor.

DIRECCIONES ELECTRÓNICAS

- AWID
  http://www.awid.com
- EXEC SISTEMAS
  http://www.execsistemas.com
- FIRMESA
  http://www.firmesa.com
- GABRIELSON Bruce, Information Security Program Development, Center for Information Security Technology Columbia, Maryland
  www.InformationSecurityProgram.http
- GUTHERY Scott, JURGENSEN Tim, Smart card developer's kit. Macmillan, United States of America. 1998.
  http://es.tldp.org/manuales-lucas/doc-unixsec/unixsec-html/node1.html.
- Handbook of Information Security Management. 2000
  http://secinf.net/info/misc/handbook/.
- HID
  http://www.HIDCorp.com
- IR Recognition Systems.
  http://hanreader.com

- LÓPEZ M. Héctor, Tecnología de Smart card, 1998.
  http://www.dcc.uchile.cl/~rbaeza/cursos/proyarq/hlopez/node1.html

- TERABEAM
  http://www.terabeam.com

- SIEMENS.
  http://www.siemens.com/s7-200

- Sistemas de Control de Acceso, kerysystems.
  http://www.kerisys.com

- Sistemas de Control de Acceso, Northern Computers.
  http://www.northern-computers.co.uk.

- SIMANTEC
  http://www.symantec.com/region/mx/enterprisesecurity/content/security_articles.ht

- Smart cards.
  http://www.fortunecity.com/westwood/calvin/275/cards/iso7816.zip

- Tarjetas magnéticas
  http.//www.fortunecity.com/westwood/calvin/275/cards/iso7811.zip

- Tecnología de tarjetas.
  http://www.geocities.com/gcataneo/tecnologia.htm

- UNANDER Joseph, Image reconstruction of the iris spectrally
  http://www.cis.rit.edu/research/thesis/bs/2000/unander/tableofcontents.html.

- WALT Charl, Introduction to Security Policies a sample Policy
  http://www.securityfocus.com/

- 3Com
  http://www.3com.com

GLOSARIO

A

Activo — Bienes de una persona o una empresa.

Administración — Proceso social orientado al logro de un fin determinado, mediante la planificación, organización, dirección, coordinación y control de los recursos disponibles

Administrador — Un usuario de la red con autoridad para realizar las tareas de alto nivel de cliente servidor. Tiene acceso y control total de todos los recursos de la red. Llamado comúnmente súper usuario.

Ancho de banda — Relación de velocidad para la transmisión de datos medidos en Kbps (kilo bits por segundo) y que representa la capacidad del canal de comunicación para transportar datos.

ANSI — Organización encargada de la documentación de los estándares en Estados Unidos.

API — Pequeños programas desarrollados para apoyar la interacción del sistema principal con las aplicaciones específicas.

Aplicaciones — Programa informático que lleva a cabo una función para ayudar a un usuario a realizar cierta actividad.

Área Crítica. — Es el área física donde se encuentra instalado equipo que requiere de cuidados especiales.

ASCII — Código utilizado para representar los caracteres de escritura en formato binario (7 bits para 128 caracteres o el modo extendido de 8 bits para 256 caracteres).

Asíncrona — Forma de transmisión de datos donde no se necesita señal adicional de reloj. La señal contiene la información de cuándo cambia cada dato.

Auditoria Registro de actividades del sistema que habilita la reconstrucción y examina la sucesión de eventos de una transacción, desde el comienzo hasta la obtención de los resultados finales. El informe de violación presenta eventos significantes, eventos orientados a seguridad que indican que se realizaron transgresiones de la política de seguridad en la auditoria.

Autenticar Comprobar que una persona es quién dice ser.

B

Backbone Parte de una red, que actúa como enlace primario para el tráfico que a menudo es fuente y destino para otras redes.

Backup Respaldo o copia de seguridad de información crítica.

Bases de Datos Es un conjunto de datos interrelacionados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.

bps Bits por segundo. Velocidad de transmisión serial.

Bridge Dispositivo por donde pasan todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

Broadcast Transmisión abierta. Mensajes que se mandan sin destino específico.

C

Cabezas Pequeños sensores electromagnéticos utilizados para generar patrones de excitación (escrituras y lecturas de datos) en los medios magnéticos (discos de almacenamiento).

CABLE UTP Abreviatura de Unshielded Twister-Pair cable, (cable no blindado con par - trenzado). Contiene cuatro pares trenzados de cobre, el gran número de torcimientos minimiza el efecto de interferencia electromagnética.

Cliente Producto o presentación de front end (directamente con el usuario) que interactúa con otros servidores o productos de back end (sin presentación directa con el usuario). El cliente realiza solicitudes y presenta los resultados. No realiza los procesos ni los cálculos, eso se los deja a los programas de back end que son más poderosos pero no tienen la capacidad de comunicarse directamente con el usuario.

Concentrador Equipo que se encarga, en primera instancia, de concentrar las señales. Algunos tienen funciones de repetir y retrasar la señal para evitar colisiones.

Conectividad Estado que permite la transferencia de datos entre dos computadoras.

CPU Unidad de Proceso Central. Director y principal realizador de procesos de la computadora. Circuito microprocesador que realiza los procesos de datos básicos y controla el funcionamiento general de la computadora.

Cracker Experto informático especialista en entrar en sistemas ajenos con fines destructivos y delictivos.

CSMA/CD Sensor de portadora de accesos múltiples con detección de colisiones. Método de transmisión de datos en donde todas las estaciones pueden mandar datos con una señal eléctrica portadora. En caso de que existan transmisiones simultáneas detectan las colisiones. Es la base de la topología Ethernet.

D

DFT Transformada de Fourier Discreta es el nombre dado a la transformada de Fourier cuando se aplica a una señal digital (discreta) en vez de una análoga (continua).

DHCP (Dynamic Host Configuration Protocol) Protocolo de Configuración Dinámica de Máquinas, especifica un método para configurar dinámicamente los parámetros de red necesarios para que un sistema pueda comunicarse efectivamente.

Disponibilidad Cuando la red, el sistema o el hardware y software son confiables y pueden recuperarse rápida y completamente en caso de interrupción.

DLL Librerías de enlace dinámico generalmente no son directamente ejecutables y no reciben mensajes. Una DLL es, en términos generales, un archivo que contiene funciones y en algunas ocasiones recursos que pueden ser utilizados por programas y por otras DLL para ejecutar ciertas tareas.

DSSS Direct-sequence spread-spectrum (DSSS) genera un patrón de bit redundante por cada bit a ser transmitido. Este bit patrón es llamado un chip (o chipping code). La longitud del chip, tiene una probabilidad mayor de que los datos puedan ser recuperados. Si uno o más bits en el chip son "dañados" durante la transmisión, se pueden recuperar los datos originales a través de técnicas estadísticas aplicadas sobre las señales de radio, sin necesidad de retransmisiones.

E

EEPROM Circuito integrado que se puede grabar por medios electrónicos especiales. Guarda información de manera no volátil y se comporta como memoria de lectura.

Emulación Imitación de la forma de comportarse de un equipo.

Encripción Proceso basado en operaciones lógicas binarias para disfrazar un dato y evitar que sea leído por otra fuente distinta al destino.

Enlaces Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.

EOF Señal que se manda para indicar dónde termina un archivo.

EOT Señal que se manda para indicar dónde termina una transmisión.

EPROM Circuito que se puede borrar y grabar de manera especial para que normalmente funcione como memoria de lectura.

Escalabilidad Característica de los equipos que nos permite ir aumentando velocidad y capacidad en: discos, memoria, procesadores y tarjetas periféricas.

Ethernet Estándar de red más popular e implementado. Utiliza CSMA/CD con una velocidad de 10 Mbps.

F

Fibra Óptica Medio físico que puede conducir la transmisión modulada de luz, este medio de transmisión es inmune a la interferencia electromagnética.

Firewall Dispositivo electrónico que se conecta entre dos o más redes para analizar todo el tráfico que pasa por el mismo, este dispositivo es capaz de permitir o denegar el paso del tráfico.

G

Ganancia de una antena La ganancia de una antena se define como la relación entre la densidad de potencia radiada en una dirección y la densidad de potencia que radiaría una antena isotrópica, a igualdad de distancias y potencias entregadas a la antena.

H

Hacker Experto informático especialista en entrar en sistemas ajenos sin permiso, generalmente para mostrar la baja seguridad de los mismos o simplemente para demostrar que es capaz de

hacerlo.

Hardware Referente a dispositivos reales, físicos. Todos los componentes electrónicos, magnéticos y mecánicos de las computadoras.

Hexadecimal Sistema numérico con base en 16, comúnmente utilizado por su estructura fácil de transformarse al binario.

I

IEEE Agrupación de ingenieros eléctricos y electrónicos de todo el mundo que, entre otras funciones, documenta desarrollos tecnológicos.

Infraestructura Conjunto de elementos equipos o servicios considerados necesarios para la creación y funcionamiento de una arquitectura de red.

Interfaz Circuitos físicos (hardware) o lógicos (software) que manejan, traducen y acoplan la información de forma tal que sea entendible para dos sistemas diferentes.

Inversión Gasto en bienes de equipo o capital, o en activos financieros, con el objeto de obtener una rentabilidad.

IP Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo.

ISO Organización que especifica estándares de calidad internacionales.

K

Kbps Abreviatura de Kilobits por segundo. Unidad de medida de capacidad de transmisión de una línea de comunicaciones.

L

LAN Abreviatura de Local Area Network (Red de área local). Red de datos de alta velocidad y bajo nivel de error que cubre una pequeña área geográfica.

Login — Proceso de entrada a la red utilizado como término para autenticar a una persona.

M

Modulación — Proceso, o resultado del proceso, de variación de algún parámetro de una señal, llamada portadora, de acuerdo con una señal mensaje (información)

N

NAT — Network Address Translation. Es un standard de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico interno y otro grupo de direcciones para el tráfico externo.

O

OFDM — (Orthogonal Frequency Division Multiplexing), este esquema de modulación utiliza múltiples sub-portadoras para transportar la información desde un usuario particular a otro. Un sistema basado en OFDM divide la información de gran velocidad en múltiples sub señales de baja velocidad que el sistema transmite simultáneamente a frecuencias diferentes en paralelo. Los beneficios de OFDM es que se tiene una alta eficiencia espectral, resistencia a interferencia de radio frecuencia (RF), y baja distorsión por múltiples caminos.

OSI — Estructura lógica de siete niveles para facilitar la comunicación entre diversos sistemas de computación.

P

Paridad — Método utilizado para detectar errores donde se cuentan los estados binarios coincidentes.

Password — Método de seguridad que autentica a un usuario específico a través de una secuencia única de caracteres para autorizar su ingreso a un sistema.

Pines — Contactos eléctricos. Pequeñas líneas salientes de metal que permiten el contacto físico entre diversos componentes de hardware.

Política — Manera de actuar de una persona, grupo, etc., con el fin de alcanzar determinados fines.

Portadora — Frecuencia continua capaz de ser modulada o readaptada por una segunda señal (información)

Protocolo — Conjunto de reglas establecidas para fijar la forma en que se realizan las transacciones.

Pulso — Cambio en el nivel o intensidad de la señal de voltaje.

Q

QPSK — Modulación digital por modulación de amplitud en cuadratura, idéntica a 4 PSK, en donde por cada dos bits de información se genera un nivel de señal modulada.

R

Radiación Isotrópica — Si una antena radia en todas direcciones de igual forma se dice que es una "Radiación Isotrópica".

Radius — Protocolo de autenticación de seguridad con clientes y servidores, muy utilizado por los proveedores de servicios Internet (ISP) en servidores remotos de sistemas operativos que no son Windows. RADIUS es el método más conocido de autenticación y autorización de usuarios de acceso telefónico y redes de túnel.

RAS — Servicio de acceso remoto a la red.

Red — Grupo de computadores y equipos periféricos asociados, conectados por un canal de comunicaciones capaz de compartir archivos y otros recursos entre usuarios.

RFID — (Radio Frequency IDentification). Método de almacenamiento remoto y recuperación de datos.

RIP (Routing Information Protocol). Protocolo utilizado por los routers para intercambiar información acerca de la red.

RJ45 RJ45 es una interfaz física comúnmente usada para terminar tipos de cables UTP. RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho 'pines' o conexiones eléctricas.

ROM Read-Only Memory. Memoria de semiconductor no destructible, es decir, que no se puede escribir sobre ella, y que conserva intacta la información almacenada, incluso en el caso de interrupción de corriente (memoria no volátil).

RS232 Interfaz serial entre DTE y DCE, velocidad máxima de transmisión de 19600 bps con una distancia máxima de 15 metros.

RS485 Interfaz serial entre DTE y DCE, velocidad máxima de transmisión de 100 kbps con una distancia máxima de 1400 metros.

S

Seguridad Calidad de seguro. Garantía que se da a alguien en la realización de algún acuerdo

Servidor Equipo destinado a proveer y administrar los servicios de red, los recursos, las aplicaciones, los archivos y la seguridad de la misma.

Sistema Operativo Software responsable de asignar espacio para recursos del sistema incluyendo memoria, tiempo de procesador, espacio de disco y equipos periféricos como impresoras, módems, etc. Todas las aplicaciones lo utilizan para acceso a los recursos necesarios para su correcta ejecución

SNMP Protocolo parte de TCP/IP para el manejo y la administración remota de los recursos de la red.

Spanning Tree — Este algoritmo cambia una red física con forma de malla, en la que se pueden formar bucles, en una red lógica en árbol en la que no se puede producir ningún lazo.

Software — Programa de aplicación o sistema operativo que una computadora ejecuta. Término amplio que puede implicar uno o varios programas y puede referirse a aplicaciones que constan de más de un programa.

SQL — El lenguaje de consulta a la base de datos cliente/servidor más conocido.

Switch — Dispositivo de red que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama. El Switch opera en la capa de enlace de datos del modelo OSI.

T

TCP/IP — Protocolos definidos por catedráticos en el proyecto ARPANet del Departamento de Defensa de Estados Unidos para la red universitaria Internet en los años setenta.

Tiempo Real — Dominación de aquellos procesos que suceden simultáneamente o con una diferencia imperceptible de tiempo. Internet ofrece tiempo real dentro de muchos servicios donde a la ejecución de una acción existe una respuesta inmediata (llegada de correo electrónico).

Topología — Descripción de las conexiones físicas de la red, el cableado y la forma en que éste se interconecta.

U

UPS — Fuente de poder que se activa cuando la señal de corriente alterna se pierde para evitar que los servidores se apaguen de manera abrupta.

V

Velocidad de transmisión — Es la velocidad a la cual los bits son enviados por unidad de tiempo, sobre el canal de comunicaciones, se expresa en bps.

W

WAN Red de área amplia que tiene nodos en diferentes localidades geográficas e implementa infraestructura de comunicaciones.

WLAN Red inalámbrica de área local (WLAN) hace exactamente lo que su nombre indica; proporciona todas las características y ventajas de las tecnologías tradicionales LAN (Local Area Network), como Ethernet y Token Ring, sin las limitaciones que imponen los cables. Pero ver una WLAN únicamente como una red sin cables, es no entenderla en absoluto: las WLAN redefinen la forma de considerar las LAN. La conectividad ya no implica una conexión física. Las áreas locales no se miden en metros, sino en kilómetros.

Wiegand Standard utilizado anteriormente para transmitir los datos entre el lector de tarjetas y el panel de control.

ANEXOS

ANEXO 1 ENCUESTAS REALIZADAS

1. ENTREVISTA REALIZADA A CADA UNO DE LOS ENCARGADOS DE LOS LABORATORIOS DEL EDIFICIO ANTIGUO DE LA EX FACULTAD DE INGENIERÍA ELÉCTRICA, EL ENCARGADO DEL CENTRO DE CÓMPUTO GENERAL.

1.1. OBJETIVO GENERAL

Conocer el estado actual de cada uno de los laboratorios del edificio antiguo de la ex facultad de ingeniería eléctrica y el centro de cómputo general frente al control de acceso físico.

1.2. OBJETIVOS ESPECIFICOS

Conocer la situación actual de cada uno de los laboratorios y del centro de cómputo general para determinar cuales son las amenazas de las cuales nos queremos proteger.

Conocer cuales son las vulnerabilidades físicas que actualmente se tienen en cada uno de los laboratorios de la ex facultad del edificio antiguo y del centro de cómputo general frente al control de acceso físico.

1.3. ENCUESTAS REALIZADAS

	Ubicación física	El 205 (Lab, Comùnicaciones)	El 204 (Lab. Postgrado)
	Nombre del encuestado	Ing. Fernando Flores	Ing. Carlos Egas
1	¿Cuántos laboratorios funcionan en esta ubicación?	3	3
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	20 sesiones/semana, aproximadamente 22 estudiantes/día	24 sesiones/semestre, 8 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No tiene un horario especifico se coordina con el encargado del laboratorio	No tiene un horario especifico se coordina con el encargado del laboratorio

4	¿Con que tipo de seguridad física cuenta el laboratorio?	Sensores de movimiento, puerta metálica	Sensor de movimiento, puerta metálica
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Se han perdido dos laptops	No han existido robos
6	¿Que número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	5 Profesores, no existen cambios de chapas, ni tampoco de claves de la consola de alarma	1 Sola persona, no existen cambios periódicos de chapas, y no se cambia la clave de la consola de alarma
7	¿Cuáles son los horarios de ingreso salida del mismo?	7am - 9pm	5pm - 9pm
8	¿Cuáles piensa usted que serían las áreas más vulnerables de este laboratorio y qué piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	El techo falso, existe una conexión directa entre el aula magna y el laboratorio	Todas las áreas
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile en el horario laborable.	2	
10	¿Cuáles serían sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?		Alarmar todo el edificio, alarmas integradas, a cada laboratorio solo tenga acceso personal autorizado, circuitos cerrados de Televisión
11	¿Cree usted qué es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si
12	¿Recomendaciones para que la comunidad Politécnica asimile estas políticas?	Mejorar la disciplina, por ejemplo salida prestada de equipos de los laboratorios	Definir claramente cuales son los derechos y obligaciones

	Ubicación física	El 203 (Lab. Redes)	El 201 (Lab. Sistemas Digitales)
	Nombre del encuestado	**Ing. Pablo Hidalgo**	**Ing. Jaime Velarde**
1	¿Cuántos laboratorios funcionan en esta ubicación?	9	2
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	6 sesiones/día, 30 estudiantes por sesión	21 sesiones/semana, 12 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y cómo se controla?	No tiene un horario especifico se coordina con el encargado del laboratorio	No tiene un horario especifico se coordina con el encargado del laboratorio
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Puerta con cerradura y sensor de movimiento	No existe ninguna seguridad
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	No han existido antecedentes	No han existido perdidas
6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	Dos personas, solo existen dos llaves.	Cuatro personas, incluyendo los ayudantes
7	¿Cuáles son los horarios de ingreso salida del mismo?	9am - 13 pm, 15 - 17, el horario es variable	9am - 6pm
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y que piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	Techo falso y la puerta, a través del techo falso existe interconexión de los diferentes laboratorios	
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile, en el horario laborable	2	2
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?	Cambiar el tipo de puertas, cambiar el techo falso, colocando una malla en el techo	Controlar el acceso, para que solo pueda ingresar personal autorizado.
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si

12	¿Recomendaciones para que la comunidad Politécnica asimile estas políticas?	Incrementar la capacitación en cuanto a seguridad, analizar detenidamente la política de seguridad para que sea implementada	Las políticas deben ser rígidas, para que las personas las cumplan.

	Ubicación física	**El 217 (Lab. Control y computación)**	**EL S25 (Lab. Taller Eléctrico)**
	Nombre del encuestado	**Ing. Yadira Bravo**	**Ing. Paco Andrade**
1	¿Cuántos laboratorios funcionan en esta ubicación?	4	1
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	35 sesiones/semana, aproximadamente 9 estudiantes/sesión	Todos los días, 25 estudiantes por día
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No tiene un horario especifico se coordina con el encargado del laboratorio	No tiene un horario definido.
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Existe una puerta metálica extra	Protecciones en las ventanas.
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Si han existido pérdidas	Se han extraviado una suelda eléctrica.
6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	7 personas, 4 ayudantes, 3 Ingenieros. No existen cambios periódicos de cerraduras.	Una sola persona.
7	¿Cuáles son los horarios de ingreso salida del mismo?	7am - 9pm	7 am – 17 pm
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y qué piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	El techo falso, puerta principal	La puerta principal
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	Siempre hay una persona	Una hora en el almuerzo.

10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?	Colocar circuitos cerrados de televisión, los mismos que se encenderán cuando no existan personas en los laboratorios.	Colocar sensores de movimiento, circuitos cerrados de televisión.
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si
12	¿Recomendaciones para que la comunidad Politécnica asimile estas políticas?	Las políticas deben ser rígidas, con sanciones para los que no las cumpla.	

	Ubicación física	**El 101 (Lab. Circuitos Eléctricos)**	**El 113 (Lab. Diseño Electrónico)**
	Nombre del encuestado	**Ing. José Medina**	**Ing. Jaime Calderón**
1	¿Cuántos laboratorios funcionan en esta ubicación?	6	1
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	12 sesiones/día, aproximadamente 62 estudiantes/día	7 sesiones/semana, 6 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No tiene un horario especifico	No tiene un horario especifico
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Puerta de hierro, en la entrada.	Sensor de movimiento.
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Sí se han perdido cosas pequeñas, como cables.	No han existido robos
6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	2 Profesores, no existen cambios de chapas.	Cuatro personas entre profesores y ayudantes.
7	¿Cuáles son los horarios de ingreso salida del mismo?	7h00 - 20h00, en forma continua	7h00 - 18h00
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y qué piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	Ventanales todo de vidrio	Proteger la puerta principal

9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	El laboratorio siempre permanece con personas en su interior durante el horario laborable.	Siempre existe alguna persona
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?		Cambiar el tipo de puertas, incrementar el número de alarmas.
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si
12	¿Recomendaciones para que la comunidad Politécnica asimile estas políticas?	Dar charlas sobre seguridad, establecer sanciones para quienes no las cumplan	

	Ubicación física	**El 105, 106, 116, 117 (Lab. Electrónica)**	**El 030, 031, (Lab. Control Industrial)**
	Nombre del encuestado	**Ing. José Pazmiño**	**Ing. Ricardo Parreño**
1	¿Cuántos laboratorios funcionan en esta ubicación?	3	2
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	40 sesiones/semana, 12 estudiantes por sesión	10 sesiones/semana, 17 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No existe un horario específico.	No existe un horario específico.
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Puerta con cerradura y sensor de movimiento, sensores magnéticos, cerradura eléctrica	Puerta metálica
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Se han perdido multímetros y calculadoras.	No los equipos que se tienen son grandes
6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	Los profesores que tienen oficinas junto al laboratorio.	Tres profesores tienen las llaves de acceso.

7	¿Cuáles son los horarios de ingreso salida del mismo?	7h00 - 18h00	7h00 - 18h00
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y que piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	Acceso por la puerta principal.	Las bodegas.
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	Máximo una hora durante el almuerzo.	1 hora
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?		Restringir el acceso.
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si
12	¿Recomendaciones para que la comunidad politécnica asimile estas políticas?	Las políticas de seguridad deben ser flexibles.	Las políticas deben ser rígidas, existe un exceso de confianza.

	Ubicación física	**El 028, 029, 012 (Lab. Control Electrónico de potencia)**	**El S03, El S04 (Lab. SEP)**
	Nombre del encuestado	**Ing. Silvana Gamboa**	**Srta. María Cardoso**
1	¿Cuántos laboratorios funcionan en esta ubicación?	3	1
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	30 sesiones/semana, aproximadamente 18 estudiantes/día	3 sesiones/día, 10 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	Nó tiene un horario especifico se coordina con el encargado del laboratorio	No tiene un horario especifico se coordina con el encargado del laboratorio
4	¿Con qué tipo de seguridad física cuenta el laboratorio?	Puerta metálica	Puerta metálica con chapa
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Se ha perdido una laptop, y cosas pequeñas durante las sesiones del laboratorio.	No han existido robos

6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	5 Profesores, y tres ayudantes.	7 personas, cada semestre se realiza cambio de chapas.
7	¿Cuáles son los horarios de ingreso salida del mismo?	8h00 - 19h30	9h00 - 19h00
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y que piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	Las puertas, por que puede ingresar cualquier persona.	La puerta de ingreso.
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	Siempre existe alguna persona	3 horas
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?	Controlar el acceso en las entradas principales. Identificación de las personas que ingresan a la universidad.	Restringir el acceso a los laboratorios solamente a personal autorizado. Almacenar la hora de ingreso y la persona que lo hizo
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	Si
12	¿Recomendaciones para que la comunidad politécnica asimile estas políticas?		

	Ubicación física	**El S17 (Lab. Máquinas Eléctricas)**	**El S05, S06, S07 (Lab. Alto Voltaje)**
	Nombre del encuestado	**Srta. María Cardoso**	**Ing. Fausto Aviles**
1	¿Cuántos laboratorios funcionan en esta ubicación?	1	1
2	¿Número de sesiones por semana, y número de estudiantes por sesión?	15 sesiones/semana, aproximadamente 6 estudiantes/sesión	4 sesiones/semana, 4 estudiantes por sesión
3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No tiene un horario especifico se coordina con el encargado del laboratorio	9h00 a 10h00, no existe ningún control.
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Ninguna	Ninguna

5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Si han existido	Se han robado equipo de laboratorio, forzando la puerta principal.
6	¿Qué número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	Tienen llaves los ayudantes de laboratorio y el jefe de departamento.	Dos personas tienen llaves de acceso al laboratorio, en su totalidad profesores.
7	¿Cuáles son los horarios de ingreso salida del mismo?	7h00 - 19h00	Todas las tardes, también durante horas en las mañanas.
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y que piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	Las puertas	La puerta
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	4 horas entre cortadas	
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?		Cambiar el tipo de puerta
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	si	si
12	¿Recomendaciones para que la comunidad politécnica asimile estas políticas?	Información constante sobre seguridad.	Dar conferencias sobre seguridad

	Ubicación física	**AD S01 (Centro de Cómputo General)**	
	Nombre del encuestado	**Ing. Juan Carlos Proaño**	
1	¿Qué tipos de servidores existen en el centro de cómputo general?	Servidor de correo, Servidor DNS, Servidor Caching Web, Servidor Web, Servidor de Matriculas, Servidor SAE.	
2	¿Cuántas personas tienen acceso a los mimos y en que horarios?	8 personas en el área de redes.	

3	¿En que horarios tiene acceso el personal de limpieza y como se controla?	No existe un horario definido, el control se lo realiza mediante la supervisión de las personas que se encuentran en el interior.	
4	¿Con que tipo de seguridad física cuenta el laboratorio?	Ninguna	
5	¿Ha existido algún evento que ha comprometido la seguridad física del mismo, como por ejemplo robos en los dos últimos años?	Hemos sido sujetos de dos robos.	
6	¿Que número de personas tienen llaves de acceso al mismo, existen cambios periódicos de chapas, en caso de existir alarmas, cuantas personas tienen acceso a las claves y con que frecuencia se cambian?	4 personas, no existen cambios periódicos de chapas.	
7	¿Cuáles son los horarios de ingreso salida del mismo?	7h30 - 18h00	
8	¿Cuáles piensa usted que serian las áreas más vulnerables de este laboratorio y que piensa usted que hay que asegurar de mejor manera o que hay que mejorar?	El área de redes y el de matriculas, debido a que estas áreas colindan con aulas las cuales son separadas por divisiones de triplex.	
9	Aproximadamente cuantas horas al día el laboratorio queda sin ninguna persona que lo vigile	ninguna	
10	¿Cuáles serian sus recomendaciones para mejorar la seguridad física en el control de acceso de esta ubicación?	Puerta eléctrica con intercomunicador, Identificación, Circuito cerrado de televisión.	
11	¿Cree usted que es necesario implantar una política de seguridad para el uso de la infraestructura de este laboratorio?	Si	
12	¿Recomendaciones para que la comunidad politécnica asimile estas políticas?	Las políticas de seguridad deben provenir desde las autoridades.	

2. ENTREVISTA REALIZADA A DIFERENTES JEFES DE DEPARTAMENTOS Y A PERSONAL EXPERTO EN SEGURIDAD.

2.1 OBJETIVO GENERAL

Obtener la opinión de las personas que interactúan con la Universidad acerca de las soluciones planteadas.

2.2 OBJETIVOS ESPECIFICOS

Obtener mayor número de criterios para mejorar la propuesta inicial acerca de las políticas de seguridad.

Identificar otros problemas que no se han podido percibir en el estudio realizado.

2.3 ENCUESTAS REALIZADAS

	Nombre del encuestado	**Ing. Juan Carlos Proaño (Encargado del área de redes de la EPN)**	**Dr. Holger Capa (Departamento de Matemática)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	si	si
2	¿Cree usted que el organismo *encargado* de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la FEPON y un representante de la AGT?	los tres primeros si los representantes de los gremios no	no se debe mezclar los gremios con un comité técnico
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran?	si	si

4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	Sí, de acuerdo a necesidades y planificación	si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	En el campo que me compete si	no , debería estar un experto en el tema
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	Debe ser de acuerdo a algún tiempo basado en algún estudio	No, se debe tener un equipo fijo.
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No, creo que a las áreas especificas sólo ingresan personas especificas, lo que se tiene que hacer es tener un buen control de acceso	no
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si	si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	De tipo administrativo y cumpliendo con las leÿes vigentes de la universidad y el país	diferentes sanciones, dependiendo del tipo de infracción
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?		controlar el acceso a cada uno de los edificios

	Nombre del encuestado	**Ing. Marcelo Muñoz (Departamento de medio Ambiente)**	**Ing. Luís Albuja (Departamento de Biológicas)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	si	si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	sin los gremios	si

3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran	si	si
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si	si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	Debe estar un ente profesional	si
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	no	no, se deben mantener las personas
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No si todo está bien definido	no
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si, además se debería tener un seguro de todos los equipos	los equipos que pertenecen a la universidad
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Se debería informar primero, la gente no es necia	depende de la infracción
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Mejorar el acceso vehicular, que no estén los guardias encargados de permitir el acceso	Permitir el ingreso de los profesores todos los días, mediante la utilización de la tarjeta.

	Nombre del encuestado	**Ing. Jenny Ruales (Departamento de Alimentos y Biotecnología)**	**Ing. Ramiro Valenzuela (Departamento de Automatización y control)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	si	si

2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	sin gremios	los gremios solo deberían aportar con sugerencias
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	cada área debería definir las políticas de seguridad y dar a conocer las mismas a las personas que interactúan con las mismas	informar de los cambios
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si, deben seguir un mejoramiento continuo	las políticas deben cambiar a largo plazo, caso contrario estarían mal definidas
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	si, en mi área	si
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	se debería invitar a un experto en el tema, para que de un diagnostico	no hay muchos cambios, se debería cambiar en el mismo periodo que el rector
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	no hay problema	no, debe existir un control de ingreso salida
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si, es una obligación de la universidad, además se debe tener un seguro de todos los equipos	si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Rígidas	las contempladas en el estatuto
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Señalización adecuada cómo la señalización que se encuentra en la entrada de eléctrica, clasificación de la basura	se debería tener algún documento que identifique a personas ajenas a la institución que desean ingresar a ciertas áreas

	Nombre del encuestado	Ing. Edwin Barriga (Departamento de Electrónica, Telecomunicaciones y Redes de Información)	Ing. Neyda Espín (Departamento de Bioprocesos)
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	si	si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	debe estar además un representante del área académica, principalmente de los postgrados	debe ser consejo politécnico
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	si	las autoridades deben dar a conocer las políticas
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si	si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	si	no
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	no simultáneamente, en mandos bajos se debería rotar.	Debe ser el mismo tiempo en que se elige consejo politécnico
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	si	no
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si	si

9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?		Consejo politécnico debe estar encargado de definir las sanciones y estas dependerán de la gravedad que se ha realizado, las políticas no puede ser ofensiva, ésta debe ser proactiva
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?		

	Nombre del encuestado	**Ing. Roberto Bohamonde (Departamento de conversión y usos de la energía)**	**Ing. Jorge Escobar (Departamento de Diseño y Producción)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	Si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	sin representantes de los gremios	Si
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	si	Si
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si	Si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	Si	no , debería estar un experto en el tema
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?		No necesariamente

7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	no	No
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Depende de la falta	Rígidas
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?		

	Nombre del encuestado	**Dr. Marco Castro (Departamento de ciencias del agua)**	**Msc. Miguel Merino (Departamento de Ciencias Sociales)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	sin representantes de los gremios	si, además debería estar el encargado de seguridad
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	no se deberían dar a conocer todas las políticas algunas si	si
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si	si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	no, debería estar un experto	no , debería estar un experto en el tema

6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	lo encargados de ejecutar las políticas si deberían ser rotados	No necesariamente en caso de necesidad si
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	no	no
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	si	si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	el organismo encargado debe definir las sanciones	rígidas
10	¿Cuáles serían sus recomendaciones para mejorar la propuesta planteada?		Se deben realizar campañas de concientización y de identidad con la politécnica

	Nombre del encuestado	**Ing. Gustavo Samaniego (Encargado de definir las políticas de seguridad Facultad de Sistemas)**	**Phd. Florinella Muñoz (Departamento de Ciencias Nucleares)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	si	Si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	Debe estar conformado por el director de recursos humanos, el director administrativo, y dos personas designadas por consejo politécnico.	El departamento de seguridad
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	si	Si

4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	si	Si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	Si	no , debería estar un experto en el tema
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	No	No
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No	No
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	Si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Depende de la gravedad de la infracción	Depende del incumplimiento
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Es urgente el implementar el control de acceso en la EPN	Se debe restringir el acceso de las personas a toda la Universidad

	Nombre del encuestado	**Ing. Oswaldo Proaño (Departamento de Procesos Industriales Químicos)**	**Ing. Jesús Játiva (Departamento de Energía Eléctrica)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	Si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	Debe estar conformado por el director Administrativo y por el experto en seguridad.	Debería ser una comisión

3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	Si	Están muchas personas, no deberían estar los representantes de los gremios.
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	Si	Si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	Si	no , soy una persona que tiene muchas ocupaciones.
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	No	Si pero no todas las personas al mismo tiempo.
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	Si	No, si se debe restringir el acceso a ciertas áreas.
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	Si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	No es una cuestión de sancionar.	De acuerdo a las políticas establecidas en el código de trabajo y de la EPN.
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Implementar lo más pronto la propuesta planteada.	Para ingresar a ciertas áreas todos los miembros de la EPN deben presentar su identificación lo mismo personas externas a la institución.

	Nombre del encuestado	**Dr. Nelson Medina (Departamento de Física)**	**Ing. Ezequiel Guaman (Departamento de pedagogía para el perfeccionamiento de la enseñanza de las ciencias básicas)**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	Si

2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	Sin los representantes de los gremios.	Debe ser conformado por personal técnico, debe estar el Director Administrativo, el Director de Construcciones y un experto en seguridad.
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	Si	Si, la comisión de seguridad esta en la obligación.
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	Si	Si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	No	Si
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	No	Las personas deberían rotar los cargos no.
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No	No
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	Si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Depende de la infracción	Deben ser multados económicamente
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?		La seguridad debe ser una política institucional.

	Nombre del encuestado	Ec. Marcelo Sosa (Departamento Financiero)	Ing. Vinicio Melo (Departamento de Petróleos y Gas Natural)
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	Si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	Si	No deben estar los representantes de los gremios.
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	Si	Si
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	Deben seguir un proceso continuo de actualización	En la actualidad no existen políticas definidas
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?		Si
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	Nò, es un órgano colegial	No son dos funciones diferentes
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No	No
8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiedad privada?	Si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	Las sanciones deben cumplir con la ley de carrera Civil y Administrativa	Debe existir una escala de sanciones y depende de la falta

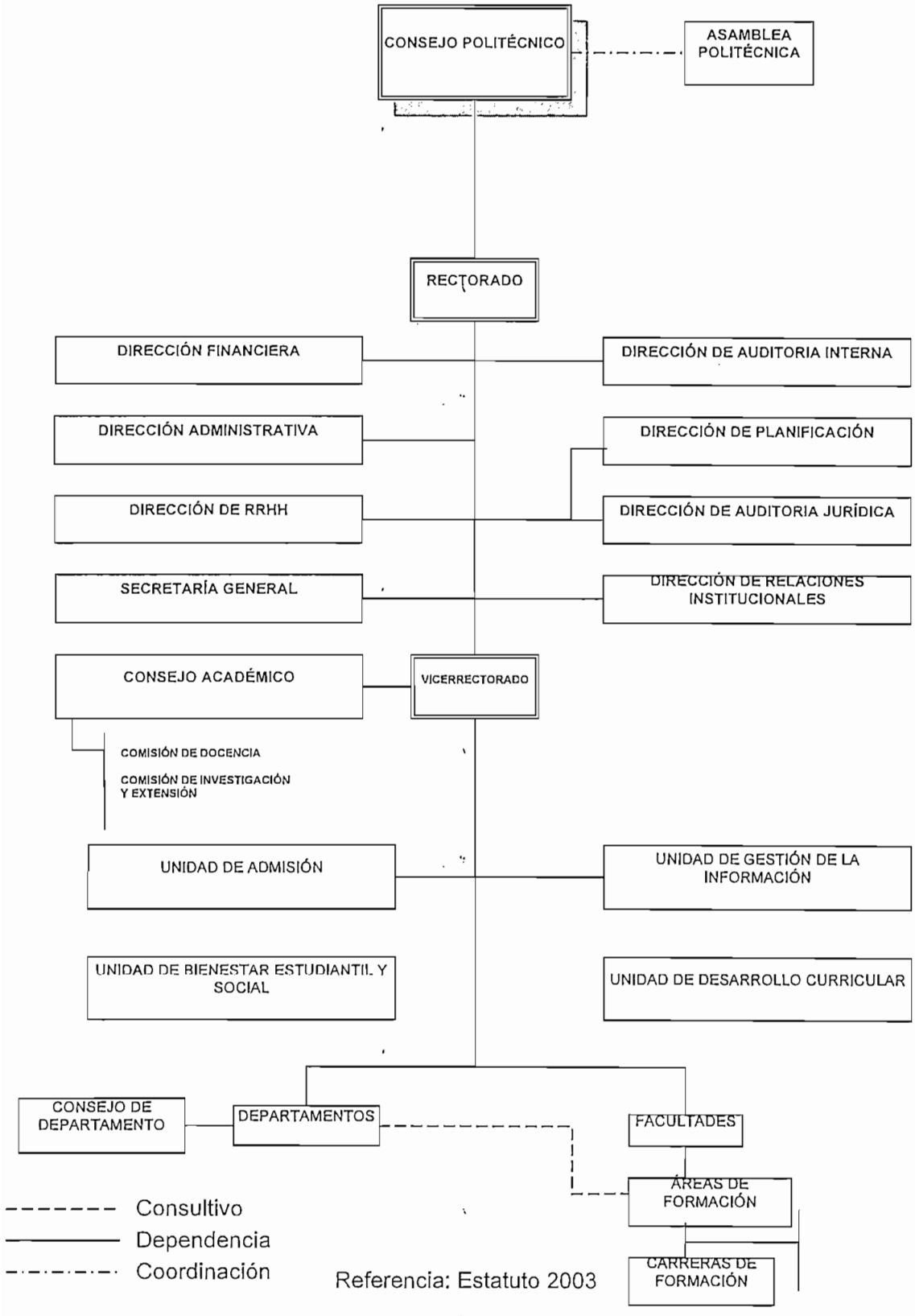
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Se deben laborar normas de seguridad y difundirlas. Crear una disciplina interna de observación de leyes.	El personal encargado de la seguridad debe conocer sobre el tema

	Nombre del encuestado	**Ing. Halina Lachowics (Departamento de Recursos Naturales y Geoquímica)**	**Ing. Enrique Mafla (Experto en Seguridad**
1	¿Cree usted que las políticas de seguridad deben ser definidas por un organismo?	Si	Si
2	¿Cree usted que el organismo encargado de definir las políticas de seguridad debe estar conformado por el director de recursos humanos, el director administrativo, un docente experto en seguridad, un representante de la ADEPON, un representante de la FEPON y un representante de la AGT?	Sin los representantes de los gremios	Debe ser conformado por un profesional en seguridad no por un docente
3	¿Cree usted que los encargados de seguridad están en la obligación de dar a conocer continuamente las políticas de seguridad que se estarán implementando en la Universidad a toda la comunidad politécnica, además estas personas deberán despejar todas las inquietudes de las personas que lo requieran.	Si	Si
4	¿Cree usted que las políticas deben seguir un proceso continuo de afinamiento?	Si	Si
5	¿Estaría usted dispuesto a colaborar como miembro del comité de seguridad para definir las mismas?	No	
6	¿Cree usted que se deben rotar periódicamente a las personas encargadas de definir las políticas de seguridad y a las personas encargadas de implementar las mismas?	Se debe rotar para tener nuevas iniciativas	Por seguridad se debería rotar a las personas de implementar las políticas
7	¿Cree usted que se estaría limitando la libertad de las personas que interactúan con la universidad si se restringe el acceso a ciertas áreas?	No	No, es necesario limitar el acceso

8	¿Se debería tener un registro de todos los equipos que se encuentran en cada uno de los laboratorios aunque algunos de los mismos sean propiédad privada?	Si	Si
9	¿Cómo deberían ser las sanciones para las personas que incumplen con las políticas de seguridad?	De acuerdo al reglamento	Combinación de políticas institucionales respetando el marco legal
10	¿Cuáles serian sus recomendaciones para mejorar la propuesta planteada?	Se deben realizar simultáneamente simulacros. Establecer planes de contingencia. Evacuar desechos tóxicos	No olvidar la seguridad lógica

Nota.- No se pudo realizar las encuestas a los demás Jefes departamentales debido a la poca información existente en la Universidad acerca de la ubicación de las oficinas de los mismos y a la falta de disponibilidad.

3. ORGANIGRAMA ESTRUCTURAL GENERAL EPN.



ANEXO 2.- ACTIVOS REGISTRADOS DE CADA UNO DE LOS LABORATORIOS DEL EDIFICIO ANTIGUO DE LA EX FACULTAD DE INGENIERÍÀ ELÉCTRICA Y EL CENTRO DE CÓMPUTO GENERAL DE LA EPN.

LABORATORIO DE COMUNICACIONES

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	CD ROM	PLÁSTICO (A/N) (A/N), 8X	1	20,40	20,40
2	COMPUTADOR	PLATINO (DTK) (CREMA) (15) CPU, con procesador intel 486 SX-25 MHz, 4 Mb. de memoria RAM, disco duro de 130 Mb), Monitor MVGA marca DTK, Mod. VM-14AF, serie # 5011752, 1 Teclado DTK, Mod. SPK-105E, serie # 950322343, 1 Mouse DTK, serie # 920880353.	1	357,00	357,00
3	COMPUTADOR	PLÁSTICO (COMPAQ) (BLANCO) (22) CPU, con microprocesador pentium 120 MHz, 32 Mb. de memoria RAM,.disco duro de 2 GIGAS,Monitor SVGA, COMPAQ, Mod. 610, serie # 641BC050G477. Teclado COMPAQ, serie # 1GD39DH13006. Mouse COMPAQ, Mod. M-S34, serie # B04AB0	1	450,60	450,60
4	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) (25) CPU, procesador pentium III, 450 MHz, disco duro de 6.4 Gb. parlantes.1 Monitor 14" SVGA marca OPTIQUEST-Q41, Mod. VCDTS21384-1E, serie # 6B90600736, 1 Teclado marca ACER, Mod. 6512-TW, serie # X1S93402477,1 Mouse marca GENIUS, serie # 90249735	4	800,00	3.200,00
5	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) (27) CPU, procesador pentium III, 450 MHz, 64 MB, disco duro de 8.4 Gb.,$ 776.00, 1 Monitor marca PREMIO, Mod. TE555G, serie # CX91711648. $ 190.00, 1 Teclado marca ACER, Mod. 6512-TW, serie # X1S93402477, 1 Mouse marca GENIUS, serie # 90249735	1	700,00	700,00
7	CPU	METÁLICO (A/N) (A/N) MINITOWER	1	150,00	150,00
8	DIMM DE MEMORIA	PLÁSTICO (A/N) (A/N) 32 Mb	1	46,78	46,78
9	DISCO	METÁLICO (A/N) (A/N) DE 1.2 Gb	1	20,00	20,00
10	DRIVE 3 ½	PLÁSTICO (A/N) (CREMA)	1	6,80	6,80
11	EXTRACTOR	METÁLICO (A/N) (A/N) DE SUELDA	1	5,60	5,60
12	FUENTE DE PODER	METÁLICO (MARCHESI) (A/N)	2	200,00	400,00
14	GENERADOR DE FUNCIONES	PLÁSTICO (NEWTRONICS) (A/N) Y PULSOS	1	630,00	630,00
15	GENERADOR DE FUNCIONES	PLÁSTICO (WAVETEK) (NEGRO)	2	530,00	1.060,00
17	MICROFONO	PLÁSTICO (A/N) (A/N)	1	2,62	2,62
18	MONITOR	PLÁSTICO (EPSON) (CREMA)	1	65,00	65,00
19	MOTHERBOARD	PLÁSTICO (A/N) (A/N) PARA ACTUALIZAR EL COMPUTADOR EPSON ACTION PC 5600	1	160,23	160,23
21	MOUSE	PLÁSTICO (EPSON) (CREMA)	1	6,55	6,55
22	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) SOFTWARE WSTRO VERSIÓN2.2 CON INTERFACE MOD. TDS2M	1	2.532,62	2.532,62
23	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) PORTATIL	1	1.230,00	1.230,00
24	PARLANTE	PLÁSTICO (A/N) (A/N)	2	2,70	5,40
26	PROCESADOR	PLÁSTICO (A/N) (A/N) PENTUIM III 350 MHz	1	122,81	122,81
27	PROGRAMADOR DE MEMORIA	PLÁSTICO (XELTEK) (A/N) EPROM, FLASH/RAM, MICROPROCESADOR I51	1	350,00	350,00
28	PROTOBOARD	PLÁSTICO (DESING LAB) (ROJO) Con Generador y Fuente Digital	2	495,00	990,00
31	TARJETA DE RED	PLÁSTICO (A/N) (A/N)	3	5,22	15,66
34	TARJETA DE RED	PLÁSTICO (A/N) (A/N) PCI	10	24,61	246,10
44	TARJETA DE RED	PLÁSTICO (A/N) (A/N) NE 2000	1	5,25	5,25
45	TARJETA DE VIDEO	PLÁSTICO (A/N) (A/N) PCI ,1Mb	3	5,98	17,94
48	TECLADO	PLÁSTICO (EPSON) (CREMA)	1	7,28	7,28
		TOTAL			12.804,64

LABORATORIO DE POSTGRADO

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor SVGA a color marca LG series No 006AC54034 Modelo 52V, (1) Teclado Windows Series No. 100090563814 - modelo SG-100, (1) Mause generico 600090448034	1,00	765,00	765
2	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), Memoria RAM 64 Mb, Disco duro 30 Gb, CD ROM 52X serie No AO3166662, Monitor marca LG de 15" serie No 005ACCO166 M odelo 552V, Mause serie No 6000101203962, Teclado generico No KJXMCK-701W	1,00	730,00	730
3	COMPUTADOR	PLÁSTICO (INTEL) (BLANCO), (1) Monitor marca VIEW SONIC 14" modelo E40 serie No. C102997177, (1) Teclado Generico, (1) Mause Marca OMEGA Modelo MUS25	1,00	725,00	725
4	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor SVGA a color marca LG series No 006AC53998 Modelo 52V, (1) Teclado Windows Series No. 100090563813 modelo SG-100, (1) Mause generico 600090447673 .	1,00	765,00	765
5	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor SVGA a color marca LG series No 006AC56963 Modelo 52V, (1) Teclado Windows Series No. 100090563812 modelo SG-100, (1) Mause genericos 600090448031.	1,00	765,00	765
6	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor SVGA a color marca LG series No 006AC5432 Modelo 52V, (1) Teclado Windows Series No. 6905170650 modelo SG-100, (1) Mause generico 600090448033.	1,00	153,00	153
7	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor marca VIEW SONIC 14" modelo E40 serie No. C103204129, (1) Teclado Generico, (1) Mause Marca OMEGA Modelo MUS25.	1,00	725,00	725
8	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor marca VIEW SONIC 14" modelo E40 Serie No. CI03203126, (1) Teclado Generico, (1) Mause Marca OMEGA Modelo MUS25.	1,00	157,83	157,83
9	COMPUTADOR	PLÁSTICO (CLON) (BLANCO), (1) Monitor marca VIEW SONIC 14" modelo E40 SEREI C103201162, (1) Teclado Generico, (1) Mause Marca OMEGA Modelo MUS25.	1,00	725,00	725
10	HUB	METÁLICO (INTEL) (NEGRO), DE 16 PUERTOS	2,00	812,00	1624
11	IMPRESORA	PLÁSTICO (HEWLETT PACKARD) 840C (BLANCO)	1,00	200,00	200
12	IMPRESORA	PLÁSTICO (EPSON) (BLANCO) MARTRICIAL	1,00	225,00	225
13	MODULO DE ADMINISTRACION	PLÁSTICO (A/N) (A/N)	2,00	888,00	1776
14	PANTALLA	TELA (BREAST DRILL) (BLANCO) DE PROYECCION DE 1.75 X 1.75 mm	1,00	114,00	114
15	PATCH PANEL	METÁLICO (A/N) (NEGRO) DE 24 PUERTOS RJ45 CAT 5E	2,00	118,00	236
16	PATCH PANEL	METÁLICO (A/N) (NEGRO) COFIGURABLE ARMADO CON 4 PUERTOS DUPLEX DE FIBRA OPTICA	1,00	490,00	490
17	RACK DE PISO	METÁLICO (A/N) (NEGRO) DE 19" PARA MONTAJE	1,00	150,00	150
18	ROUTER	PLÁSTICO (MOTOROLA) (NEGRO)	2,00	1.201,50	2403
19	ROUTER	METÁLICO (CISCO) (PLOMO) CISCO 2610: Con tarjeta WAN CISCO Serie No. 30763054. Cable CISCO Smart Serial Crossover	2,00	1.593,00	3186
20	SCANNER	PLÁSTICO (A/N) (BLANCO)	1,00	75,00	75
21	SWITCH	PLÁSTICO (INTEL) (NEGRO) DE 16 PUERTOS	2,00	1.473,59	2947,18
22	TARJETA DE VOZ	PLÁSTICO (A/N) (A/N)	2,00	628,20	1256,4
23	UGRADE DE MEMORIA	PLÁSTICO (A/N) (A/N) FRAME RELAY E IP. 8 Mb	2,00	154,80	309,6
		TOTAL			19738,01

LABORATORIO DE REDES

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	COMPUTADOR	CLON	18	987,00	17766
2	RUTEADOR	PLASTICO SINTETICO (CISCO), WIC 2T, 2 puertos seriales para interfaz WAN, cable.	1	2.894,41	2894,41
3	RUTEADOR	PLASTICO SINTETICO (CISCO), WIC 2T, 2 puertos seriales para interfaz WAN, cable.	1	2.956,00	2956
4	SWITCH	PLÁSTICO (Cisco) de 24 puertos	1	1.473,59	1473,59
		TOTAL			25090

LABORATORIO DE SISTEMAS DIGITALES

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ABSORVEDOR DE SUELDA	METÁLICO (A/N) (AZUL) (87)	1	8,00	8,00
2	CAJA	METÁLICO (A/N) (A/N) (138) PORTAELEMENTOS DE 16 COMPARTIMENTOS	1	27,00	27,00
3	CHUPA SUELDA	METÁLICO (A/N) (AZUL) (154)	1	4,80	4,80
4	CHUPA SUELDA	METÁLICO (A/N) (AZUL) (160)	1	5,00	5,00
5	COMPUTADOR	PLÁSTICO (CLON) (CREMA) (185) ALTON PLUS	2	510,05	1.020,10
7	CURSOS (VIDEO)	PLÁSTICO (A/N) (A/N) (143).DE ELECTRONICA ANALOGA AC, CON VIDEOS, MUEBLE Y BETA	1	16,32	16,32
8	DISCO	METÁLICO (IBM) (A/N) (151) DURO DE 10 MB.	1	1,63	1,63
9	EQUIPO DE AIRE ACONDICIONADO	METÁLICO (GENERAL ELECTRIC) (A/N) (68)	1	7,90	7,90
10	EXTENSOR DE SEÑALES PARA C.I	PLÁSTICO (A/N) (A/N) (84) DE16 PATAS PC-16	1	3,00	3,00
11	EXTENSOR DE SEÑALES PARA C.I	PLÁSTICO (A/N) (A/N) (86) DE 40 PATAS PC-40	1	3,00	3,00
12	FUENTE DE PODER	METÁLICO (MARCHESI) (N/N) (97) Triple	3	200,00	600,00
15	FUENTE DE PODER	METÁLICO (BK PRECISION) (CREMA-AZUL)	4	750,00	3.000,00
19	FUENTE REGULADA	METÁLICO (HEATKIT) (N/N) (115)	1	59,00	59,00
20	GENERADOR DE FUNCIONES	METÁLICO (B&K PRECISION) (A/N) (157)	4	216,64	866,56
24	GENERADOR DE FUNCIONES	PLÁSTICO (WAVETEK) (NEGRO)	4	530,00	2.120,00
28	IMPRESORA TÉRMICA	PLÁSTICO (A/N) (A/N) (29)	1	69,00	69,00
29	LÁMPARA ULTRAVIOLETA	METÁLICO (A/N) (NEGRO) (1) PARA BORRADO DE MEMORIAS PROGRAMABLES	1	180,00	180,00
30	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (N/N) (43) DC 1-10 Ua	2	250,00	500,00
32	MONITOR	PLÁSTICO (CRT LEEDEX) (A/N) (13)	1	160,00	160,00
33	MONITOR	PLÁSTICO (APPLE MACINTOSH) (CREMA) (144) 2 SIN SERIE	1	160,00	160,00
34	MULTÍMETRO	METÁLICO (A/N) (A/N) (127) Y I BUFER INTERFASE PARA COMPUTADOR	1	92,10	92,10
35	MULTÍMETRO	PLÁSTICO (METEX) (A/N) (158) DIGITAL DE 3 1/2 DIGITOS	1	54,00	54,00
36	MULTÍMETRO	PLÁSTICO (ER) (A/N) (172)	1	10,80	10,80
37	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (65)	1	2.532,62	2.532,62
38	OSCILOSCOPIO	PLÁSTICO (PHILIPS) (CREMA) (77) TIPO PM 3211	2	1.230,00	2.460,00
40	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) CON PUNTAS DE PRUEBA	1	2.532,00	2.532,00
41	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA-AZUL) DE DOS CANALES	4	2.532,00	10.128,00
45	PORTACABLE	METÁLICO (TERCO) (N/N) (69) y (116)	2	5,00	10,00
47	PÓRTICO (PUERTO) DE COMUNICACIÓN	PLÁSTICO (A/N) (A/N)	1	49,87	49,87
48	PROGRAMADOR UNIVERSAL	PLÁSTICO (A/N) (A/N) (184) CON CABLE DE CONECCIÓN	1	148,05	148,05

49	PROTOBOARD	PLÁSTICO (DESING LAB) (ROJO) CON GENERADOR Y FUENTE DIGITAL	4	495,00	1.980,00
53	REGLETA TOMACORRIENTE	PLÁSTICO (A/N) (PLOMO) (113) (plugmolds)	9	10,00	90,00
		TOTAL			28.890,75

LABORATORIO DE CONTROL Y COMPUTACIÓN

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ACCESORIOS	METÁLICO (TEKTRONIX) (PLOMO) PARA INSTALAR UNA UNIDAD DE DISKETTES	1	6,25	6,25
2	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2, kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, series # 844BL002100535, 1 Teclado marca PREMIO, Mod. KFKEA5XA, series # 83J41626, 1 mouse marca MICROSOFT, series # 2358003	1	493,08	493,08
3	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, series # 844BL002100 269 1 Teclado marca PREMIO, Mod. KFKEA5XA, series # 83J40743, 1 mouse marca MICROSOFT, series # 2831725	1	493,08	493,08
4	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, series # 844BL002100270 1 Teclado marca PREMIO, Mod. KFKEA5XA, series # 83J41629 1 mouse marca MICROSOFT, serie # 2358082	1	493,08	493,08
5	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, serie # 844BL002100265 1 Teclado marca PREMIO, Mod. KFKEA5XA, serie # 83J41624 1 mouse marca MICROSOFT, serie # 2831644	1	493,08	493,08
6	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, serie # 844BL002100279 1 Teclado marca PREMIO, Mod. KFKEA5XA, serie # 83J40748 1 mouse marca MICROSOFT, serie # 2831671	1	493,08	493,08

7	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, serie # 844BL002100278 1 Teclado marca PREMIO, Mod. KFKEA5XA, serie # 83J41853 1 mouse marca MICROSOFT, serie # 2400825	1	493,08	493,08
8	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, serie # 844BL002100544 1 Teclado marca PREMIO, Mod. KFKEA5XA, serie # 83J41632 1 mouse marca MICROSOFT, serie # 2831597	1	493,08	493,08
9	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) 1 C.P.U.procesador intel pentium II 333 MHz, Memoria.Ram64 Mb. Memoria cache 512 Kb. Disco duro de 6.4 Gb. Drive de 3 1/2 kit multimedia 36X, 2 parlantes c/u. Tarjeta de sonido de 16 bits, 1 Monitor PREMIO 15", SVGA, Mod. M571, serie # 844BL002100267. 1 Teclado marca PREMIO, Mod. KFKEA5XA, serie # 83J41625 1 mouse marca MICROSOFT, serie # 2400834.	1	493,08	493,08
10	COMPUTADOR	PLÁSTICO (EAI) (AMARILLO) 1 Consola básica con:Controle, Panele programable, Expansiones analogicas, Expansiones logicas-Generador de funciones, Generador de funciones logicas.19 Tarjetas de funciones varias, en c/u de los computadores 11 Paneles de conexión, en total para los 2 computadores.	1	597,00	597,00
11	COMPUTADOR	PLÁSTICO (EAI) (AMARILLO) 1 Consola básica con:Controle, Panele programable, Expansiones analogicas, Expansiones logicas-Generador de funciones, Generador de funciones logicas. 19 Tarjetas de funciones varias, en c/u de los computadores 11 Paneles de conexión, en total para los 2 computadores.	1	597,00	597,00
12	COMPUTADOR	PLÁSTICO (IBM) (CREMA) TIPO 8560041 1 C.P.U. con procesador matematico INTEL 80287-10 1 Monitor a color, marca IBM, tipo 8513-001, serie # 72-0122379 1 Teclado en español, marca I.B.M. Mod. M, serie # 78-0078027	1	655,00	655,00
13	COMPUTADOR	PLÁSTICO (COMPAQ) (CREMA) 1 C.P.U. monitor , con procesador 80486DX2, 8 MB memoria RAM, 1.44 MB, disco duro de 340 MB, 1 puerto paralelo, 2 puertos seriales, fax modem integrado, 2 slots de extensión ISA. 1 Teclado marca COMPAQ, Mod. RT102, serie # 120083-014A. 1 Mouse, marca COMPAQ, Mod. M-S28-6MD, serie # 1D768AB26076	1	655,00	655,00
14	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) 1 C.P.U. microprocesador intel de 120 MHz, 16 Mb. de ram, disco de 1.2 Gb. 1 Monitor PREMIO color SVGA, Mod. H450, serie # 702RL00AU00005. 1 Teclado marca PREMIO, Mod. KPQA5ZA, serie # 693J2546*7279. 1 Mouse marca PREMIO, Mod. ECM-S3902, serie # 0066663.	1	205,20	205,20
15	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) 1 C.P.U. microprocesador intel MMX 233 MHz, 64 Mb. ram, disco de 1.2 Gb drive de 3 1/2, disco de 4.3 Gb. tarjetas de video, sonido y de red NE2000. 1 Monitor marca PREMIO SVGA 15", Mod. H554, series # 8114U002U00873 1 Teclado marca PREMIO, Mod. KPQEA5ZA, series # 7B3D1972*7746 -	1	332,70	332,70

16	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) 1 C.P.U. microprocesador intel MMX 233 MHz, 64 Mb. ram, disco de 1.2 Gb drive de 3 1/2, disco de 4.3 Gb. tarjetas de video, sonido y de red NE2000. 1 Monitor marca PREMIO SVGA 15", Mod. H554, series # 8284U002U00242. 1 Teclado marca PREMIO, Mod. KPQEA5ZA, series # 7B3D1242*7746.	1	332,70	332,70
17	COMPUTADOR	PLÁSTICO (IBM) (BLANCO) PS/2 1 C.P.U. 286 procesador matemàtico memoria RAM 1 Mb. disco duro de 80 MB 1 drive de disco flexible 3 1/2, con cable	1	255,00	255,00
18	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) MONITOR MARCA "LG" DE 15" MODELO 55V. SERIE No 005AC97519, TECLADO MARCA SOFT SERIE No CAP0007X237964. MOUSE MARCA GENIUS	1	640,00	640,00
19	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) 1 C.P.U. con procesador pentium III, 450 MHz, disco duro de 6.4 Gb, drive de 3 1/2, con tarjetas de red y fax 56.6K. CD ROM DE 48X , PARLANRES 1 Monitor 14" OPTIQUEST-Q41, Mod. VCDTS21384-1E, serie # 6B90900878 1 Teclado marca ACER, Mod. 6512-TW, serie # X1S93402475 1 Mouse marca GENIUS, serie # 90249710	1	601,51	601,51
20	COMPUTADOR	PLÁSTICO (CLON) (AZUL Y BLANCO) PROCESADOR PENTIUM DE 550MHz, DISCO DURO MARCA QUANTUM MONITOR MARCA "LG" SVGA 14" SERIE No 005AC42634 MODELO 45V, TECLADO MARCA KEYBOARD SERIE No 3892A059 MODELO NK 118, MAUSE SERIE No 699080118683 JUEGO DE PARLANTES Y MICROFONO.	1	825,00	825,00
21	COMPUTADOR	PLÁSTICO (CLON) (AZUL Y BLANCO) PROCESADOR PENTIUM DE 550MHz, DISCO DURO MARCA QUANTUM. MONITOR MARCA "LG" SVGA 14" SERIE No 005AC42650 MODELO 45V, TECLADO MARCA KEYBOARD SERIE No 3892A059 MODELO NK 118, MAUSE SERIE No 699080118660 JUEGO DE PARLANTES Y MICROFONO.	1	825,00	825,00
22	CONECTOR	PLÁSTICO (A/N) (VERDE)	4	3,36	13,44
23	DÉCADA CAPACITIVA	ACRÍLICO (HEATKIT) (NEGRO)	2	10,00	20,00
24	DÉCADA DE RESISTENCIA	ACRÍLICO (COENELL DIBILLER) (CONCHO DE VINO)	4	10,00	40,00
25	ENTORCHADOR DESENTORCHADOR	METÁLICO (A/N) (CROMADO) DE ALAMBRE	1	7,00	7,00
26	ESTACIÓN DE ADQUISICIÓN DE DATOS	METÁLICO (KEITHLEY) (PLOMO)	1	175,90	175,90
27	ESTACIÓN PARA SOLDAR	PLÁSTICO (ER) (AMARILLO)	1	7,20	7,20
28	EXPANSOR DE MEMORIA	METÁLICO (TEKTRONIX) (PLOMO)	1	4,77	4,77
29	FUENTE DE PODER	METÁLICO (MARCHESI) (VERDE)	1	220,00	220,00
30	GENERADOR DE FUNCIONES	PLÁSTICO (SIMPSON) (CELESTE) O DE SEÑALES	1	340,00	340,00
31	GENERADOR DE FUNCIONES	PLÁSTICO (BK PRECISION) (NEGRO)	1	196,00	196,00
32	GENERADOR DE FUNCIONES	ACRÍLICO (B&K PRECISION) (NEGRO)	1	216,40	216,40
33	GRAFIZADOR	METÁLICO (HEWLETT PACKARD) (CREMA) XY	1	245,00	245,00
34	GRAFIZADOR	METÁLICO (HEWLETT PACKARD) (CREMA) XY	1	133,00	133,00
35	GRAFIZADOR	ACRÍLICO (TEKTRONIX) (PLOMO) DIGITAL X Y	1	133,00	133,00
36	IMPRESORA	PLÁSTICO SINTETICO (EPSON) (AMARILLO) FX-286E DE 132 COLUMNAS	1	64,00	64,00
37	IMPRESORA	PLÁSTICO (IBM) (BLANCO) PROPINTER	1	64,00	64,00
38	IMPRESORA	PLÁSTICO (TEKTRONIX) (AMARILLO)	1	64,00	64,00
39	IMPRESORA	PLÁSTICO (HEWLETT PACKARD) (BLANCO)	1	64,00	64,00
.40	MICROCOMPUTADOR	PLÁSTICO (MAGISTRONIC) (PLOMO) MONITOR COLOR AMARILLO	1	130,36	130,36
41	MICROCOMPUTADOR	PLÁSTICO (TEKTRONIX) (AZUL Y BLANCO)	1	143,10	143,10

42	MICROCOMPUTADOR	PLÁSTICO (MAGITRONIC) (BLANCO) 1.- MONITOR MARCA MAGITRONIC	1	111,40	111,40
43	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) AMPLIFICADOR DE BASE DE TIEMPO	1	71,00	71,00
44	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) AMPLIFICADOR DE CUATRO CANALES	1	198,00	198,00
45	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) AMPLIFICADOR DE DOBLE CANAL	1	37,00	37,00
46	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) AMPLIFICADOR DE DOBLE TRAZO	1	100,00	100,00
47	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) AMPLIFICADOR DIFERENCIAL	1	290,00	290,00
48	MÓDULO	ALUMINIO (TEKTRONIX) (PLATEADO) BASE DE TIEMPO Y AMPLIFICADOR HORIZONTAL	1	260,00	260,00
49	MÓDULO	PLÁSTICO SINTETICO (A/N) (NEGRO) PARA EL MULTIMETRO MARCA FLUKE MODELO 80TK	1	179,00	179,00
50	MÓDULO	PLÁSTICO SINTETICO (A/N) (PLOMO) MICROLAB	2	135,00	270,00
51	MÓDULO	PLÁSTICO (A/N) (PLOMO) DIDACTICOS PARA MICRO BASIC	2	117,90	235,80
52	MÓDULO	PLÁSTICO (A/N) (PLOMO) DIDACTICOS PARA MICRO LAB	2	491,60	983,20
53	MOUSE	PLÁSTICO (LOGITECH) (BLANCO)	1	2,06	2,06
54	MOUSE	PLÁSTICO (IBM) (BLANCO)	1	2,06	2,06
55	MULTÍMETRO	PLÁSTICO (KT) (CREMA)	1	36,00	36,00
56	MULTÍMETRO	PLÁSTICO (GOLDSTAR) (AMARILLO)	1	151,60	151,60
57	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL)	1	599,00	599,00
58	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) DE DOBLE TRAZO	1	461,00	461,00
59	OSCILOSCOPIO	PLÁSTICO (PHILIPS) (NEGRO) TIPO PM-3211	2	540,00	1.080,00
60	PORTACABLE	METÁLICO (TERCO) (AZUL)	1	5,00	5,00
61	PROBADOR LÓGICO	PLÁSTICO SINTETICO (B&K PRECISION) (AMARILLO) TIPO PUNTA	2	35,00	70,00
		TOTAL			17.889,04

CUARTO DE TELECOMUNICACIONES

Nº	Activo Fijo	Descripción	CANTIDAD	PRECIO UNITARO $	PRECIO TOTAL $
1	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) (25) CPU, procesador pentium III, 450 MHz, disco duro de 6.4 Gb. parlantes.1 Monitor 14" SVGA marca OPTIQUEST-Q41, Mod. VCDTS21384-1E, serie # 6B90600736, 1 Teclado marca ACER, Mod. 6512-TW, serie # X1S93402477,1 Mouse marca GENIUS, serie # 90249735	3	800,00	2.400,00
4	CONVERTIDOR	PLÁSTICO (ALUED TELESYN) (PLOMO) MEDIA	1	149,00	149,00
5	MOTOROLA	PLÁSTICO (A/N) (A/N) (24) 1 Ruteador de 1 puerto serial, 1 puerto de control CTP de 2 Mb. De memoria Flash. $ 395.40, 1 Modem digital DSU tipo tarjeta para anidar en equipos motorola vanguard port 2. $. 83.68, 1 Tarjeta de voz FXS/FXO, para equipos de motorola vanguard. $.	1	696,66	696,66
6	SWITCH	PLÁSTICO (IBM) (NEGRO) DE 24 PUERTOS 10 BASE -TX, 1 PUERTO 100 BASE-TX	2	543,23	1.086,46
8	SERVIDOR PROXY	IBM	1	1.300,00	1.300,00
9	SERVIDOR RAS	SOHO ROUTER	1	1.650,00	1.650,00
10	HUB	METÁLICO (INTEL) (NEGRO) DE 16 PUERTOS	1	812,00	812,00
		TOTAL			8.094,12

LABORATORIO DE CIRCUITOS ELÉCTRICOS

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	AMPERÍMETRO	METÁLICO (TRIPLETT) (A/N), DC 0-1 A, CON CAJA	10	65,00	650,00
2	AMPERÍMETRO	METÁLICO (NORMA) (A/N), (517) 1.2-6 30A	3	100,00	300,00
3	AMPERÍMETRO	METÁLICO (YEW) (A/N), (75) DeCC 1 A TIPO 2143	2	100,00	200,00
4	AMPERÍMETRO	METÁLICO (NORMA) (A/N)	3	100,00	300,00
5	AMPLIFICADOR	PLÁSTICO (WESTINNGHOUSE) (A/N) (113) BIESTABLE	1	100,00	100,00
6	ANALIZADOR DE ONDA	(25) METÁLICO (HEWLETT PACKARD) (A/N)	1	151,00	151,00
7	ANALIZADOR DE REDES	METÁLICO (SIEMENS) (A/N) (522) DE CC, MARCA SIEMENS CON: 6 GENERADORES DE 36 LINEAS, 27 CARGAS, 12x2 SUBESTACIONES; CON ALIMENTADOR	1	268,00	268,00
8	AUTOTRANSFORMADOR	PLÁSTICO (POWESTER) (A/N) (129) DE 280 V, 3.5 A, 0.98 KVA.	5	200,00	1.000,00
9	AUTOTRANSFORMADOR	PLÁSTICO (GENERAL RADIO) (A/N) (18) MONOFÁSICO 140 V, 5A	6	158,00	948,00
10	AUTOTRANSFORMADOR	PLÁSTICO (GENERAL ELECTRIC) (A/N) (17) TRIFÁSICO, PATENTE 2949592	2	158,00	316,00
11	AUTOTRANSFORMADOR	PLÁSTICO (GENERAL RADIO) (A/N) (90) VARIABLES, DE 120 V, 60 CICLOS 0-140 V 5 A PATENTE 2949592	3	170,00	510,00
12	AUTOTRANSFORMADOR	PLÁSTICO (GENERAL RADIO) (A/N)	1	170,00	170,00
13	AUTOTRANSFORMADOR	PLÁSTICO (POWERSTAT) (A/N) (95) VARIABLES, 2 DE 9 A TIPO 2PF 236; 1 DE 20 A TIPO 2PF 136	2	170,00	340,00
14	AUXILIAR	MADERA (A/N) (VERDE) (144) FORRADO CON FORMICA	1	10,00	10,00
15	BOBINA	PLÁSTICO (SYBRON) (A/N) (130) FLEXIFORME DE 120/150 V.	1	10,00	10,00
16	BOBINA	PLÁSTICO (SUPERIOR ELECTRIC) (A/N) (127) SUPERIOR 120/1000 V FLEXIFORME	1	10,00	10,00
17	BOBINA	PLÁSTICO (SUPERIOR ELECTRIC) (A/N) (128) SUPERIOR REACTOR 120 V, 4 OHM TYPELR - 2	6	10,00	60,00
18	CAJA DIVISOR DE VOLTAJE	METÁLICO (LEEDS NORTHRUP) (A/N) (43), DE 750 Ohm/V	1	25,00	25,00
19	CALIBRADOR	(2) METÁLICO (A/N) (PLATEADO)	1	15,00	15,00
20	CALIBRADOR MÉTRICO	(83) METÁLICO (HEWLETT PACKARD) (PLATEADO)	1	19,00	19,00
21	CAUTÍN ELÉCTRICO	PLÁSTICO (WELLER) (N/N) (552) DE PISTOLA, DE 140/100 W	1	10,00	10,00
22	CELDA STANDARD	METÁLICO (NEWPORT INC) (A/N) (44) CATALOGO No. 100	2	10,00	20,00
23	COCHE TRANSPORTABLE	MADERA / METALICO (A/N) (A/N) (142) DE 2 TABLEROS, SUPERIOR DE MADERA TRIPLEX, E INFERIOR METÁLICO.	2	20,00	40,00
24	CONTADOR DE CORRIENTE	METÁLICO (AEG) (A/N) (197) ALTERNA 110 V, 10(20) A TIPO CG1	2	18,00	36,00
25	CONTADOR DE CORRIENTE	METÁLICO (A/N) (A/N) (194) TRIFÁSICO 121/210 V, TIPO HG20	1	18,00	18,00
26	CONTADOR DE CORRIENTE	METÁLICO (A/N) (A/N) (I96) TRIFÁSICO 210/120, 10 A, TIPO MG1	1	18,00	18,00
27	CONTADOR ELECTRÓNICO	(26) METÁLICO (HEWLETT PACKARD) (A/N)	1	54,00	54,00
28	DÉCADA CAPACITIVA	(500) METÁLICO (GENERAL RADIO) (A/N)	1	10,00	10,00
29	DÉCADA CAPACITIVA	METÁLICO (GENERAL RADIO) (A/N) (51) Tipo 1419-M	2	10,00	20,00
30	DÉCADA CAPACITIVA	(188) METÁLICO (HELETT PACKARD) (A/N)	5	10,00	50,00
31	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) (49) TIPO DK-40.1 uF S/N 50306	1	10,00	10,00
32	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) (49) TIPO DK-40.1 uF S/N 50307.	1	10,00	10,00
33	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) (49) TIPO DK-100.01 uF S/N 50380	1	10,00	10,00
34	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) (49)TIPO DK-100.01 uF S/N 50381	1	10,00	10,00

35	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) TIPO DK-5A S/N 50480	1	10,00	10,00
36	DÉCADA CAPACITIVA	METÁLICO (INDUSTRIAL INSTRUMENTS) (A/N) (49) TIPO DK-5A S/N 50259	1	10,00	10,00
37	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. a) TIPO RDA S/N 62549	1	10,00	10,00
38	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. a) TIPO RDA S/N 62587	1	10,00	10,00
39	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. a) Tipo RDA S/N 62588.	1	10,00	10,00
40	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. b) TIPO RDB S/N -58133.	1	10,00	10,00
41	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. b) TIPO RDB S/N 56841	1	10,00	10,00
42	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. b) TIPO RDB S/N 51248	1	10,00	10,00
43	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. b) TIPO RDB S/N 56830	1	10,00	10,00
44	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. c) TIPO RDC S/N 66167	1	10,00	10,00
45	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. c) TIPO RDC S/N 66238	1	10,00	10,00
46	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. c) TIPO RDC S/N 66280-FALTA 66278	1	10,00	10,00
47	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. d) TIPO CD A -2 S/N 63804	1	10,00	10,00
48	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. d) TIPO CD A -2 S/N 64116	1	10,00	10,00
49	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. d) TIPO CD A -2 S/N -64127	1	10,00	10,00
50	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. d) TIPO CD A -2 S/N -64128	1	10,00	10,00
51	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. d) TIPO CD A -2 S/N 64135	1	10,00	10,00
52	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD B -3 S/N 64259	1	10,00	10,00
53	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD B -3 S/N 64268	1	10,00	10,00
54	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD B -3 S/N -65502	1	10,00	10,00
55	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD B -3 S/N 65515	1	10,00	10,00
56	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD B -3 S/N-65875	1	10,00	10,00
57	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS e) TIPO CD C -3 S/N-64817	1	10,00	10,00
58	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD C -3 S/N-64822	1	10,00	10,00
59	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD C -3 S/N-64823	1	10,00	10,00
60	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD C -3 S/N-64824	1	10,00	10,00
61	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CD C -3 S/N-65283	1	10,00	10,00
62	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CDE S/N-65338	1	10,00	10,00
63	DÉCADA DE CONDENSADOR	METÁLICO (CORNELL DUBILIER) (A/N) (50) Y RESISTENCIAS. e) TIPO CDE S/N-65362	1	10,00	10,00
64	DÉCADA DE CONDENSADOR	(501) METÁLICO (HEATKIT) (A/N)	3	10,00	30,00
65	DÉCADA DE DIVISIÓN	METÁLICO (GENERAL RADIO) (A/N) (16) TIPO 1455-B	2	15,00	30,00
66	DÉCADA DE DIVISIÓN	METÁLICO (GENERAL RADIO) (A/N) (507) DE VOLTAJE TIPO 1454-AH	1	15,00	15,00
67	DÉCADA DE INDUCCIÓN	METÁLICO (MARCHESI) (A/N) (502) DE 0.1 mH A 1 mH MONTADA EN CAJA METÁLICA	9	15,00	135,00
68	DÉCADA DE RESISTENCIA	METÁLICO (GENERAL RADIO) (A/N) (47) TIPO 1432-T	6	10,00	60,00
69	DÉCADA INDUCTIVA	(21) METÁLICO (GENERAL RADIO) (A/N)	1	10,00	10,00
70	DÉCADA INDUCTIVA	METÁLICO (GENERAL RADIO) (A/N) (19) TIPO 1491G	2	10,00	20,00
71	DÉCADA RESISTIVA	METÁLICO (GENERAL RADIO) (A/N) (15) TIPO 1433 W	20	10,00	200,00

72	DÉCADA RESISTIVA	(78) METÁLICO (HICKOK) (A/N)	6	10,00	60,00
73	FRECUENCÍMETRO	PLÁSTICO (YEW) (A/N) (185) RPA	1	65,00	65,00
74	FUENTE DE CORRIENTE	PLÁSTICO (KEPCO) (A/N) (79)	1	58,00	58,00
75	FUENTE DE PODER	PLÁSTICO (UNIVERSAL LABORATORY) (A/N) (84) AC/DC	1	200,00	200,00
76	FUENTE DE PODER	PLÁSTICO (RFL INDUSTRIES) (A/N) (524) STANDARD CON CABLE SEPARADO	1	200,00	200,00
77	FUENTE DE PODER	PLÁSTICO (HELETT PACKARD) (A/N) (80) DC	1	200,00	200,00
78	FUENTE DE PODER	(87) PLÁSTICO (HELETT PACKARD) (A/N)	4	200,00	800,00
79	FUENTE DE PODER	PLÁSTICO (MARCHESI) (VERDE) (527) TRIPLE	7	200,00	1.400,00
80	FUENTE DE PODER	METÁLICO (OMEGA) (A/N) (565) VARIABLE, RANGO 0-20 V..2.5 A	5	200,00	1.000,00
81	FUENTE DE REFERENCIA	PLÁSTICO (FLUKE) (A/N) (39) STANDARD 110 V PARA DC TIPO 731B	1	180,00	180,00
82	FUENTE DE TRANSISTOR	(525) PLÁSTICO (HEATKIT) (A/N)	2	180,00	360,00
83	GALVANOMETRO	METÁLICO (LEEDS NORTHRUP) (A/N) (124) DE SUSPENSIÓN	1	80,00	80,00
84	GALVANOMETRO	METÁLICO (LEEDS NORTHRUP) (A/N) (7) dc	1	80,00	80,00
85	GALVANÓMETRO	PLÁSTICO (NEUBERGER) (A/N) (60) de 30-0 30	4	100,00	400,00
86	GALVANÓMETRO	METÁLICO (YEW) (A/N) (175) BALISTICO DC, G-3D	1	100,00	100,00
87	GALVANÓMETRO	METÁLICO (LEEDS NORTHRUP) (A/N) (123) BALISTICO	1	100,00	100,00
88	GALVANOMETRO DE AGUJA	(5) PLÁSTICO (LEEDS NORTHRUP) (A/N)	6	50,00	300,00
89	GALVANOMETRO ELECTRONICO	(523) PLÁSTICO (YEW YOKAGAWA E.W) (A/N)	2	50,00	100,00
90	GENERADOR DE BAJA FRECUENCIA	PLÁSTICO (HELETT PACKARD) (A/N) (19) DE CUADRO TRIANGULAR	1	530,00	530,00
91	GENERADOR DE FUNCIONES	(82) PLÁSTICO (HELETT PACKARD) (A/N)	2	530,00	1.060,00
92	GENERADOR DE FUNCIONES	(86) PLÁSTICO (HEWLETT PACKARD) (A/N)	3	530,00	1.590,00
93	GENERADOR DE FUNCIONES	PLÁSTICO (TEKTRONIX) (HABANO)	3	590,41	1.771,23
94	GENERADOR DE FUNCIONES	(564) PLÁSTICO (B & K) (A/N)	6	530,00	3.180,00
95	GENERADOR DE PULSOS	PLÁSTICO (WESTINNGHOUSE) (A/N) (132) TIPO RELUCTANCIA CON ACCESORIO DE MONTAJE	1	590,41	590,41
96	GENERADOR DE TACÓMETRO	(23) PLÁSTICO (HEWLETT PACKARD) (A/N)	1	0,10	0,10
97	GRAFIZADOR DE CAMPO	PLÁSTICO (SUNSHINE) (A/N) (108) con pantográfo	1	250,00	250,00
98	INDICADOR DE FRECUENCIA DE VELOCIDAD	PLÁSTICO (WESTINNGHOUSE) (A/N) (115) TIPO VC-842, STYLE FE-35487-8	1	150,00	150,00
99	INDICADOR DE FRECUENCIA DE VELOCIDAD	PLÁSTICO (WESTINNGHOUSE) (A/N) (114) FE-35487-N3-9, 1200 FPM, TIPO FX382	1	150,00	150,00
100	INDUCTANCIA VARIABLE	(508) PLÁSTICO (GENERAL RADIO) (A/N)	1	15,00	15,00
101	INDUCTANCIA VARIABLE	PLÁSTICO (GENERAL RADIO) (A/N) (33) TIPO 107 K	2	15,00	30,00
102	INDUCTOR	PLÁSTICO (LEEDS NORTHRUP) (A/N) (36) MUTUA STANDARD CAT. 1540	1	10,00	10,00
103	INDUCTOR	PLÁSTICO (SPRAGUE) (A/N) (35) DECADA, TIPO 850 WA1 0-01H	7	10,00	70,00
104	INDUCTOR VARIABLE	PLÁSTICO (GENERAL RADIO) (A/N) (39) TIPO 107 J	1	10,00	10,00
105	INDUCTOR VARIABLE	PLÁSTICO (GENERAL RADIO) (A/N) (40) TIPO 107 M	2	10,00	20,00
106	INDUCTOR VARIABLE	PLÁSTICO (GENERAL RADIO) (A/N) (34) TIPO 107 N	2	10,00	20,00
107	INDUCTOR VARIABLE	PLÁSTICO (GENERAL RADIO) (A/N) (38) TIPO 107 L	2	10,00	20,00
108	INTERFASE	PLÁSTICO (TEKTRONIX) (A/N) INSTALADO EN EL OSCILOSCOPIO. S/N B092883	1	285,36	285,36
109	INTERFASE	PLÁSTICO (TEKTRONIX) (A/N) INSTALADO EN EL OSCILOSCOPIO. S/N B094636	1	285,36	285,36
110	LLAVE DE CUCHILLA	(12) METÁLICO (LEEDS NORTHRUP) (A/N)	3	10,00	30,00
111	LLAVE DE DOBLE CONTACTOR	(11) METÁLICO (LEEDS NORTHRUP) (A/N)	3	10,00	30,00
112	LLAVE DE MONOCONTACTO	(13)METÁLICO (LEEDS NORTHRUP) (A/N)	3	10,00	30,00

113	MÁQUINA DE ESCRIBIR	METÁLICO (RATH GERBER) (A/N) (216) MECÁNICA CON CARRO DE 15"	1	35,00	35,00
114	MEDIDOR	PLÁSTICO (WESTINNGHOUSE) (A/N) (220) KWH. TIPO 510C904G00,,	1	150,00	150,00
115	MEDIDOR	PLÁSTICO (WESTINNGHOUSE) (A/N) (219). MONOFÁSICO, STYLE 510C906G10, TIPO D3S	1	150,00	150,00
116	MEDIDOR	PLÁSTICO (WESTINNGHOUSE) (A/N) (121) 240 V TIPO D2A	2	150,00	300,00
117	MEDIDOR	PLÁSTICO (WESTINNGHOUSE) (A/N) (120) POLIFÁSICOS TIPO D2A-8 ROTO	2	150,00	300,00
118	MEDIDOR	METÁLICO (YEW) (A/N) (186) UNIVERSAL DE FACTOR DE POTENCIA TIPO DPPU	1	150,00	150,00
119	MEDIDOR	METÁLICO (YOKOGAWA) (A/N) (54) DE FACTOR DE POTENCIA 110 V/1A TIPO 2147	1	150,00	150,00
120	MEDIDOR DE COS P	PLÁSTICO (YEW) (A/N) (528) 0.2/1 A	10	117,00	1.170,00
121	MEDIDOR DE ENERGÍA	PLÁSTICO (KDK) (ABANO) (215) PATRON MONOFÁSICO	1	117,00	117,00
122	MEDIDOR DE FACTOR	PLÁSTICO (YOKOGAWA) (A/N) (55) DE POTENCIA 110 V/5A TIPO 2147	2	117,00	234,00
123	MEDIDOR DE FACTOR	PLÁSTICO (YEW) (A/N) (530) DE POTENCIA (Cos P), 1/5 A	5	117,00	585,00
124	MEDIDOR DE POTENCIA	PLÁSTICO (CELCA) (A/N) (529) 5 A, ESCALA 0.5-1-05, TRIFÁSICO	1	117,00	117,00
125	MICROAMPERÍMETRO	PLÁSTICO (NEUBERGER) (A/N) (67) AC 600 uA	1	250,00	250,00
126	MICROAMPERÍMETRO	PLÁSTICO (NEUBERGER) (A/N) (70) CA 0-100uA	1	250,00	250,00
127	MICROAMPERÍMETRO	PLÁSTICO (NEUBERGER) (A/N) (71) CC 10 uA	2	250,00	500,00
128	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-10 uA, CON CAJA	5	250,00	1.250,00
129	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-20 uA, CON CAJA	1	250,00	250,00
130	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-50 uA, CON CAJA	1	250,00	250,00
131	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-50 uA	2	250,00	500,00
132	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-100 uA, CON CAJA	1	250,00	250,00
133	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) CD 0-200 uA, CON CAJA	3	250,00	750,00
134	MILIAMPERÍMETRO	PLÁSTICO (A/N) (A/N) (174) TIPO SPFB	2	100,00	200,00
135	MILIAMPERÍMETRO	PLÁSTICO (NORMA) (A/N) (66) CC.	1	100,00	100,00
136	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-1 mA CON CAJAS	1	100,00	100,00
137	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N)	1	100,00	100,00
138	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-5 mA	4	100,00	400,00
139	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-3 mA	4	100,00	400,00
140	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-10 mA, CON CAJAS	5	100,00	500,00
141	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-20 mA, CON CAJAS	1	100,00	100,00
142	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-50 mA, CON CAJAS	1	100,00	100,00
143	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-500 mA, CON CAJAS	4	100,00	400,00
144	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-200 mA, CON CAJA	3	100,00	300,00
145	MILIAMPERÍMETRO ALTA FRECUENCIA	PLÁSTICO (A/N) (A/N) (253) CA,100/200/500/1000 mA TIPO 2016	2	200,00	400,00
146	MILIAMPERÍMETRO ALTA FRECUENCIA	PLÁSTICO (A/N) (A/N) (252) CA 20/50/100/200 mA TIPO 2016	4	200,00	800,00
147	MILIAMPERÍMETRO ALTA FRECUENCIA	METÁLICO (A/N) (A/N) (251) CA. 5/10/20/50 mA, TIPO 2016	4	200,00	800,00
148	MILIAMPERÍMETRO ALTA SENSIBILIDAD	PLÁSTICO (SINGER) (A/N) (74) DC.	1	200,00	200,00
149	MILIAMPERÍMETRO DE CA DE TABLERO	PLÁSTICO (YEW) (A/N) (76) 1 A.	5	200,00	1.000,00
150	MILIAMPERÍMETRO DE CA DE TABLERO	PLÁSTICO (YEW) (A/N) (60) 2142, 10 mA	2	200,00	400,00
151	MILIAMPERÍMETRO DE CA DE TABLERO	PLÁSTICO (YEW) (A/N) (59) 2144 100mA	2	200,00	400,00
152	MILIAMPERÍMETRO DE CC DE TABLERO	PLÁSTICO (YEW) (A/N) (67) 1 mA	1	200,00	200,00
153	MILIAMPERÍMETRO DE CC DE TABLERO	PLÁSTICO (YEW) (A/N) (68) 5 MA TIPO 2141	2	200,00	400,00

154	MILIAMPERÍMETRO DE CC DE TABLERO	PLÁSTICO (YEW) (A/N) (69) 500 V, 10 mA, TIPO	4	200,00	800,00
155	MILIAMPERÍMETRO DE CC DE TABLERO	PLÁSTICO (YEW) (A/N) (65) 100 mA TIPO 2141	2	200,00	400,00
156	MILIÓMETRO	(84) PLÁSTICO (HEWLETT PACKARD) (A/N)	1	118,00	118,00
157	MILIVOLTÍMETRO	PLÁSTICO (SINGER) (A/N) (81) Patron DC	1	210,00	210,00
158	MILIVOLTÍMETRO	PLÁSTICO (PRI NEUBERGER) (A/N) (52) DC. 0.80mV	4	100,00	400,00
159	MODEN EXTERNO	PLÁSTICO (EMERSON) (A/N) (568) SERIAL, 2400 BAUDIOS, TIPO HAYES COMPATIBLE	1	10,08	10,08
160	MULTÍMETRO	(99) PLÁSTICO (AVOMETER) (A/N)	1	50,00	50,00
161	MULTÍMETRO	PLÁSTICO (PHILIPS) (A/N) (40) ADV, TIPO 2412/02, No 9447-024-12021	5	50,00	250,00
162	MULTÍMETRO	PLÁSTICO (PHILIPS) (A/N) (41) ELECTRÓNICOS TIPO PM2503/02 Nº 9447-025-03021	5	50,00	250,00
163	MULTÍMETRO	PLÁSTICO (TRIPLETT) (A/N) (88) DE SUSPENSIÓN CON BANDA	6	50,00	300,00
164	MULTÍMETRO	(42) PLÁSTICO (SIMPSON) (A/N)	8	50,00	400,00
165	MULTÍMETRO	PLÁSTICO (FLUKE) (A/N) (32) DIGITAL DE 3-1/2 DÍGITOS CON SALIDA A IMPRESORA	1	180,00	180,00
166	MULTÍMETRO	PLÁSTICO (HICKOK) (A/N) (77) DIGITAL	4	81,00	324,00
167	MULTÍMETRO	PLÁSTICO (FLUKE) (A/N) (38) de 4 1/2 DÍGITOS	6	81,00	486,00
168	MULTÍMETRO	/531) PLÁSTICO (KEITLEY) (A/N)	8	35,00	280,00
169	MULTÍMETRO	PLÁSTICO (FLUKE) (A/N) (31) DIGITAL	4	35,00	140,00
170	MULTÍMETRO	PLÁSTICO (HEWLETT PACKARD) (A/N) (35) DIGITAL	10	35,00	350,00
171	MULTÍMETRO	METÁLICO (SIEMENS MULTIZETS) (A/N) (89) PARA AC/CD	3	35,00	105,00
172	OSCILADOR DE AUDIO	(20) PLÁSTICO (HEWLETT PACKARD) (A/N)	4	140,00	560,00
173	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (HABANO) DOS PUNTAS DE PRUEBA	2	1.463,72	2.927,44
174	OSCILOSCOPIO	(187)PLÁSTICO (HEWLETT PACKARD) (CREMA)	4	540,00	2.160,00
175	OSCILOSCOPIO	PLÁSTICO (PHILIPS) (CREMA) (532) DE 2 CANALES (DOBLE TRAZO) TIPO PM3211	6	540,00	3.240,00
176	OSCILOSCOPIO	(533) PLÁSTICO (HEWLETT PACKARD) (CREMA)	2	540,00	1.080,00
177	OSCILOSCOPIO	(33) PLÁSTICO (HEWLETT PACKARD) (CREMA)	2	540,00	1.080,00
178	REGLETA TOMACORRIENTE	(169) PLÁSTICO (A/N) (A/N)	28	10,00	280,00
179	REGULADOR DE VOLTAJE	METÁLICO-MADERA (SOLA ELECTRONICO) (A/N)	1	25,00	25,00
180	REGULADOR DE VOLTAJE	METÁLICO-MADERA (SOLA ELECTRONICO) (A/N) (111) 118 V , 2	1	25,00	25,00
181	REOSTATO	METÁLICO (YEW) (A/N) (510) DE 10Ohm, 4 A	1	15,00	15,00
182	REOSTATO	METÁLICO (A/N) (A/N) (122) a) 5 DE 5700 Ohm, 27 A,	14	15,00	210,00
183	REOSTATO	METÁLICO (A/N) (A/N) 5 DE 710 Ohm, 0.77 A,	5	15,00	75,00
184	REOSTATO	METÁLICO (A/N) (A/N) DE 360 Ohm 1.1 A.	1	15,00	15,00
185	REOSTATO	METÁLICO (A/N) (A/N) (122) DE 33 Ohm 44/31 A.	18	15,00	270,00
186	REOSTATO TUBULAR	METÁLICO (YEW) (A/N) (511) 1400 Ohm, 0.35 A	4	26,00	104,00
187	REOSTATO TUBULAR	METÁLICO (YEW) (A/N) (512) 600 Ohm, 0.5 A	22	26,00	572,00
188	REOSTATO TUBULAR	METÁLICO (YEW) (A/N) (513) 170 Ohm, 1 A	14	26,00	364,00
189	REOSTATO TUBULAR	MADERA / METALICO (SIEMENS) (A/N) (514) DE 0-53 Ohm, 3.2 A TIPO 2GA 2447-1T	5	26,00	130,00
190	REOSTATO TUBULAR	METÁLICO (SIEMENS) (A/N) (515) DE 0-86 Ohm, 2.7 A TIPO 2GA 2448-1S	2	26,00	52,00
191	RESISTENCIA	METÁLICO (SIEMENS) (A/N) (90) DE 30 A	1	10,00	10,00
192	RESISTENCIA	METÁLICO (GENERAL RADIO) (A/N) (516) DE PRESICIÓN CAT. 1440-9671	5	10,00	50,00
193	RESISTENCIA	METÁLICO (GENERAL RADIO) (A/N) (44) FIJAS de 10 Oh, tipo 500 B	19	10,00	190,00
194	RESISTENCIA	METÁLICO (HEWLETT PACKARD) (A/N) (43) Shunt.- de 0.1 Oh. Mod. 11029 A	4	10,00	40,00
195	SECUENCIMETRO	METÁLICO (A/N) (A/N) (214) rango de voltaje 100-500, 3 fases	2	10,00	20,00
196	SHUNT UNIVERSAL	METÁLICO (YEW) (A/N) (177) Tipo GS-1A	1	30,00	30,00
197	SIMULADOR TRIFÁSICO DE PRUEBA	PLÁSTICO (KDK) (A/N) (214) 127/220V	1	52,00	52,00

198	TACÓMETRO	METÁLICO (HEWLETT PACKARD) (A/N) (6) Optico	1	130,00	130,00
199	TALADRO	(1) PLÁSTICO (SAFETY) (A/N)	1	45,00	45,00
200	TELÉFONO DE MESA	(259) PLÁSTICO (ERISCSSON) (PLOMO)	1	10,00	10,00
201	TELESCOPIO	METÁLICO (LEEDS NORTHRUP) (A/N) (15) de escala galvanómetro	2	50,00	100,00
202	TRANSDUCTOR	METÁLICO (WESTINNGHOUSE) (A/N) (131) de corriente teleductor	1	8,00	8,00
203	TRANSDUCTOR	METÁLICO (WESTINNGHOUSE) (A/N) (133) de frecuencia	1	11,00	11,00
204	TRANSDUCTOR	(118) METÁLICO (WESTINNGHOUSE) (A/N)	1	8,00	8,00
205	TRANSFORMADOR DE CORRIENTE	METÁLICO (SINGER) (A/N) (82) 5 VA, Tipo 1	1	35,00	35,00
206	TRANSFORMADOR DE CORRIENTE	METÁLICO (CENCO) (A/N) (112) De 579 Ohm a 75 Ohm Cat. No. 78535	1	35,00	35,00
207	VATÍMETRO	METÁLICO (NORMA) (A/N) (76) 5.20 A, 130-280-520 V	2	250,00	500,00
208	VATÍMETRO	METÁLICO (SINGER) (A/N) (86) 37.5/75/150 W	1	250,00	250,00
209	VATÍMETRO	METÁLICO (NORMA) (A/N) (77) 0.25-0.5 A. 130-260-520 V	2	250,00	500,00
210	VATÍMETRO	MADERA TRIPLEX (NORMA) (A/N) (75) 1-5A 130-260-520 V	8	250,00	2.000,00
211	VATÍMETRO	METÁLICO (NORMA) (A/N) (79) AC 0.5-1 A, 6-12-30-60 V	2	250,00	500,00
212	VATÍMETRO	METÁLICO (YOKOGAWA) (A/N) (57) 110 V .5 A Tipo 2146	4	250,00	1.000,00
213	VATÍMETRO	METÁLICO (YEW) (A/N) (535) CC/CA 120/240V.0.2/A	8	250,00	2.000,00
214	VATÍMETRO	METÁLICO (A/N) (A/N) (248) portatil standard CA/CC, 0.21/1 A, 120/240 V , tipo 204101	3	250,00	750,00
215	VATÍMETRO DE EFECTO	METÁLICO (WESTINNGHOUSE) (A/N) (119) HALL AC tipo KP 241 Style FE-35487-10	1	250,00	250,00
216	VATÍMETRO MONOFÁSICO	METÁLICO (YEW) (A/N) (97) ,tipo DPB-IWL, con estuche	1	60,00	60,00
217	VATÍMETRO MONOFÁSICO	METÁLICO (YEW) (A/N) (52) CC/CA.0.2/1A,120/240V. TIPO 2041	4	100,00	400,00
218	VATÍMETRO MONOFÁSICO	METÁLICO (YEW) (A/N) (47) portatiles CA 02/1 A 120/240 V.0.2 FP Tipo 2041	2	100,00	200,00
219	VATÍMETRO MONOFÁSICO	METÁLICO (YEW) (A/N) (49) portatil CA 120/240 V, 1/5 A, 0.2 FP	4	100,00	400,00
220	VATÍMETRO MONOFÁSICO	METÁLICO (YEW) (A/N) (51) portatil CC/CA, 120/240 V. 1/5 A Tipo 2041.	4	100,00	400,00
221	VATÍMETRO PATRÓN	METÁLICO (SINGER) (A/N) (87) 150/300/600 W	1	100,00	100,00
222	VATÍMETRO PATRÓN	METÁLICO (SINGER) (A/N) (85) DC 500/1000/2000 W	1	100,00	100,00
223	VATÍMETRO PATRÓN	METÁLICO (SINGER) (A/N) (80) DC/AC 110/220 V, 75/150/300 W	1	100,00	100,00
224	VATÍMETRO POLIFÁSICO	METÁLICO (YEW) (A/N) (184) . tipo DPW-3	1	100,00	100,00
225	VATÍMETRO ROTATIVO	METÁLICO (A/N) (A/N) (222) patrón trifásico.	1	100,00	100,00
226	VATÍMETRO STANDARD	METÁLICO (A/N) (A/N) (249) portatil CA. 0.2/1 A 120/240 V tipo 2041-11	3	100,00	300,00
227	VATÍMETRO TRIFÁSICO	METÁLICO (YEW) (A/N) (48) 5/25 A, 120/240 V, tipo 2042	2	100,00	200,00
228	VATÍMETRO TRIFÁSICO	METÁLICO (YEW) (A/N) (536) 120/240 V, 1/5 A	8	161,00	1.288,00
229	VATÍMETRO TRIFÁSICO	METÁLICO (YEW) (A/N) (53) 0.2/1 A, 120/240 V Tipo 2042	4	161,00	644,00
230	VATÍMETRO TRIFÁSICO	METÁLICO (YEW) (A/N) (46) 1/5 A tipo 2042	4	161,00	644,00
231	VATÍMETRO TRIFÁSICO	METÁLICO (A/N) (A/N) (250) portatiles standard, 0.2/1 A , 120/240 V, tipo 2042	2	161,00	322,00
232	VATÍMETRO TRIFÁSICO DE TABLERO	METÁLICO (YOKOGAWA) (A/N) (56) 110V/5A, tipo 2145	4	161,00	644,00
233	VOLTÍMETRO	METÁLICO (YEW) (A/N) (173) AC, tipo SPFB	2	100,00	200,00
234	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (55) AC/DC, 130/260/520.	5	100,00	500,00
235	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (58) AC/DC 65/130-260 V	19	100,00	1.900,00
236	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (59) AC/DC 6-30-60 V	4	100,00	400,00
237	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (537) 65/130-260	1	100,00	100,00
238	VOLTÍMETRO	MADERA TRIPLEX (YEW) (A/N) (96)	1	100,00	100,00
239	VOLTÍMETRO	METÁLICO (YEW) (A/N) (98) CA tipo TPFB para el marco EPNSTEIN 7 R:N	1	100,00	100,00
240	VOLTÍMETRO	METÁLICO (YEW) (A/N) (74) CA 300V tipo 2142	2	100,00	200,00

241	VOLTÍMETRO	METÁLICO (NEUBERGER) (A/N) (57) A. C 150 V,. con caja de madera	5	100,00	500,00
242	VOLTÍMETRO	METÁLICO (YEW) (A/N) (172) DC, 1/3/10/30 V,tipo MP	12	100,00	1.200,00
243	VOLTÍMETRO AMPERÍMETRO	METÁLICO (EICO) (A/N) (101) tipo 72011	2	100,00	200,00
244	VOLTÍMETRO DE CA DE TABLERO	METÁLICO (YEW) (A/N) (70) 10 V Tipo 2142	5	100,00	500,00
245	VOLTÍMETRO DE CA DE TABLERO	METÁLICO (YEW) (A/N) (72) 100V, Tipo 2142	2	100,00	200,00
246	VOLTÍMETRO DE CA DE TABLERO	METÁLICO (YEW) (A/N) (73) 150V, tipo 2142	2	100,00	200,00
247	VOLTÍMETRO DE CA DE TABLERO	METÁLICO (YEW) (A/N) (71) 30V, Tipo 2142	5	100,00	500,00
248	VOLTÍMETRO DE CC DE TABLERO	METÁLICO (YEW) (A/N)	1	100,00	100,00
		TOTAL			76.989,98

LABORATORIO DE DISEÑO ELECTRÓNICO

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ATENUADOR	MELAMINICO (MARCONI INSTRUMENT) (A/N)	1	100,00	100,00
2	CAJA PORTAINSTRUMENTOS	METÁLICO (TRIPLETT) (A/N)	8	10,00	80,00
10	CAJA PORTAINSTRUMENTOS	METÁLICO (A/N) (A/N) DE 0.80 X 0.39 X 0.13 Cm	2	8,00	16,00
12	CAUTÍN ELÉCTRICO	PLÁSTICO (WELLER) (NEGRO) DE 100 W TIPO PISTOLA	1	7,00	7,00
13	COMPUTADOR	PLÁSTICO (IBM) (BLANCO)	1	430,00	430,00
14	COMPUTADOR	CLON	1	890,00	890,00
14	ESTABILIZADOR DE VOLTAJE	METÁLICO (PHILIPS) (A/N)	1	33,00	33,00
15	FUENTE DE PODER	METÁLICO (MARCHESI) (A/N)	2	220,00	440,00
17	FUENTE DE PODER	METÁLICO (VIZ) (A/N) VARIABLE AC 150V	1	320,00	320,00
18	FUENTE DE PODER	METÁLICO (HEAT ZENIT) (A/N) VARIABLE TRIPLE DC, 5-20 V	2	320,00	640,00
20	GABINETE	METÁLICO (EQUIPTO) (A/N)	1	15,00	15,00
21	GENERADOR DE SEÑALES	METÁLICO (WAVETEK) (A/N)	1	530,00	530,00
22	GENERADOR DE SEÑALES	METÁLICO (HEWLETT PACKARD) (A/N)	1	530,00	530,00
23	IMPRESORA	PLÁSTICO (EPSON) (BLANCO)	1	88,00	88,00
24	MEDIDOR	METÁLICO (GENERAL RADIO) (A/N) DE MAGNITUDES ELECTRICAS RLC	1	239,00	239,00
25	MEDIDOR DE INTENSIDAD DE LUZ	PLÁSTICO (EXTECH) (NEGRO) digital	1	235,00	235,00
26	MEDIDOR DE INTENSIDAD DE SONIDO	PLÁSTICO (EXTECH) (NEGRO)	1	306,00	306,00
27	MEDIDOR DE POTENCIA	METÁLICO (GENERAL RADIO) (A/N)	1	180,00	180,00
28	MEDIDOR DE POTENCIA	METÁLICO (MARCONI INSTRUMENT) (A/N) DE R. F	1	150,00	150,00
29	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0-100 uA	3	250,00	750,00
32	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0 -20 mA	1	250,00	250,00
33	MILIAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) DC 0 -50 mA	4	250,00	1.000,00
37	MULTÍMETRO	METÁLICO (METRICS) (A/N) ANALOGO	1	80,00	80,00
38	MULTÍMETRO	METÁLICO (KEITHLEY) (A/N) DIGITAL	2	35,00	70,00
40	MULTÍMETRO VOLTÍMETRO	PLÁSTICO (LEADER) (NEGRO) DIGITALES	2	100,00	200,00
42	OSCILADOR	PLÁSTICO (HEWLETT PACKARD) (A/N)	1	160,00	160,00
43	OSCILADOR	PLÁSTICO (OLTRONIX) (A/N) 1 MALO	2	230,00	460,00
45	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL)	4	2.532,62	10.130,48
49	PUENTE	METÁLICO (A/N) (A/N) AMECO SWR O MEDIDOR DE ONDA ESTACIONARIA	1	350,00	350,00
50	PUNCH	METÁLICO (GREENLE) (A/N) 1 1/2"	5	10,00	50,00
51	PUNCH	METÁLICO (GREENLE) (A/N) 1 1/8"	3	10,00	30,00
52	PUNCH	METÁLICO (GREENLE) (A/N) 1 1/4"	1	10,00	10,00
56	PUNCH	METÁLICO (GREENLE) (A/N) 1"	1	10,00	10,00
58	PUNCH	METÁLICO (GREENLE) (A/N) 3/4"	1	10,00	10,00
59	PUNCH	METÁLICO (GREENLE) (A/N) 5/8"	1	10,00	10,00
62	REGLETA TOMACORRIENTE	PLÁSTICO (A/N) (PLOMO)	7	10,00	70,00

69	TALADRO	PLÁSTICO (STANLEY) (A/N)	1	180,00	180,00
70	TARRAJA	HIERRO (A/N) (A/N) MARCA ACE	1	20,00	20,00
71	UNIDAD DE ANÁLISIS	METÁLICO (A/N) (A/N) O PRUEBAS LOGICAS CON 1 PULSADOR LOGICO	1	375,00	375,00
72	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) DE DOBLE CANAL	1	370,00	370,00
73	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) DE DOBLE CANAL	1	370,00	370,00
74	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) VERTICALES DE DOS CANALES	1	330,00	330,00
75	UNIDAD,BASE DE TIEMPO	METÁLICO (TEKTRONIX) (A/N)	1	174,00	174,00
		TOTAL			20.588,48

LABORATORIO DE CONTROL INDUSTRIAL

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	AUTOTRANSFORMADOR	METÁLICO (POWERSTAT) (A/N) VARIABLE TIPO 1156-B (73)	1	200,00	200,00
2	AUTOTRANSFORMADOR	METÁLICO (POWESTAR) (A/N) VARIABLE TRIFASICO 240/280 V. 22 A, 10.7 KVA TIPO 136B-3(75)	1	321,75	321,75
3	BLOQUE DE DISTRIBUCIÓN	METÁLICO (FESTO) (A/N) TIPO FR-8-1/8(83)	1	669,90	669,90
4	CAJA DE ENSEÑANZA	MADERA (SIMATIC) (A/N) (76)	1	150,00	150,00
5	COMPRESOR DE AIRE	HIERRO (THOMAS) (VERDE) AÑO 1974 KARGARD CON MOTOR EMERSON DE 1 1/2 HP MODELO K563XCDR-2149 (35)	1	450,75	450,75
6	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) TIPO 486DX4-100 (58)	2	425,00	850,00
7	COMPUTADOR	PLÁSTICO (PREMIO) (BLANCO) (81)	2	425,00	850,00
8	CONTACTOR	PLÁSTICO (LOVATO) (A/N) TIPO B9 (39)	1	140,00	140,00
9	CONTACTOR	PLÁSTICO (LOVATO) (A/N) TIPO C4 (25)	1	140,00	140,00
10	CONTACTOR	PLÁSTICO (LOVATO) (A/N) TIPO B12 (13)	4	140,00	560,00
11	CONTACTOR	PLÁSTICO (LOVATO) (A/N) TIPO C4 (25)	3	140,00	420,00
12	CONTACTOR	PLÁSTICO (LOVATO) (A/N) TIPO B9 (6)	2	140,00	280,00
13	CONTACTOR	PLÁSTICO (AEG) (A/N) 5 LS 36/L 44 TKS-50/500A: 5 LS 32/L 40 TKS-32/500 A (68)	10	140,00	1.400,00
14	CONTACTOR	PLÁSTICO (AEG) (A/N) 8 TIPO LS6/L 11.22-10: 2 TIPO L 14.11-Tth 30 A (69)	10	140,00	1.400,00
15	ELECTROVÁLVULA	METÁLICO (A/N) (A/N) TIPO MFH-3M5(84)	4	98,67	394,68
16	ELECTROVÁLVULA	METÁLICO (A/N) (A/N) DE IMPULSOS TIPO JMFH-5-1/8(87)	2	130,00	260,00
17	ENTENALLA	HIERRO (WABECO) (AZUL) (31)	1	159,00	159,00
18	EQUIPO DE DEMOSTRACIÓN	METÁLICO (FESTO) (A/N) EXPERIMENTAL (24)	1	128,00	128,00
19	EQUIPO EDUCATIVO PARA LA ENSEÑANZA	METÁLICO (MECKMAN) (A/N) DE CONTROL ELECTRICO Y NEUMATICO(78)	1	53,72	53,72
20	EQUIPO NEUMÁTICO	METÁLICO (ALECOOP) (A/N) DIGITAL (27)	1	192,00	192,00
21	EQUIPO NEUMÁTICO	METÁLICO (ALECOOP) (A/N) ELECTRONEUMATICO (28)	1	192,00	192,00
22	IMPRESORA	PLÁSTICO (EPSON) (BLANCO) 132 COLUMNAS. (46)	1	35,23	35,23
23	INTERFASE	CAUCHO (ALLEN BRADLEY) (A/N) PARA LA CONEXION PLC Y COMPUTADOR CAT. 1747-PIC (43)	1	158,90	158,90
24	INTERFASE	CAUCHO (ALLEN BRADLEY) (PLOMO) (51)	1	140,00	140,00
25	INTERRUPTOR DE LLAVE	PLÁSTICO (ERSCE) (A/N) DE 2 POSICIONES (38)	1	48,00	48,00
26	MÓDULO ACOPLADOR	PLÁSTICO (ALLEN BRADLEY) (A/N) PARA P.L.C. CAT. 1747 AIC (55)	1	20,34	20,34
27	MÓDULO ANÁLOGO	PLÁSTICO (A/N) (NEGRO) PARA P.L.C. CAT. 1746-NIO41 (54)	1	61,72	61,72
28	MOTOR	HIERRO (A/N) (A/N) DE 04 HP, TIPO NV71A 4 (36)	2	1.320,00	2.640,00
29	MOTOR	HIERRO (A/N) (A/N) DE 06 HP', TIPO MV 71B 4 (37)	3	1.320,00	3.960,00
30	MOTOR DE INDUCCIÓN	HIERRO (LOGICAL DEVICES) (A/N) 1730/860 rpm 0.75 HP(80)	1	1.320,00	1.320,00
31	MOTOR TRIFÁSICO DE JAULA	HIERRO (ELNOR) (A/N) 1730 rpm	1	1.320,00	1.320,00

32	MULTÍMETRO	PLÁSTICO (HUNG CHANG) (NEGRO) (40)	2	117,75	235,50
33	P.L.C.	PLÁSTICO (ALLEN BRADLEY) (NEGRO) (41)		750,00	0,00
34	P.L.C.	PLÁSTICO (ALLEN BRADLEY) (NEGRO) CAT. 1747-L20A (50),	2	750,00	1.500,00
35	P.L.C.	PLÁSTICO (ALLEN BRADLEY) (NEGRO) CONTROLADOR LOGICO (56)	1	750,00	750,00
36	PULSADOR	PLÁSTICO (ERSCE) (A/N) TIPO C 11 (17)	6	11,70	70,20
37	PULSADOR	METÁLICO (KLOCKMER MOLLER) (A/N) TIPO VDE-0660 (64)	2	9,75	19,50
38	PULSADOR	PLÁSTICO (EGA) (A/N) TIPO 5002(65)	14	9,75	136,50
39	RELE CÍCLICO	PLÁSTICO (AICO) (A/N) TIPO RTC2, 120 V AC, 5A (29)	1	36,50	36,50
40	RELE DE TIEMPO	PLÁSTICO (SIEMENS) (NEGRO) TIPO 20 7PR32024GF DE 0.15" /60 (32)	2	36,50	73,00
41	RELE DE TIEMPO	PLÁSTICO (SIEMENS) (NEGRO) TIPO 7PV14645GG (33)	5	67,50	337,50
42	RELE DE TIEMPO	PLÁSTICO (A/N) (A/N) ON DELAY CON MOTOR, 4 TIPO ZR 719; 1 TIPO ZR 720 (71)	5	67,50	337,50
43	RELE DE VOLTAJE	PLÁSTICO (AICO) (NEGRO) (12)	1	67,50	67,50
44	RELE NEUMÁTICO	METÁLICO (A/N) (A/N) DE TIEMPO, 220 V TIPO VZPR211(74)	2	92,00	184,00
45	RELE ON DELAY	PLÁSTICO (AICO) (NEGRO) 120/220 V (11)	2	107,30	214,60
46	RELE TÉRMICO	PLÁSTICO (LOVATO) (NEGRO) RC-22 (14)	2	195,00	390,00
47	RELE TÉRMICO	PLÁSTICO (AGUT) (A/N) TIPO RIK1-2-6 REG. 2-3.2A (63)	2	95,00	190,00
48	RELE TÉRMICO	PLÁSTICO (AGUT) (A/N) TERMICO DIFERENCIAL TIPO RIK 1-1-3 REG 1-1.6A (62)	4	95,00	380,00
49	RELE TÉRMICO	METÁLICO (AGUT) (A/N) TIPO RIK 1-5-5 REG 4.2.-6.7 A (66)	3	95,00	285,00
50	RELE TÉRMICO	METÁLICO (AGUT) (A/N) TIPO RIK 1.13, REG. 10.16 (67)	3	95,00	285,00
51	SCANNER	PLÁSTICO (ARTEC ASE) (A/N) (82)	1	94,98	94,98
52	SELECTOR	PLÁSTICO (ERSCE) (A/N) (23)	1	18,50	18,50
53	SELECTOR	PLÁSTICO (ERSCE) (A/N) (22)	2	18,50	37,00
54	SENSOR	METÁLICO (A/N) (A/N) TIPO SMED-1-LED-24 B(85)	4	7,88	31,52
55	SENSOR DE NIVEL	METÁLICO (LOVATO) (A/N) TIPO LV2 (15)	1	7,88	7,88
56	SENSOR FOTOELÉCTRICO	METÁLICO (PEXTRON) (A/N) TIPO VRF 3121 (26)	2	7,88	15,76
57	TALADRO	PLÁSTICO (A/N) (AMARILLO) (30)	1	75,00	75,00
58	TARJETA MÓDULO INTERFASE	PLÁSTICO (A/N) (A/N) PC-DH-485, CAT. 1784-KR INSTALADA EN EL COMPUTADOR PREMIO ORD. 58 (53)	1	164,85	164,85
59	VÁLVULA	METÁLICO (A/N) (A/N) DE IMPULSOS TIPO JMFH-5-1/8(86)	1	179,80	179,80
60	VÁLVULA DE RODILLO	HIERRO (FESTO) (A/N) 3/2 TIPO R-3-M5 (60)	1	96,80	96,80
61	VÁLVULA DE RODILLO	METÁLICO (A/N) (A/N) TIPO 4938(88)	2	96,80	193,60
		TOTAL			25.123,98

LABORATORIO DE CONTROL ELECTRÓNICO DE POTENCIA

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	AMPERÍMETRO	METÁLICO (TRIPLETT) (PLOMO) (140) DC, 0-5	1	100,00	100,00
2	AMPERÍMETRO	METÁLICO (TRIPLETT) (PLOMO) (145) DC 0-5	1	100,00	100,00
3	AMPERÍMETRO	METÁLICO (TRIPLETT) (PLOMO) (163) DC 0-1 A	2	115,00	230,00
4	AMPERÍMETRO	METÁLICO (TRIPLETT) (PLOMO) (86) CD DE 0-1 A	2	116,00	232,00
5	AMPERÍMETRO	METÁLICO (TRIPLETT) (NEGRO) (88) DC DE 0.10 A (1 CAMBIADO ESCALA A 20 A EN LA FUENTE DC Y 1 EN EL CONTROL DE MOTOR DC.	2	218,00	436,00
6	AMPERÍMETRO	PLÁSTICO (TRIPLETT) (NEGRO) (87) DC DE 0.5 A	2	197,00	394,00
7	AMPERÍMETRO	PLÁSTICO (TRIPLETT) (NEGRO) (91) RF DE TERMOCUPLA 0.5 A	2	197,00	394,00
8	AMPERÍMETRO	METÁLICO (TRIPLETT) (NEGRO) (92) DE RF DE 0-10	1	197,00	197,00

9	AMPERÍMETRO	PLÁSTICO (HUNG CHANG) (NEGRO) (182) DE GANCHO DIGITALES	2	100,00	200,00
10	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (14) DE 4 CANALES	1	530,00	530,00
11	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (107 Y 98) DE DOBLE CANAL	2	470,00	940,00
12	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (21) DIFERENCIAL	1	600,00	600,00
13	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (109) DIFERENCIAL	1	600,00	600,00
14	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (22) DIFERENCIAL	1	470,00	470,00
15	AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (24) VERTICAL DE DOS CANALES	1	470,00	470,00
16	ANALIZADOR	METÁLICO (FLUKE) (A/N) (240) Y SONDA DE CORRIENTE	1	396,89	396,89
17	ANTENA	HIERRO (A/N) (A/N) (3) DE TV	1	25,00	25,00
18	AUTOTRANSFORMADOR	METÁLICO (OHMITE) (PLOMO) (118)	3	267,00	801,00
19	BANCO DE CARGA CAPACITIVA	METÁLICO (HAMPDEN) (PLOMO) (10) No L3	2	323,00	646,00
20	BANCO DE INDUCTORES	METÁLICO (HAMPDEN) (PLOMO) (9) No L3	2	378,00	756,00
21	BANCO DE RESISTENCIA	METÁLICO (HAMPDEN) (PLOMO) (8) No L3	2	375,00	750,00
22	CÁMARA FOTOGRÁFICA	PLÁSTICO (POLAROID) (NEGRO) (234) PARA OSCILOSCOPIO CON ADAPTADOR 3 PIEZAS	1	550,00	550,00
23	COMPENSADOR	ALUMINIO (A/N) (PLATEADO) (165) ESTATICO DE POTENCIA REACTIVA PARA RED TRIFASICA	1	768,00	768,00
24	COMPUTADOR	PLÁSTICO (CLON) (CREMA) (194)	1	700,00	700,00
25	COMPUTADOR	PLÁSTICO (MAGISTRONIC) (CREMA) (202) 1.- MONITOR SVGA A COLOR MARCA SANSUNG SYNG MASTER 3 MOD. CVM4967T SERIE No H2KBC11193 . 1.- TECLADO MARAC HACER MOD. 6512-TW SERIE D10671S00000. 1.- MAUSE MARCA TECH, MOD. H8GAM555P SERIE No 931213475. 1.- SUPRESOR DE PICOS UL, MOD,. PT-ADA DE 6	1	657,00	657,00
26	COMPUTADOR	PLÁSTICO (COMPAQ) (CREMA) (224) CON 1.- MONITOR MARCA COMPAQ A COLOR MOD. 473B, SERIE S19AF05BA540 $ 42.26 1.- TECLADO ENHANCED MARCA COMPAQ MOD. ENHANCED III SERIE No CIGE035074 $ 12.79. 1.- MAUSE TIPO BUS MARCA COMPAQ SERIE No 1D7-7AY58050 $ 7.79	1	200,72	200,72
27	COMPUTADOR	PLÁSTICO (PREMIO) (CREMA) (242) CON 1.- MONITOR SVGA 15" MARCA PREMIO MOD. H 566 SERIE No 804RM0021O1175 $ 79.85. 1.- TECLADO MARCA PREMIO MOD. KPQEA5ZA SERIE No 7B3D0241*7746 $ 8.87. 1.- MOUSE MARCA MICROSOFT SERIE No 02137115 $ 14.72	1	332,70	332,70
28	COMPUTADOR	PLÁSTICO SINTETICO (PREMIO) (BLANCO) 1 CPU, CON PROCES. INTEL PENTIUM 150 MHz, 16 Mb.Ram DISCO DURO DE 1.6 Gb. FLOPPY DE 3 1/2, TARJETA DE VIDEO pci 1Mb,	1	205,15	205,15
29	COMPUTADOR	PLÁSTICO (CLON) (CREMA) CASE SUPER POWER + CD ROM + CD WRITER. TECLADO MARCA GENIUS SERIE ZM2400164481. MOUSE MARCA GENIUS 850. MONITOR MARCA SANSUNG MOD. 551V SERIE No. AN15HXAT100267R	1	775,00	775,00
30	CONTADOR	METÁLICO (TEKTRONIX) (A/N) 101) DIGITAL	1	100,00	100,00
31	CONTROL DE CONVERSORES	METÁLICO (A/N) (A/N) (171) SEMICONTROLADOS PC DE XAVIER VINUEZA	1	326,00	326,00
32	CONTROL DE MOTOR	METÁLICO (A/N) (A/N) (153) DC	1	150,00	150,00
33	CONTROL DE VELOCIDAD	METÁLICO (A/N) (A/N) (166) DE RESISTENCIA ROTORICA	1	178,00	178,00
34	DATA SWICH	PLÁSTICO (A/N) (CREMA) (174) CONMUTADOR DE DATOS	1	35,00	35,00
35	EQUIPO EDUCATIVO PARA LA ENSEÑANZA	METÁLICO (A/N) (PLOMO) (217) PARA CONVERSOR AC-DC POR TECNICA DE MUESTREO: TESIS DE ANTONIO ZAPATER.	1	700,00	700,00
36	EXCITATRIS ESTATICA	METÁLICO (A/N) (A/N) (221) BASADO EN MICROCONTROLADOR 8751 TESIS DE CARLOS REVERA	1	540,00	540,00
38	FUENTE DE PODER	METÁLICO (OLTRONIX) (PLOMO) (125)	1	200,00	200,00

39	FUENTE DE PODER	METÁLICO (OLTRONIX) (PLOMO) (114)	2	200,00	400,00
40	FUENTE DE PODER	METÁLICO (A/N) (AZUL) (45) CON PANELES DE CIRCUITOS LÓGICOS	2	200,00	400,00
41	FUENTE DE PODER	METÁLICO (MARCHESI) (VERDE) (167) TRIPLE	4	200,00	800,00
42	FUENTE DE PODER	METÁLICO (OLTRONIX) (PLOMO) (126)	1	200,00	200,00
43	FUENTE DE PODER	METÁLICO (HEATKIT) (CAFÉ) (116)	2	200,00	400,00
44	FUENTE DE PODER	METÁLICO (MARCHESI) (A/N) (235) TRIPLE	1	200,00	200,00
45	FUENTE DE PODER	METÁLICO (BK PRECISION) (CAFÉ)	1	200,00	200,00
46	FUENTE DE VOLTAJE	METÁLICO (A/N) (NEGRO CON PLOMO) (223) TIPO SWITCHING, VOLTAJE DE SALIDA 30 A 125 VDC 10 A	1	200,00	200,00
47	FUENTE REGULADA	METÁLICO (HEATKIT) (CAFÉ) (40)	2	40,11	80,22
48	GENERADOR	METÁLICO (A/N) (A/N) (222) ESTATICO DE POTENCIA REACTIVA TRIFASICA	1	1.130,00	1.130,00
49	GENERADOR	METÁLICO (HEWLETT PACKARD) (A/N) (128) DE ONDA CUADRADA	1	530,00	530,00
50	GENERADOR DE FUNCIONES	ALUMINIO (TEKTRONIX) (PLATEADO) (103)	1	530,00	530,00
51	GENERADOR DE FUNCIONES	PLÁSTICO (B&K PRECISION) (A/N) (185) DE 1 MHz	1	530,00	530,00
52	GENERADOR DE FUNCIONES	METÁLICO (SIMPSON) (NEGRO) (110)	1	540,00	540,00
53	GENERADOR DE PULSOS	METÁLICO (A/N) (AZUL) (111) CON FUENTE DE PODER TM 503	1	555,00	555,00
54	GENERADOR DE PULSOS	METÁLICO (HEWLETT PACKARD) (A/N) (148)	1	511,35	511,35
55	GENERADOR DE SEÑALES	PLÁSTICO (TEKTRONIX) (AZUL) (105)	1	530,00	530,00
56	IMPRESORA	PLÁSTICO (HEWLETT PACKARD) (CREMA) (225)	1	68,39	68,39
57	INVERSOR	METÁLICO (A/N) (A/N) (216) MONOFASICO CON MODULACION PWM DE 2 Y 3 NIVELES BASADO EN MICROPROCESADOR 8751: TESIS DE MARCO COPO	1	48,00	48,00
58	KIT MULTIMEDIA	PLÁSTICO (A/N) (A/N) (230) 4X MEDIA VISION, 1T47522J6A495476	1	33,30	33,30
59	MEDIDOR	METÁLICO (HEWLETT PACKARD) (A/N) (121)	1	150,00	150,00
60	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) (75) DE 0-100 Ua	1	250,00	250,00
61	MICROAMPERÍMETRO	METÁLICO (TRIPLETT) (A/N) (75) DE 0-100 uA UNO SIN ESCALA	1	250,00	250,00
62	MOTOR	METÁLICO (A/N) (PLOMO) (32) TRIFÁSICO DE 3/4 HP TIPO 3AB	1	1.320,00	1.320,00
63	MOTOR	HIERRO (A/N) (PLOMO) (33) DE 0.9 HP TIPO NV80A4	2	1.320,00	2.640,00
64	MOTOR	METÁLICO (BALDOR) (AZUL) (159) CC 1 HP a 180 VDC, 1750 rpm, Cat No 3455	2	1.320,00	2.640,00
65	MOTOR	METÁLICO (BALDOR) (AZUL) (156) CC 3/4 HP a 90 VDC, 1750 rpm	2	1.320,00	2.640,00
66	MOTOR	HIERRO (ASTROSYN) (A/N) (191) DE PASO CC 1 DE TIPO 34PM-C124 Y 1 DE TIPO 34PN-C101	2	1.320,00	2.640,00
67	MOTOR	HIERRO (BROWN BOVERI) (A/N) (232) TRIFASICO TIPO MU1254A	1	1.320,00	1.320,00
68	MULTÍMETRO	METÁLICO (TRIPLETT) (A/N) (41)	5	90,00	450,00
69	MULTÍMETRO	METÁLICO (KEITLEY) (A/N) (6) DIGITALCON CABLE INCORPORADO	1	90,00	90,00
70	MULTÍMETRO	ALUMINIO (TEKTRONIX) (PLATEADO) (104) DIGITAL	1	90,00	90,00
71	MULTÍMETRO	METÁLICO (HUNG CHANG) (AMARILLO) (181) DIGITALES DE 4 1/2 DIGITOS	2	90,00	180,00
72	MULTÍMETRO	PLÁSTICO SINTETICO (FLUKE) (AMARILLO) (186) DIGITALES DE 401/2 DIGITOS CON ESTUCHE	2	90,00	180,00
73	MULTÍMETRO	METÁLICO (FLUKE) (A/N) (241)	2	490,00	980,00
74	OSCILADOR	METÁLICO (HEWLETT PACKARD) (A/N) (39) DE RC 110/220 V. 50-100 KHz	1	140,00	140,00
75	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (96)	1	2.532,62	2.532,62
76	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (23)	1	2.532,62	2.532,62
77	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (100)	1	2.532,62	2.532,62
78	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (16) CON RETENCION DE IMAGEN	1	2.532,62	2.532,62
79	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) DE ALMACENAMIENTO DIGITAL CON INTERFASE GP1B IEEE-488	1	2.532,62	2.532,62

80	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (CREMA) (190) PORTATILES. 2 CANALES, PANEL PROTECTOR	4	2.532,62	10.130,48
81	PROBADOR LÓGICO	METÁLICO (CIE) (A/N) (188) TIPO PUNTA	1	120,00	120,00
82	PROGRAMADOR UNIVERSAL	PLÁSTICO (A/N) (A/N) (214) DE MEMORIAS Y MICROCOMPUTADORES CON TARJETA ENCHUFABLE DENTRO DEL COMPUTADOR XT CAJAS DE PROGRAMAS DE: MEMORIA, MICROS 8748 Y 8051	1	148,05	148,05
83	PUNTA DE CORRIENTE	METÁLICO (TEKTRONIX) (A/N) (31)	2	115,00	230,00
84	PUNTA DE EFECTO	METÁLICO (FLUKE) (A/N) (213) HALL PARA MEDICION DE CORRIENTE AC-DC, TIPO PINZA	2	12,00	24,00
85	REGULADOR DE VOLTAJE	METÁLICO (A/N) (A/N) (218) MEDIANTE INTERCAMBIADOR DE TAPS, BASASDO EN EL MICROPROCESADOR 8749: TESIS DE CARLOS COKA	1	25,00	25,00
86	REGULADOR DE VOLTAJE	METÁLICO (A/N) (A/N) (220) BASADO EN UN AMPLIFICADOR LINEAL: TESIS DE RAUL ONTANEDA	1	25,00	25,00
87	SCANNER	PLÁSTICO (DFI) (CREMA) (179) CON TARJETA	1	96,40	96,40
88	SERVOMOTOR	METÁLICO (DAYTON) (PLOMO) /161 Y 160) 115 V. AC o DC CON CAJA	4	216,00	864,00
89	SISTEMA DE ALIMENTACION ININTERRUPIDA	METÁLICO (A/N) (A/N) (219) UPS FUERA DE LINEA TESIS DE RENE RODRIGUEZ	1	64,00	64,00
90	SISTEMA DE CONTROL	METÁLICO (KORBY) (A/N) (187)	1	368,00	368,00
91	SISTEMA MODULAR	METÁLICO (A/N) (A/N) (184) COMPUESTO DE UNA FUENTE DE PODER, UN GENERADOR DE FUNCIONES, UN MULTIMETRO DIGITAL	1	2.400,00	2.400,00
92	TARJETA DE ADQUISICION DE DATOS	PLÁSTICO (A/N) (A/N) LAB-PC1200	1	209,26	209,26
93	TARJETA DE FAX MODEM	PLÁSTICO (A/N) (A/N) (231)	1	6,66	6,66
94	TELÉFONO DE MESA	PLÁSTICO (ERISCSSON) (GRIS) (236)	1	10,00	10,00
95	TRANSFORMADOR	METÁLICO (ADVANCE) (PLOMO) (119) ESTABILIZADORES DE VOLTAJE	2	267,00	534,00
96	TRANSFORMADOR	METÁLICO (ADVANCE) (PLOMO) (120) ESTABILIZADORES DE VOLTAJE	2	267,00	534,00
97	TRANSFORMADOR	METÁLICO (CETEL) (A/N) (197) TRIFASICI ZIG-ZAG EN EL AIRE 220/203/380 V.	1	267,00	267,00
98	UNIDAD COMPARADORA	ALUMINIO (TEKTRONIX) (PLATEADO) (28) DIFERENCIALES	2	178,00	356,00
99	UNIDAD DE GENERACION	METÁLICO (TEKTRONIX) (A/N) (106) DE CALIBRACION	1	145,00	145,00
100	UNIDAD ESPECTROSCOPIO	ALUMINIO (TEKTRONIX) (PLATEADO) (20)	1	730,00	730,00
101	UNIDAD TRAZADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (99)	1	680,00	680,00
102	UNIDAD, AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (18) DE DOBLE TRAZO	2	330,00	660,00
103	UNIDAD, AMPLIFICADOR	ALUMINIO (TEKTRONIX) (PLATEADO) (17) DIFERENCIALES DOBLES	2	357,00	714,00
104	UNIDAD,BASE DE TIEMPO	ALUMINIO (TEKTRONIX) (PLATEADO) (15) AMPLIFICADOR HORIZONTAL	1	174,00	174,00
105	UNIDAD,BASE DE TIEMPO	ALUMINIO (TEKTRONIX) (PLATEADO) (25)	1	174,00	174,00
106	UNIDAD,BASE DE TIEMPO	ALUMINIO (TEKTRONIX) (PLATEADO) (108 y 97) Y AMPLIFICADOR HORIZONTAL	1	174,00	174,00
107	UNIDAD,BASE DE TIEMPO	ALUMINIO (TEKTRONIX) (PLATEADO) (19) AMPLIFICADOR HORIZONTAL	1	174,00	174,00
108	VARIAC	METÁLICO (A/N) (PLOMO) (149) con servomotor, tipo 30 MD 136 B	1	220,00	220,00
109	VARIADOR DE VELOCIDAD	METÁLICO (TELEMECANIQUE ALTIVARS) (A/N) (212) 3HP	2	356,00	712,00
		TOTAL			73.243,67

LABORATORIO DE TALLER ELÉCTRICO

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	BOBINADORA ELECTRICA	METÁLICO (MEYRA) (PLOMO) (146) CON MOTOR ELECTRICO EDON 1/4 HP MOD. 7055	1,00	360,00	360,00
2	CAUTÍN	PLÁSTICO (A/N) (NEGRO) (96) DE 300 GRAMOS	1,00	10,00	10,00

3	CORTADORA	METÁLICO (ADEL TOOLCO) (A/N) (199) DE LAMINAS PAT. No. 2542103	1,00	172,43	172,43
4	DOBLADORA	HIERRO (ROPER WHITNEY) (VERDE) (178) UNIVERSAL DE 48" DE LARGO	1,00	597,39	597,39
5	ENTENALLA	(86) HIERRO (YORK) (AZUL)	1,00	230,00	230,00
6	ENTENALLA	HIERRO (FUKUNG BRAND) (A/N) (133) DE 5" No. 125	1,00	230,00	230,00
7	ENTENALLA	HIERRO (YORK) (ROJO) DE 100 mm	1,00	187,00	187,00
8	ESCALERA	ALUMINIO (A/N) (PLATEADO) (210) PIE DE GALLO DE 3 METROS	1,00	35,00	35,00
9	ESMERIL	HIERRO (LETAG) (A/N) (144) TIPO E/5, 1.8 CV	1,00	289,90	289,90
10	ESMERIL	PLÁSTICO (BLACK & DEKER) (VERDE) (161) DE 1/3 HP TIPO M	1,00	230,00	230,00
11	EXTINGUIDOR DE INCENDIOS	METÁLICO (GENERAL) (ROJO) (187)	1,00	24,00	24,00
12	EXTRACTOR DE OLOR	METÁLICO (CHAC KUANG) (A/N) (141) DE 18 "	1,00	57,00	57,00
13	GENERADOR	HIERRO (HOLLZER CABOT) (NEGRO) (33) DE CC 4 KW, R CRD, TIPO CBD	1,00	400,00	400,00
14	GRABADOR DE METALES	METÁLICO (GREEN ENGRACEA) (A/N) (200) CON TODOS SUS ACCESORIOS	1,00	160,00	160,00
15	GUILLOTINA	METÁLICO (ROPER WHITNEY) (VERDE) (177) DE 57" No. 9027 C	1,00	268,00	268,00
16	JUEGO	PLÁSTICO (SPEADEX) (A/N) (195) EN CAJA	1,00	63,00	63,00
17	JUEGO DE COPAS	METÁLICO (DREHMAX) (A/N) (95) Y DESTORNILLADORES 4 - 14 mm	1,00	15,00	15,00
18	JUEGO DE COPAS	HIERRO (A/N) (PLATEADO) (132) DE 24 PIEZAS	1,00	15,00	15,00
19	JUEGO DE LLAVES CORONA	HIERRO (CROMO VANADIUM) (PLATEADO) (108) DE 8 PIEZAS DE 6 a 22 mm: 6-7; 8-9; 10-11; 12-13; 14-15; 16-17; 18-19; 20-22.	1,00	45,00	45,00
20	JUEGO DE LLAVES CORONA	HIERRO (CROMO VANADIUM) (PLATEADO) (109) DE 8 PIEZAS EN PULGADAS 1/4-5/16; 3/8-7/19; 1/2-9/16; 19/32-11/16; 5/8-3/4: 25/32-7/8	1,00	45,00	45,00
21	JUEGO DE LLAVES DE BOCA	HIERRO (DROP FORGED) (PLATEADO) (106) DE 6 PIEZAS EN PULGADAS 1/4-5/16; 3/8-7/19; 1/2-9/16; 19/32-11/16; 5/8-3/4: 25/32-7/8	2,00	50,00	100,00
22	JUEGO DE LLAVES DE BOCA	HIERRO (ALLOYSTAAL) (PLATEADO) (107) DE 8 PIEZAS, DE 6 a 22 mm: 6-7; 8-9; 10-11; 12-13; 14-15; 16-17; 18-19; 20-22.	2,00	50,00	100,00
23	JUEGO DE TARRAJAS	HIERRO (ANGELITO) (PLATEADO) (128) DE 15 PIEZAS EN MILIMETROS CON PORTA MACHUELOS ROTO	1,00	36,00	36,00
24	JUEGO DE TARRAJAS	HIERRO (ANGELITO) (PLATEADO) (129) DE 15 PIEZAS EN PULGADAS	1,00	36,00	36,00
25	MANDRIL	HIERRO (A/N) (A/N) (150) DE 3/4 PARA SER USADO EN EL TALADRO DE COLUMNA ERLO O EN EL TORNO COLCHESTER	1,00	25,00	25,00
26	MICRÓMETRO	ALUMINIO (A/N) (PLATEADO)	1,00	50,00	50,00
27	MICRÓMETRO	ALUMINIO (CRANSTON) (PLATEADO) (197) CENTRAL DE 1"	1,00	50,00	50,00
28	MICRÓMETRO	ALUMINIO (NSK) (PLOMO) (84) de -25 mm	1,00	50,00	50,00
29	MOTOR	HIERRO (ASEA) (NEGRO) de 0.5 HP	1,00	1.320,00	1.320,00
30	MOTOR	HIERRO (GENERAL ELECTRIC) (NEGRO) (10) DE CC TIPO COMPOUND DE 1/8 HP	1,00	1.320,00	1.320,00
31	MOTOR	HIERRO (VELOX) (A/N) (11) DE CC 110 V	1,00	1.320,00	1.320,00
32	MOTOR	HIERRO (GENERAL ELECTRIC) (NEGRO) (13) DE REPULSION DE 1/5 HP TIPO R 5A	1,00	1.010,00	1.010,00
33	MOTOR	METÁLICO (A/N) (A/N) (14) DE REPULSION DE 1/4 HP DE 220 V	1,00	980,00	980,00
34	MOTOR	METÁLICO (A/N) (A/N) (18) TRIFASICO DE 1.25 HP	1,00	750,00	750,00
35	MOTOR	METÁLICO (ELECTRIC) (A/N) (19) TRIFASICO DE 5 HP	1,00	1.400,00	1.400,00
36	MOTOR	METÁLICO (WEG) (AMARILLO) (34) ELECTRICO DE 1/4 HP, 110 V TIPO ACMRT-1 HP	1,00	1.400,00	1.400,00
37	MOTOR DE CC	HIERRO (A/N) (A/N) (164) DE 1.5 HP, 24 V	1,00	520,00	520,00
38	MOTOR DE INDUCCIÓN	HIERRO (GENERAL ELECTRIC) (NEGRO) (12) MOMNOFASICO DE 1/6 HP TIPO SA	1,00	630,00	630,00
39	PISTOLA PARA PINTAR	(135) METÁLICO (THOMAS) (PLATEADO)	1,00	90,00	90,00
40	SIERRA	HIERRO (UNIZ) (PLOMO) (145) ELECTRICA PARA METALES DE 14" CON MOTOR MARCA AJA, 220/380 V. 1 HP	1,00	370,00	370,00
41	SOLDADORA	METÁLICO (LINCWELDER) (ROJO) (206) COD. No. 87-12-710, 220 V.	1,00	1.230,00	1.230,00

42	SOPLETE	METÁLICO (SIEVERT) (DORADO) (76) A GASOLINA	1,00	40,00	40,00
43	TALADRO	HIERRO (ERLO) (VERDE) (143) PAT. 99145 CON MOTOR TRIFASICO MARCA SIEMENS, 1 CV No 1658704	1,00	168,00	168,00
44	TALADRO	HIERRO (SMITH CORP) (VERDE) (162) TIPO C1 DE 1/2 HP	1,00	110,00	110,00
45	TALADRO	PLÁSTICO (BLACK & DEKER) (NEGRO) (181) DE 3/8" No. 7104, TYPE 1	1,00	160,00	160,00
46	TELÉFONO DE MESA	PLÁSTICO (ERICSSON) (GRIS) (158)	1,00	15,00	15,00
47	TORNO	(152) HIERRO (COLCHESTER MASTER) (VERDE) TORNO PARALELO DE PRECISION, 5 HP, 220 V, , Mod. 2500 - 6.1/2", con (1) Bancada endurecida por inducción, Caja NORTON para cambios rápidos parada y reversa instantaneo por sistema de CLUTCH, Motor eléctrico trifásico de 5 HP, 220/380, Recipiente con bomba de refrigeración , (1) Dispositivo transformador de seguridad de bajo voltaje 50 V, 40 W. AC. (1) Mandril de 3 garras, PRATT BURNERD, Cat. # 1272-32005, S/N. BP76/15893, (1) Plato de arrastre, (2) Puntos fijos, (1) Punto movil, marca J & S LUNZER, 330B, (1) Copiador de conos, (1) Torrete portaherramientas para 4 posiciones del carro transversal, (1) Tope protector del carro logitudinal de 5 posiciones, (1) Mandril de 4 garras de acoplamiento 225 mm, marca COLCHESTER, Mod. 1562-32601,serie # D13824.	1,00	594,00	594,00
48	TORNO	(160) HIERRO (SOUTH BEND) (VERDE), (160) CAT: CL670R CON MOTOR 1/2 HP, MOD. 5KC45MG185A CON, (3) Portaherramientas para cortar, marca WILLIAMS, # 20205, # 29L, # 2020R, (3) Perros o arrastradores, (1) # 1655 NR1 de 1 11/16", (1) # 1654 NR1 1 5/8", (1) # 1651 NR1 de 5/8", (1) Portaherramienta para tornear, 2010L, marca HOMECRAFT, (1) Portaherramienta para tornear # 2050, marca HOMECRAFT, (1) Torre de portaherramientas, (3) Muelas # 592-1-2-3 para exteriores, (1) Barra para interiores # OB 1/2", marca WILLIAMS, (1) Punto Fijo, (1) Mandril para brocas JACOBS CHUC # 34. (3) Portaherramientas.	1,00	780,00	780,00
49	VOLTÍMETRO	PLÁSTICO (STERLING) (A/N) (28) DE 10 V	1,00	50,00	50,00
50	VOLTÍMETRO AMPERÍMETRO	PLÁSTICO (SIMPSON) (NEGRO) (189) DE PINZA	1,00	100,00	100,00
		TOTAL			17.877,72

LABORATORIO DE SISTEMAS ELÉCTRICOS DE POTENCIA

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ANALIZADOR DE REDES	METÁLICO (WESTINNGHOUSE) (A/N) (1) Compuesto de 9 gavinetes	1,00	268,00	268,00
2	CALCULADORA	ACRÍLICO (HEWLETT PACKARD) (BLANCO)	1,00	63,00	63,00
3	CD ROM	METÁLICO (LG) (BLANCO) 52x	1,00	41,00	41,00
4	COMPUTADOR	PLÁSTICO (DTK) (BLANCO) (73) TIPO PENTIUM DESHTOP (1) C.P.U. procesador pentium intel de 75 MHz, 8 MB. de RAM, disco 1 Gb. drive de 3 1/2, 2 puertos seriales, 1 paralelo, 3 slots PCI, y 4 slots ISA, (1) Monitor a color SPVG marca DTK, Mod. CMD-1411, serie # G019819. (1) Teclado marca DTK, Mod. SPK-106S, S/N. (1) Mouse marca DTK, 3 botones Mod. 2900, serie # 502123791.	1,00	420,00	420,00

5	COMPUTADOR	PLÁSTICO (DTK) (BLANCO) (72) TIPO PENTIUM MIMI TOWER (1) C.P.U.procesador pentium intel de 100 MHz, 8 MB. de RAM, disco 1.2 Gb. drive de 3 1/2, 2 puertos seriales, 1 paralelo, 3 slots PCI, y 5 slots ISA, tarjeta de video, 1 Kit cd rom 6X con 2 parlantes stereo, tarjeta de sonido, (1) módulo de memoria SIMM, de 72 pines 8 Mb. (1) Monitor a color SPVG marca DTK, Mod. CMD-1411, serie # G019792. (1) Teclado marca DTK, Mod. SPK-106S, S/N. (1) Mouse marca DTK, 3 botones Mod. 2900, serie # 502123788.	1,00	420,00	420,00
6	COMPUTADOR	PLÁSTICO (DTK) (BLANCO) (74) TIPO MIDI TOWER (1) C.P.U. procesador pentium intel de 100 MHz, 8 MB. de RAM, disco 1 Gb. drive de 3 1/2, 2 puertos seriales, 1 paralelo, 4 slots PCI, y 4 slots ISA, (1) Monitor a color SPVG marca DTK, Mod. CMD-1411, serie # G019654. (1) Teclado marca DTK, Mod. SPK-106S, S/N. (1) Mouse marca DTK, 3 botones Mod. 2900, serie # 502123796.	1,00	420,00	420,00
7	COMPUTADOR	(77) PLÁSTICO (PACKARD BELL) (BLANCO) (1) C.P.U. microprocesador pentium 233 MMX, 32 MB. de RAM, disco 4 Gb. drive de 3 1/2, 1 fax modem de 56 kbps, 1 kit multimedia 24x. (1) Monitor SPVG 14" PACKARD BELL, Mod. 1024S, serie # GVMN74300150. (1) Teclado marca PACKARD BELL, Mod. 5131C, serie # C7C080705. (1) Mouse marca PACKARD BELL, Mod. FDM-611, serie # FWMC71605680.	1,00	420,00	420,00
8	COMPUTADOR	(81) PLÁSTICO (CLON) (BLANCO) C.P.U. pentium II celeron 400 MHz, 64 MB. de RAM, disco duro de 8.4 Gb, floppy de 1.44Mb. Tarjetas de video y sonido fax modem de 56.6, de red 10/100 y kit multimedia 48X, incluye parlantes 1.- Monitores 15" marca LG, Mod. 520 SI, serie # 906NT00/ 189, 1.- Teclados marca LOT, Mod. NK-668, ID. NZHNK-33, 1.- Mouses 3 botones, Mod. MUS2P, serie # 0105301,	1,00	840,00	840,00
9	COMPUTADOR	(81) PLÁSTICO (CLON) (BLANCO) C.P.U. pentium II celeron 400 MHz, 64 MB. de RAM, disco duro de 8.4 Gb, floppy de 1.44Mb. Tarjetas de video y sonido fax modem de 56.6, de red 10/100 y kit multimedia 48X, incluye parlantes 1.- Monitores 15" marca LG, Mod. 520 SI, serie # 906NT00/ 213 1.- Teclados marca LOT, Mod. NK-668, ID. NZHNK-33, 1.- Mouses 3 botones, Mod. MUS2P, serie # 116453	1,00	840,00	840,00
10	COMPUTADOR	(81) PLÁSTICO (CLON) (BLANCO) C.P.U. pentium II celeron 400 MHz, 64 MB. de RAM, disco duro de 8.4 Gb, floppy de 1.44Mb. Tarjetas de video y sonido fax modem de 56.6, de red 10/100 y kit multimedia 48X, incluye parlantes 1.- Monitores 15" marca LG, Mod. 520 SI, serie # 906NT00/ 413 1.- Teclados marca LOT, Mod. NK-668, ID. NZHNK-33, 1.- Mouses 3 botones, Mod. MUS2P, serie # 16454	1,00	840,00	840,00
11	COMPUTADOR	(82) PLÁSTICO (CLON) (BLANCO) C.P.U. con mainboard que incluye tarjeta de video y sonido procesador intel celeron de 500 MHz, 64 MB. de RAMPC100, disco duro de 10.2 GB, drive de 3 1/2, fax modem y cd-rom 52X 1 par de parlantes 1 Monitor marca LG, Mod. 45V, serie # C85644 1 Teclado en español, 1 Mouse 2 botones, marca LCT, S/N.	1,00	650,00	650,00
12	COMPUTADOR	(82) PLÁSTICO (CLON) (BLANCO) C.P.U. con mainboard que incluye tarjeta de video y sonido procesador intel celeron de 500 MHz, 64 MB. de RAMPC100, disco duro de 10.2 GB, drive de 3 1/2, fax modem y cd-rom 52X 1 par de parlantes 1 Monitor marca LG, Mod. 45V, serie # C86060 1 Teclado en español, 1 Mouse 2 botones, marca LCT, S/N.,	1,00	650,00	650,00
13	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Computadoras INTEL PENTIUM III 800MHz No POOBBO201373- Motherboard AEGIS P6300 cache 256 Kb, Floppy 2.5" serie No P0285625 1 Monitore Marca ACER de 15" serie No 7035DDD002592 Modelo JD166LS 1 Mause Marca QBEX series No 00105088 modelo LYNX30 1 Teclado marca QBEX serie No 001013155 - modelo SCORPIOS 98A 1 Juego de parlantes y microfonos.	1,00	985,00	985,00

14	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Computadoras INTEL PENTIUM III 800MHz NoPOOBBO201379 Motherboard AEGIS P6300 cache 256 Kb, Floppy 2.5" serie No P0285625 1 Monitore Marca ACER de 15" serie No 7035DDD002884 Modelo JD166LS 1 Mause Marca QBEX series No 001060811 modelo LYNX30 1 Teclados marca QBEX serie No 001061092 modelo SCORPIOS 98A 1 Juego de parlantes y microfonos.	1,00	985,00	985,00
15	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) 1 CPU, mainboard tarjeta de video y sonido, ntel celeron de 500 MHz, 64 MB. rampc100, disco duro de 10.2 GB. Drive de 3 1/2, fax modem,y cd-rom 52X, 1 Monitor marca LG, Mod. 45V, serie # C85636, 1 Teclado en español. 1 Mouse 2 botones marca LCT, S/N., 1 Juego de parlantes .	1,00	650,00	650,00
16	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX113828F, Teclado Marca AOPEN serie No. 41114691TC, Mouse marca GENIUS serie No. 10935504724	1,00	650,00	650,00
17	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX114032Y, Teclado Marca AOPEN serie No. 41114695TC, Mouse marca GENIUS serie No. 10935504730	1,00	650,00	650,00
18	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX114019V, Teclado Marca AOPEN serie No. 41114692TC, Mouse marca GENIUS serie No. 10935504701	1,00	650,00	650,00
19	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX113927D, Teclado Marca AOPENserie No. 41114696TC, Mouse marca GENIUSserie No. 10935504707	1,00	650,00	650,00
20	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX113949Z, Teclado Marca AOPEN serie No. 41114694TC, Mouse marca GENIUSserie No. 10935504750	1,00	650,00	650,00
21	COMPUTADOR	PLÁSTICO (CLON) (BLANCO) Monitor marca SANSUNG serie No. AV17HCGX114162F, Teclado Marca AOPENserie No. 41114693TC, Mouse marca GENIUSserie No. 10935504727	1,00	650,00	650,00
22	HUB	METÁLICO (ENCORE) (PLOMO) DE 8 PUERTOS	2,00	50,00	100,00
24	IMPRESORA	PLÁSTICO (EPSON) (BLANCO) (78) STYLUS COLOR 400	1,00	44,58	44,58
25	IMPRESORA	METÁLICO (IBM) (BLANCO) (79) PROPINTER 2 CON CABLE Y CABLE SHIP GROUP	1,00	58,00	58,00
26	IMPRESORA	PLÁSTICO (EPSON) (BLANCO) (33) DE 290 CPS.136 COLUMNAS FX-1050	1,00	26,00	26,00
27	MAIN BOARD	PLÁSTICO (A/N) (VERDE)	1,00	78,00	78,00
28	MICROCOMPUTADOR	(75) PLÁSTICO (DTK) (BLANCO) 1 CPU, con tarjeta de gráficos , tarjeta de comunicaciones 3 com 3C503-16 ethernet, drive de 5 1/4, serie # 3VB89999, 1 Monitor marca SAMSUNG, Mod. SING-MASTER 3 N, serie # H8ZC605973. 1 Teclado marca BTC, ID. E5X5R5BTC, serie K302131896, 1 Mouse serie # E6QMOUSE X31.	1,00	456,00	456,00
29	MOUSE	PLÁSTICO (A/N) (BLANCO) PS/2 A4-TECH	1,00	3,50	3,50
30	MOUSE	PLÁSTICO (A/N) (BLANCO)	2,00	2,50	5,00
32	MOUSE	PLÁSTICO (A/N) (BLANCO) PS/2 A4-TECH	1,00	3,50	3,50
33	RELAY DE CORRIENTE	PLÁSTICO (OERLIKON) (NEGRO) (39)	1,00	141,00	141,00
34	RELAY DE CORRIENTE	PLÁSTICO (A/N) (NEGRO) (49) R.C MONOFASICO 30A FORMA MR-A	2,00	141,00	282,00
36	RELAY DE CORRIENTE	PLÁSTICO (BROWN BOVERI) (NEGRO) (42) SECUNDARIO DE TIEMPO No B-856179	1,00	141,00	141,00
37	RELAY DE SOBRECORRIENTE	PLÁSTICO (WESTINNGHOUSE) (NEGRO) (38) TYPE 00.6	1,00	141,00	141,00
38	RELAY DIFERENCIAL	(46) PLÁSTICO (OERLIKON) (NEGRO)	1,00	141,00	141,00
39	RELAY DIFERENCIAL	PLÁSTICO (GENERAL ELECTRIC) (NEGRO) (47) DE 115 V	1,00	141,00	141,00
40	RELAY DIFERENCIAL	(48)PLÁSTICO (GENERAL ELECTRIC) (NEGRO)	2,00	141,00	282,00
42	RELAY LIMITADOR	PLÁSTICO (OERLIKON) (NEGRO) (43) TIPO BITS 818290HO1.1	1,00	141,00	141,00
43	RELAY TERMICO	PLÁSTICO (BROWN BOVERI) (NEGRO) (40) No B-245934	1,00	141,00	141,00
44	RELAY TERMICO	PLÁSTICO (BROWN BOVERI) (NEGRO) (41) No H-253501	1,00	141,00	141,00

45	TABLA DE DIGITACION	(76) MADERA (SUMMAGRAPHICS) (A/N)	1,00	140,90	140,90
46	TARJETA DE COMUNICACIONES	PLÁSTICO (NOVELL) (VERDE) MICROCANAL 16 BIT PARA PS/2	1,00	23,48	23,48
47	TARJETA DE RED	PLÁSTICO (ENCORE) (VERDE) 10/100 INSTALADO EN EL COMPUTADOR CON SERIE No 2351173	1,00	15,00	15,00
48	TARJETA DE RED	PLÁSTICO (ENCORE) (VERDE) 10/100 INSTALADO EN EL COMPUTADOR CON SERIE No 2351173	1,00	15,00	15,00
49	TECNIGRAFO	METÁLICO (FRANK KUHLMANN) (VERDE) (69) MAQUINA DE DUBUJO No 10/011384, CON MESA DE DIBUJO	1,00	180,00	180,00
50	TELÉFONO DE MESA	ACRÍLICO (A/N) (VERDE)	1,00	20,00	20,00
51	TEMPORIZADOR	ACRÍLICO (OERLIKON) (NEGRO) (45) TIPO MSG No 41441HO5.2	1,00	48,00	48,00
52	TEMPORIZADOR	ACRÍLICO (A/N) (NEGRO) (44) TIPO MSG No 358039	1,00	48,00	48,00
53	VOLTÍMETRO	(18) PLÁSTICO (HEWLETT PACKARD) (AMARILLO)	2,00	100,00	200,00
		TOTAL			15.548,96

LABORATORIO DE MAQUINAS ELÉCTRICAS

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ACCESORIO	(7) METÁLICO (A/N) (A/N) GRUPO DE ACCESORIOS, CON: a) 1 Reostato de campo 417 Ohm, 1.05 A, # 48951, SG7. b) 1 Reostato de campo 300 Ohm 1.3 A # 47778 tipo KG600. c) 1 Arrancador 1/2 2.2 KW, 110 V, # 48447, tipo GL 2.5. d) 1 Reostao 296 Ohm 1.4 A, tipo SG-8, # 48381. e) 1 Reostato 300 Ohm 1.3 A, # 45502, tipo KG 600. f) 1 Arrancador 1/2 2.2 KW, 110 V, tipo GL 2.5, # 46748. g) 1 Arrancador estrella triangulo manual 125.	1	190,00	190,00
2	ACCESORIO	(9) METÁLICO (A/N) (A/N) (9) METÁLICO (A/N) (A/N) GRUPO DE ACCESORIOS, CON: a) 1 Arrancador 1/2 2.2 KW, 110 V, tipo GL 2.5, # 46747 b) 1 Reostato 296 Ohm, 1.4 A, tipo SG8, # 45157 c) 1 Reostato de campo 300 Ohm 1.3 A, KG 600,# 45505 d) 1 Arrancador 1/2 2.2 KW, 110 V, tipo GL 2.5, # 48440 e) 1 Reostato 296 Ohm, 1.4 A, tipo SG-8, # 45153 f) 1 Reostato de campo 300 Ohm, 1.3 A, KG 600 # 45497 g) 1 Arrancador retorico 150 V, 15 A, DL 2.5, # 49015 h) 1 Reostato de campo 296 ohm, 1.4 A, SG-8, # 48385	1	200,00	200,00
3	ACCESORIO	(10) METÁLICO (A/N) (A/N) a) 1 Reostato 55.3 Ohm, 3.1 A, marca BRUXELLES b) 1 Arrancador 1/2 2.2 KW, 110 V, tipo GL 2.5 # 48433 c) 1 Reostato 570 Ohm, 09 A, tipo SG-7, # 45163 d) 1 Reostato 500 Ohm, 0.9 A, tipo KG 600 # 45476 e) 2 Arrancadores estrella triangulo manuales f) 2 Arrancadores retoricos 150 V, 15 A, tipo DL 2.5, # 49011 - 49012 (1 sin caja) g) 1 Reostato de regulacion 1.4 A, 296 Ohm, SG8 # 45155 h) 1 Reostato 0.22 A, 12725 Ohm, marca BRUXELLES.	1	190,00	190,00
4	ACOPLES	HIERRO (A/N) (A/N) (13) EN DOS MEDIDAS	3	75,00	225,00
5	ALTENADOR	METÁLICO (CETEL) (A/N) (79) De 3 x 220 v, 2.75 KVA, 1800 rpm, tipo S611-2, 1 base soldada No 141824A, 1 acoplamiento semi-elastico	1	230,00	230,00
6	AMPERÍMETRO	METÁLICO (NORMA) (A/N) (18) Galvanómetro 40.0.40	1	100,00	100,00
7	AMPERÍMETRO	METÁLICO (NORMA) (A/N) (21) DE 2-10 A	1	100,00	100,00
8	AMPERÍMETRO	METÁLICO (NORMA) (A/N) (39) CC 1.2-6-30 A	1	100,00	100,00
9	AMPERÍMETRO	METÁLICO (YEW) (A/N) (11) DE CC 1/3/10/30 A TIPO 2011	1	100,00	100,00
10	AMPERÍMETRO	METÁLICO (YEW) (A/N) (9) DE PINZAS 15/30/75/150/300 A	2	100,00	200,00
11	AMPERÍMETRO	METÁLICO (NORMA) (A/N) (27) de CA / CC, 5-20 A	6	100,00	600,00
12	AMPERÍMETRO	METÁLICO (NORMA) (A/N) (25) DE CC 0.12-0.6-3 A	2	100,00	200,00

13	AMPERÍMETRO	METÁLICO (GOSSEN) (A/N) (3) de cc 1.2/2.4/6/42/24 A	8	100,00	800,00
14	AMPERÍMETRO	METÁLICO (GOSSEN) (A/N) (4) DE CC 1.2/6 A	2	100,00	200,00
15	AMPERÍMETRO	METÁLICO (GOSSEN) (A/N) (5) DE DC/AC 12/24 A	6	100,00	600,00
16	AMPERÍMETRO	METÁLICO (YEW) (A/N) (11) DE CA 1.1/0.2/5.5/1 A, TIPO 2013	7	100,00	700,00
17	AMPERÍMETRO	METÁLICO (YEW) (A/N) (8) DE CC, TIPO 2011	5	100,00	500,00
18	AMPERÍMETRO	METÁLICO (YEW) (A/N) (7) DE CC 0.1/0.3/1/3 A, TIPO 2011	5	100,00	500,00
19	AMPERÍMETRO	METÁLICO (AEG) (A/N) (197) DE PRECICIÓN SIN ESCALA	4	100,00	400,00
20	AMPERÍMETRO	METÁLICO (A/N) (A/N) (117) PORTATIL AC	10	100,00	1000,00
21	ANALIZADOR	METÁLICO (AEG) (A/N) (57) INDUSTRIAL	1	100,00	100,00
22	ANALIZADOR	METÁLICO (SIEMENS) (A/N) (1) INDUSTRIAL CON: 2 TRANSFORMADORES, 1VOLTIMETRO, 1 AMPERIMETRO, 1 VATIMETRO CADA UNO	3	293,00	879,00
23	ANALIZADOR	METÁLICO (SIEMENS) (A/N) (135) INDUSTRIAL , TIPO C 70240 - 45050A	3	369,00	1107,00
24	AUTOTRANSFORMADOR	METÁLICO (GENERAL RADIO) (PLOMO) (44)	1	200,00	200,00
25	AUTOTRANSFORMADOR	METÁLICO (POWERSTAT) (A/N) (202) Trifásicos 240/280 v, 22 A, 10.7 KVA	2	330,00	660,00
26	BANCOS DE CARGA	METÁLICO (TOTTENHAM) (PLOMO) (228) Trifásico de 220 V, 4 A	1	330,00	330,00
27	BANCOS DE CARGA	METÁLICO (TOTTENHAM) (PLOMO) (228) Trifásico de 220 V, 4 A	1	90,00	90,00
28	BASE	ACERO (A/N) (VERDE) (96) DE 1.15 X 0.15 m DE ANCHO X 0.05 nm DE ESPESOR.	1	25,00	25,00
29	BASE	ACERO (A/N) (VERDE) (99) EN U DE 1.20 X 0.15 X 0.05 m X 1/4",	1	25,00	25,00
30	BASE	ACERO (A/N) (VERDE) (12) MOVILES PARA MOTORES	1	25,00	25,00
31	BASE	ACERO (A/N) (VERDE) (12) MOVILES PARA MOTORES	1	25,00	25,00
32	BOBINA	METÁLICO (NORMA) (A/N) (56)	1	15,00	15,00
33	CAPACIMETRO DIGITAL	METÁLICO (CHAUVIN ARNDUX) (A/N) (120) A TRANSITORES TRIFASICO 5 A	1	110,00	110,00
34	CARGA CAPACITIVA	METÁLICO (HAMPDEN) (PLOMO) (10)	2	50,00	100,00
35	CARGA INDUCTIVA	(9) METÁLICO (HAMPDEN) (PLOMO)	2	23,00	46,00
36	CARGA RESISTIVA	(8) METÁLICO (HAMPDEN) (PLOMO)	2	23,00	46,00
37	CARGA RESISTIVA	METÁLICO (A/N) (PLOMO) (16) Reactivas	2	23,00	46,00
38	CARGADOR DE BATERÍA	METÁLICO (SCHRACK) (PLOMO) (89)	1	250,00	250,00
39	COCHE TRANSPORTABLE	METÁLICO (A/N) (PLOMO) (194) con garruchas	2	40,00	80,00
40	COMPUTADOR	PLÁSTICO (DTK) (BLANCO) (272) (HA) 1 C.P.U. procesador INTEL 80386-15DX, procesador matematico 80387 de 4 MB RAM, 1 Disco 120 MB, 1 floppy de 5 1/4 de 1.2 MB, 1 flopy de 3 1/2 de 1.4 MB., 2 puertos seriales y 1 puerto paralelo. 1 Monitor a color VGA, marca LEADER EDGE, Mod. CMC 14-17AE, serie # 9975415306. 1 Teclado, marca DTK 101 teclas, ID: FKD46K108, serie # KB2062021.	1	148,97	148,97
41	CONJUNTO	METÁLICO (MAWDSLEY'S) (A/N) (223) EXPERIMENTALES PARA SUMINISTRO DE CA (HA) 1.- 1 Maquina de demostracion 360/210 V, serie No.: SD/54/480 con: Estator CA delta-estrella, Rotor CA delta, y Colector CC. 2.- 1 Motriz devanado para 110 V, CC, 4000 rpm, serie #s: 50CM/480 3.- 1 Consola metálica sobre ruedas para montaje de elementos de la máquina demostrativa MAWDSLEY'S Ord. 225 4.- 1 Tacogenerador MAWDSLEY'S 19 V, 1000 rpm, # 6GT; . Con balanzas de 0-100 Newtons, marca SALTER. Ord. 224	2	733,00	1466,00
42	CONTROL DE VELOCIDAD	METÁLICO (A/N) (A/N) DE MOTOR TRIFASICO ASINCRONICO (TESIS EGAS - GALARZA)	1	84,00	84,00
43	CONVERTIDOR	METÁLICO (A/N) (PLOMO) (73) de AC/DC con motor trifasico y un generador CC tipo G10 92-4 serie 617197	1	141,00	141,00

44	CONVERTIDOR DE FRECUENCIA	(77) METÁLICO (SIEMENS) (PLOMO) 1.- Generador CC tipo G1592-4, serie # 616993 2.- 1 Motor trifasico tipo R1426-4, serie # 825837 3.- 1 Maquina compuesta de: a) 1 Motor CC tipo QG1292-4, serie # 617366 b) 1 Motor tipo R8, 9-2E4, serie 3 901794 4.- 1 Alternador trifasico tipo QF1292-4, serie # 790787, con motor tipo R8, 9-2E4, s/n 901792	1	547,00	547,00
45	COSFIMETRO	METÁLICO (GOSSEN) (A/N) (8) TRIFASICO 5 A. No. 1806884-1806885	2	117,00	234,00
46	DÉCADA DE INDUCCIÓN	ALUMINIO (GENERAL RADIO) (PLATEADO) (142) 0.1 - 1 H	1	10,00	10,00
47	DINAMO COMPUND	METÁLICO (CETEL) (A/N) (15 y 80) 110 V, 2KW, 1800 rpm: 1 c	2	24,00	48,00
48	DINAMÓMETRO	METÁLICO (CETEL) (A/N) (97) BALANZA DINAMOELECTRI 110 V. 2.5 KW, 1800 rpmTIPO S-600	1	30,00	30,00
49	DINAMÓMETRO	METÁLICO (HAMPDEN) (A/N) (11) CADA UNO CON TORQUIMETRO, BRAZO	2	79,00	158,00
50	DRIVE	PLÁSTICO (MITSUMI) (BLANCO) (276) INSTALADO EN EL COMPUTADOR ZEOS 286 DE	1	5,00	5,00
51	ELECTRODINAMOMETRO	METÁLICO (MAWDSLEY'S) (A/N) (231) DE TORQUE CC 110 V CLASE F	2	79,00	158,00
52	ELEMENTOS DE MÁQUINA	METÁLICO (A/N) (A/N) (86)Combinada, 1 juego de polos, de 2 unidades, 1 inducido a jaula, 1 inducido a doble jaula, 1 inducido conmutatriz	1	28,00	28,00
53	EQUIPO	METÁLICO (TOTTENHAM) (A/N) (226) DE CONTROL PARA LA MAQUINA DE 3 HP, 110V	2	39,00	78,00
54	ESTROBOSCOPIO	METÁLICO (AEG) (A/N) (133) UNIVERSAL 141 TIPO LBS	1	56,00	56,00
55	ESTROBOSCOPIO	METÁLICO (GENERAL RADIO) (A/N) (10) TIPO 1531 PATENTE 2977508- 3350602	3	56,00	168,00
56	EXTINGUIDOR DE INCENDIOS	METÁLICO (GENRAL) (ROJO) (6)	1	24,00	24,00
57	FRECUENCÍMETRO	MERCURIO (HEWLETT PACKARD) (A/N) (34) ELECTRONICO	1	100,00	100,00
58	FRECUENCÍMETRO	METÁLICO (AEG) (A/N) (52(DOBLE 220 V	1	80,00	80,00
59	FRECUENCÍMETRO	METÁLICO (SACI) (A/N) 56-64 Hz CLASE 0.5	4	60,00	240,00
60	FRECUENCÍMETRO	METÁLICO (GOSSEN) (A/N) (179) ANAOLOGICOS 100/220/380 V	1	60,00	60,00
61	FRENO FOUNCAULT	METÁLICO (A/N) (PLOMO) (100) de 110 V, 1800 rpm, No 2 CH, 4 pesas	1	33,00	33,00
62	GENERADOR	METÁLICO (A/N) (A/N) DE RELUCTANCIA (TESIS PEDRO TOINGA)	1	238,00	238,00
63	GENERADOR	METÁLICO (YEW) (A/N) (1) PARA TACÓMETRO , TIPO 2611-00, 500/1000/2000/5000 rpm	9	238,00	2142,00
64	IMPRESORA	PLÁSTICO (EPSON) (BLANCO) (274) LQ-1070 DE 24 PINES	1	33,30	33,30
65	INDICADOR	ESTAÑO (YEW) (A/N) (115) PARA TACÓMETROS POETATILES. TIPO VPF	2	4,00	8,00
66	INDICADOR	METÁLICO (YEW) (A/N) (6) PARA TACÓMETROS , 500/1000/2000, TIPO 2601-00	3	10,00	30,00
67	INSTRUMENTOS PARA MEDIR	MADERA / METALICO (GOSSEN) (A/N) (9) 200/1000/2000 rpm TIPO ZYKLOMAT EN FORMA DE PISTOLA	3	0,16	0,48
68	INTERRUPTOR	METÁLICO (OERLIKON) (A/N) (36)	1	20,00	20,00
69	LUXOMETRO	METÁLICO (GOSSEN) (A/N) (50) LUX CON CELULA SEPARADA EN LA MANIJA	1	180,00	180,00
70	MÁQUINA	METÁLICO (HAMPDEN) (PLOMO) (3) Electricas	2	470,00	940,00
71	MÁQUINA	(95) METÁLICO (A/N) (VERDE) 1.- 1 Motor 220/380 V, 5 CV, 3450 rpm, marca CETEL, tipo S-611, # 20 2.- 1 Amplidina 220 v, 10.5 A, 3450 rpm, marca CETEL, tipo S-611, # 20, 2.3 KW. 3.- 1 Base soldada # 141885B. 4.- 1 Acoplamiento semielastico.	1	810,00	810,00
72	MÁQUINA	(85) METÁLICO (CETEL) (A/N) 1.- 1 inducido con colector, en el Ordinal 84 2.- 1 estator 1800 rpm, marca CETEL, serie # 141805A, 220/230 V CA 3.- 1 rotor de bobina a 3 anillos.	1	320,00	320,00

73	MÁQUINA	(84) METÁLICO (CETEL) (A/N) 1.- 1 Base sin # en la mesa No. 1. 2.- 1 Acoplamiento en la Maquina 85. 3.- 1 Maquina CC, 110 V, 1.7 CV, 1800 rpm, marca CETEL, tipo S-611, # 17, # 141804A - 141821A 4.- 1 Juego de polos compound (shunt), de 2 unidades.	1	720,00	720,00
74	MÁQUINA	(83)METÁLICO (CETEL) (A/N) 1.- 1 Motor CA 220/380 V, 4 CV, 1800 rpm, marca CETEL, tipo S611, # 16 2.- 1 Dinamo CC, 110 V, 2 KW, 1800 rpm, marca CETEL, Exitacion independiente, # 16 3.- 1 Dinamo shunt, 110 V, 200 W, 1800 rpm, marca CETEL, Dinamo Shunt # 16 4.- 1 Motor 110 V, 2 CV, 1800 rpm, serie # 141882A 5.- 1 Base soldada # 141839A 6.- 2 Acoplamientos semielasticos.	1	550,00	550,00
75	MÁQUINA	(87) METÁLICO (A/N) (A/N) COMBINADA CONMUTATRIZ CA/CC 2 KW, 110, 1800 RPM, CON: 1.- 1 Conmutariz CA/CC 110 V, 1800 rpm # 10, # 141873A 2.- 1 Transformador de 2 KVA, serie # PE752918, tipo S-611. # 10 3.- 1 Interruptor centrifugal, marca CETEL.	1	350,00	350,00
76	MÁQUINA	METÁLICO (SIEMENS) (A/N) (137) Combinada Convertidor trifásico: 1 Motor 4.1 KW No 67514569/01; Generador 3.5 KVA, No E062949901001	1	310,00	310,00
77	MÁQUINA	METÁLICO (BROWN BOVERI) (A/N) (29) Con: 1 motor trifásico No 299072, tipo MSP34 y 1 Dinamo A303820 tipo GC32	1	820,00	820,00
78	MÁQUINA	(95) +METÁLICO (GENERAL ELECTRIC) (A/N) UNA MAQUINA COMBINADA, CON: 1.- 1 Motor 220/380 V, 5 CV, 3450 rpm, marca CETEL, tipo S-611, # 20 2.- 1 Amplidina 220 v, 10.5 A, 3450 rpm, marca CETEL, tipo S-611, #'20, 2.3 KW. 3.- 1 Base soldada # 141885B. 4.- 1 Acoplamiento semielastico.	1	820,00	820,00
79	MÁQUINA	METÁLICO (HAMPDEN) (A/N) (6) Combinada trifásica	2	590,00	1180,00
80	MÁQUINA	(88) METÁLICO (A/N) (A/N) UNA MAQUINA COMBINADA TRIFASICA A COLECTOR, CON: 1.- 1 Motor trifasico 220/380, 0,85/3.3 KW, tipo S-611, # 19 2.- 1 Regulador de velocidad 675 a 2500 rpm. 3.- 1 Servomotor tipo DSO # 94967	1	600,00	600,00
81	MEDIDOR	METÁLICO (WESTOM) (A/N) (249) DE ANGULO DE FASE, FASIMETRO	1	140,00	140,00
82	MEDIDOR	METÁLICO (GOSSEN) (A/N) (10) DE TEMPERATURA TIPO MAVOTHERM DIGITAL II	2	33,00	66,00
83	MEDIDOR DE FACTOR	METÁLICO (NORMA) (A/N) (52) DE POTENCIA TRIFACISCO	3	117,00	351,00
84	MEDIDOR DE FACTOR	METÁLICO (NORMA) (A/N) (112) DE POTENCIA (FACIMETRO) MONOFASICO	3	117,00	351,00
85	MEDIDOR DE FACTOR	METÁLICO (NORMA) (A/N) (121) DE POTENCIA (FACIMETRO)	2	117,00	234,00
86	MEDIDOR DE FACTOR	METÁLICO (NORMA) (A/N) 55) DE WEBWE 10-4 W 0-75	1	117,00	117,00
87	MILIAMPERÍMETRO	METÁLICO (A/N) (A/N) (246) DC 0-30 Ma	1	100,00	100,00
88	MILIVOLTÍMETRO	METÁLICO (NORMA) (A/N) (19) CC 60mV	2	100,00	200,00
89	MILIVOLTÍMETRO	METÁLICO (A/N) (A/N) (116) PORTATILES DC 60/150/600 mV CLASE 1.5	3	100,00	300,00
90	MONITOR	PLÁSTICO (PC PARTINER) (BLANCO) (275)	1	25,20	25,20
91	MOTOR	HIERRO (HAMPDEN) (A/N) (4) de rotor bobinado	2	550,00	1100,00
92	MOTOR	HIERRO (BROWN BOVERI) (A/N) (30) Tipo Me-36	1	600,00	600,00
93	MOTOR	HIERRO (THOMAS THRIGE) (A/N) (67) monofásico con arranque capacitivo 1730 rpm, tipo HMC3,	1	400,00	400,00
94	MOTOR	HIERRO (THRIGE) (A/N) (69) MONOFÁSICO DE INDUCCIÓN 0.6 HP, 1720 RPM	1	300,00	300,00
95	MOTOR	HIERRO (CETEL) (A/N) (92) sincronico a reluctancia 220/380 V 1800 rpm	1	550,00	550,00
96	MOTOR	PLÁSTICO (THOMAS THRIGE) (A/N) (247) Trifásico 208/360 V 1700 rpm Tipo HLV3,	1	700,00	700,00
97	MOTOR	HIERRO (OERLIKON) (A/N) (40) Trifásico a corto circuito Tipo 8624	1	560,00	560,00
98	MOTOR	HIERRO (CETEL) (A/N) (14) Trifásico con anillos 220/380 V 5.5 HP, 1740 rpm No 3	1	510,00	510,00

99	MOTOR	HIERRO (ERCOLE MARELLI) (A/N) (85) Trifásico de inducción 1.15 HP , Tipo AN10/4	1	560,00	560,00
100	MOTOR	HIERRO (CETEL) (A/N) (81) CC 110 V 3.5 CV, 1800 rpm Tipo S 6-11	2	710,00	1420,00
101	MOTOR	(2) HIERRO (HAMPDEN) (A/N)	2	310,00	620,00
102	MOTOR	HIERRO (HAMPDEN) (A/N) (5) de inducción trifásica	2	220,00	440,00
103	MOTOR	HIERRO (HAMPDEN) (A/N) (7) de 2 HP, 72A	3	710,00	2130,00
104	MOTOR	HIERRO (WESTINNGHOUSE) (A/N) (100) generador de CA, 31. 26KVA. 208/120V	1	920,00	920,00
105	MOTOR	(1) HIERRO (HANPDEN) (A/N)	2	920,00	1840,00
106	MOTOR ASINCRONICO	HIERRO (A/N) (A/N) (94) a condensador 115/230 V, 1740 rpm, 328-47380	1	300,00	300,00
107	MOTOR ASINCRONICO	HIERRO (A/N) (A/N) (90) Bifasico 0.5 CV, 1800 rpm, No 901890A tipo s611, No 15.	1	510,00	510,00
108	MOTOR DE CC	HIERRO (THE LOUIS ALLISCO) (A/N) (98) 1750 rpm, 230 V, 20 A, conexion shunt, tipo OGNA	1	800,00	800,00
109	MOTOR DE REPULSION	HIERRO (CETEL) (A/N) (93) 220V, 0.3 CV, 1800 rpm	1	510,00	510,00
110	MOUSE	PLÁSTICO (MIC) (BLANCO) (273)	1	1,48	1,48
111	MULTÍMETRO	METÁLICO (KETHLEY) (A/N) (7) DIGITAL	5	130,00	650,00
112	MULTÍMETRO	METÁLICO (HUNG CHANG) (A/N) (270) ANALOGO	2	73,00	146,00
113	OSCILOSCOPIO	PLÁSTICO (GOULDS) (A/N) OPCION No 4022, CON INTERFASE INCORPORADO MOD. IEEE 488 TIPO 4024 No445	1	394,70	394,70
114	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) (25) tipo 564B	1	1.463,72	1463,72
115	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) (14) CON RETENCION DE IMAGEN	2	1.463,72	2927,44
116	OSCILOSCOPIO	PLÁSTICO (A/N) (AZUL) (28)	2	540,00	1080,00
117	PANTALLA	METÁLICO (KNOX ESPECTADOR) (NEGRO) CON TRIPODE	1	550,00	550,00
118	PANTALLA	METÁLICO (DRAPER) (BLANCO) (33) DE 502 X 50"	1	700,00	700,00
119	PORTAOSCILOSCOPIO	METÁLICO (HEWLETT PACKARD) (A/N)	1	15,00	15,00
120	POTENCIÓMETRO	ACERO (CHAUVIN ARNDUX) (A/N) (119) Piro 1.5 V con adaptador	1	13,00	13,00
121	PROYECTOR	METÁLICO (ORION) (PLOMO) (3) DE CUERPOS OPACOS O EPISCOPIO	1	241,00	241,00
122	PROYECTOR	METÁLICO (A/N) (NEGRO) (2) DE SLYTTES AV-341-H, LENTE EKTANAR 102mm F:2.8,1 LENTE ZOON FF 150mm	1	138,00	138,00
123	PUENTE	METÁLICO (CHAUVIN ARNDUX) (A/N) (118) DE THOMSON CON ACCESORIOS	2	80,00	160,00
124	PUENTE DE WEASTONE	METÁLICO (YEW) (A/N) (1) TIPO L-3, No N2020D20 - N2020D31	2	80,00	160,00
125	PUPITRE DE MANDO	(75) METÁLICO (SIEMENS) (PLOMO)	2	39,00	78,00
126	PUPITRE EXPERIMENTAL	METÁLICO (WESTINNGHOUSE) (PLOMO) (11) CON 8 ITEMS 1.- 1 Motor Tachometer 2.- Motor CC, 3 HP, 240 V, marca WESTINGHOUSE, tipo SK, serie # 1 S-64 3.- 1 Torquemeter con dispositivo de control 4.- 1 Generalized machine, estilo 378P123G01. 5.- 1 Motor CC 1/4 HP. 1740 rpm, style 319P031G01-A 6.- 1 Tacometro 7.- 1 Base marca WESTINGHOUSE. 8.- 1 Mesa estructura metálica con tablero de madera.	1	2.920,00	2920,00

127	PUPITRE EXPERIMENTAL	METÁLICO (AEG) (PLOMO) (108) CON ACCESORIOS 1.- Pupitre experimental CC marca AEG, con accesorios: a.- 4 Máquinas marca AEG, tipo 627, series # 667795-667805-667813-667992 b.- 1 Tacómetro de rpm. c.- 8 Interruptores. d.- 10 Reóstatos de: 4 de 24 Ohm, 3 A # N41919-N41920-N41921-N41922 2 de 1700 Ohm, 0.45 A # N41925-N41926. 2 de 6.7 Ohm, 5 A # N41923-N41924. 2 de 6.7 Ohm, 5 A # N41923-N41924. 2 de 11.8 Ohm, 3.3 A # N41927-N41928. e.- 1 Freno de prony f.- 7 acoples o adaptadores 2.- Pupitre experimental CA, marca AEG, con accesorios: a.- 4 Máquinas marca AEG: 1 de CC tipo EV45 # 456301 2 de CA tipo DGA/4 serie # 456302-456303 1 de CA tipo A 2.2 serie # 9007338 b.- 1 Tacómetro de rpm b.- 1 Tacómetro de rpm c.- 14 Interruptores d.- 7 Reóstatos de: 3 de 4.8 Ohm, 12 A series # 2 s/n; 1 N41933. 1 de 16 Ohm, 6.5 A, serie # N41929 3 de 600 Ohm, 1 A, serie # N41930-N41931-N41942. e.- 1 Freno de prony f.- 7 Acoples o adpatadores 3.- Máquina eléctrica elemental didáctica a.- 9 Piezas componentes b.- 7 Conductores de varilla de arco 4.- Grupo didáctico de transformadores: a.- 10 piezas nucleos de hierro b.- 8 Bobinas c.- 1 Bobina circular.5.- 2 aisladores 6.- 1 anillo de Founcaul 7.- 1 Pie con lámina de pieza (fungible) 8.- 1 anillo de aluminio (fungible) 9.- 2 Placas de acero (FUNGIBLE) 10.- 1 LLave mixta boca corona. 11.- Dispositivo mostrador con 6 boquillas 12.- 1 Espejo rotatorio con base 13.- 1 Conmutador bipolar (fungible) 14.- 1 Banco condensador 15.- 1 Reóstato de 1000 Ohm, # 40550 16.- 1 Electroscopio 17.- 1 Voltímetro con hierro móvil 0-30-520 V 18.- 1 Amperímetro de bobina móvil 0-3 12 A.	1	2.850,00	2850,00
128	RECTIFICADOR	HIERRO (FERRATI) (A/N) (195) de enseñanza con alimentación trifásica 220 V, con transformador movil serie No 156433	1	370,00	370,00
129	RECTIFICADOR	HIERRO (SIEMENS) (A/N) (74) estatico tipo vertical, tipo GL3-D115+115/100W/5/643	1	290,00	290,00
130	REGULADOR	HIERRO (SIEMENS) (A/N) (71) De doble inducción	1	232,00	232,00
131	REOSTATO	METÁLICO (CENCO) (VERDE) (11) CAT. 82910-10 DE 1.5 A, 177 Ohm	1	10,00	10,00
132	REOSTATO	METÁLICO (REO) (NEGRO) (90) DE 10 Ohm, 5 A	6	10,00	60,00
133	REOSTATO	METÁLICO (CENCO) (NEGRO) (192) DE 10-23 Ohm,20-42 A , CAT. 829652	4	10,00	40,00
134	REOSTATO	METÁLICO (CENCO) (NEGRO) (179) DE1436 Ohm,0.54 A, CAT. 829106	2	10,00	20,00
135	REOSTATO	METÁLICO (CENCO) (NEGRO) (189) DE 17 Ohm, 6.2 - 4.4 A. CAT. 8291514	4	10,00	40,00
136	REOSTATO	METÁLICO (CENCO) (NEGRO) (182) DE 177 Ohm, 1.5 A. CAT. 8291010	4	10,00	40,00
137	REOSTATO	METÁLICO (CENCO) (NEGRO) (185) DE 22Ohm, 4.4 A CAT. 8291010	4	10,00	40,00
138	REOSTATO	METÁLICO (CENCO) (NEGRO) (190) DE 23-5 Ohm 15-28 A, CAT. 829105	6	10,00	60,00
139	REOSTATO	METÁLICO (CENCO) (NEGRO) (186) DE 2.8 Ohm 12.3 A, CAT 8291017	4	10,00	40,00
140	REOSTATO	METÁLICO (CENCO) (NEGRO) (188) DE 33 Ohm, 4.4 A, CAT 8291513	4	10,00	40,00
141	REOSTATO	METÁLICO (CENCO) (NEGRO) (181) DE 357 Ohm, 1.1 A, CAT 829108	5	10,00	50,00
142	REOSTATO	METÁLICO (REO) (NEGRO) (91) DE 3.30 Ohm, 9 A,	9	10,00	90,00
143	REOSTATO	METÁLICO (REO) (NEGRO) (91) DE 3.30 Ohm, 9 A,	1	10,00	10,00
144	REOSTATO	METÁLICO (CENCO) (NEGRO) /177) DE 4050 Ohm, 0.30 A, CAT. 829104	2	10,00	20,00
145	REOSTATO	METÁLICO (CENCO) (NEGRO) (184) DE 44 Ohm, 3.1 A CAT. 8291012	4	10,00	40,00
146	REOSTATO	METÁLICO (CENCO) (NEGRO) (176) DE 5700 Ohm, 0.25 A, CAT. 829103	2	10,00	20,00
147	REOSTATO	METÁLICO (CENCO) (NEGRO) (191) DE 5-1.1 Ohm, 28-60 A, CAT. 829653	4	10,00	40,00

148	REOSTATO	METÁLICO (CENCO) (NEGRO) (187) DE 66 Ohm, 3.1 A. CAT. 8291512	4	10,00	40,00
149	REOSTATO	METÁLICO (CENCO) (NEGRO) (180) DE 750 Ohm, 0.77 A, CAT. 829107	5	10,00	50,00
150	REOSTATO	METÁLICO (CENCO) (NEGRO) (183) DE 89 Ohm, 2.2 A, CAT. 8291011	4	10,00	40,00
151	REOSTATO	METÁLICO (CENCO) (NEGRO) (174) DE W-20 Ohm, 5.9 A,	3	10,00	30,00
152	REOSTATO	METÁLICO (CENCO) (NEGRO) (175) DE W-30 Ohm 5.3 A	3	10,00	30,00
153	REOSTATO	METÁLICO (CENCO) (NEGRO) (176) DE W-40 Ohm,	1	10,00	10,00
154	REOSTATO	METÁLICO (CRESSAL) (N/N) (232) CIRCULAR DE 0.1/2. 58 A,1120 Ohm, TIPO S500BB, MANUAL	2	10,00	20,00
155	REOSTATO	METÁLICO (CRESSAL) (N/N) (227) CIRCULAR 2.5/0.5 A, 200 Ohm, TIPO 5300 FB/S	2	10,00	20,00
156	RESISTENCIA	PLÁSTICO (NORMA) (A/N) (122) Para vatímetro	2	10,00	20,00
157	RESISTENCIA	METÁLICO (CETEL) (N/N) (13) DE CARGA 10.5 A, TIPO S611	1	15,00	15,00
158	RESISTENCIA	METÁLICO (CETEL) (A/N) (5) IPO S611	1	15,00	15,00
159	RESISTENCIA	METÁLICO (CETEL) (A/N) (103) DE CARGA CC 2KW, 110 V, TIPO S 611	1	15,00	15,00
160	RESISTENCIA	METÁLICO (CETEL) (A/N) (6) INDUCTIVA 2.2 KVA. TIPO 6611	1	18,00	18,00
161	RESISTENCIA	METÁLICO (KETHLEY) (A/N) (8) PARA MEDIR CORRIENTE,DE HA-50 50 A, 50 MV	1	9,00	9,00
162	RESISTENCIA	METÁLICO (CETEL) (A/N) (2) DE CARGA 2 KW, 110V TIPO S611	3	10,00	30,00
163	RESISTENCIA	METÁLICO (CETEL) (A/N) (1) DE CARGA TRIFASICA 220/380 V, 25.5 KW,TIPO S611	2	8,00	16,00
164	RESISTENCIA	METÁLICO (NORMA) (A/N) (62) SHUNT EN PARALELO 30-60-120 A,	2	8,00	16,00
165	RESISTENCIA	MELAMINICO (NORMA) (A/N) (64) PARA VATIMETRO	3	10,00	30,00
166	RESISTENCIA	METÁLICO (NORMA) (A/N) (111) PARA VATIMETROS	3	10,00	30,00
167	RESISTENCIA	METÁLICO (NORMA) (A/N) (59) PARA VOLTIMETROS EN SERIE CON FACTOR DE POTENCIA	3	2,00	6,00
168	SECUENCIMETRO	METÁLICO (A/N) (A/N) (65) de 600 V	1	180,00	180,00
169	SECUENCIMETRO	METÁLICO (NORMA) (A/N) (57) SECUENDARIO DE FASE 80-400-500 V	2	180,00	360,00
170	SINCRONIZADOR ELECTRICO	METÁLICO (A/N) (A/N) TESIS: CON 1 PULSANTE MARCHA-PARO Y CONTACTOR TIPO B9	1	110,00	110,00
171	SINCRONOSCOPIO	METÁLICO (CETEL) (PLOMO) (17) O COLUMNAS DE SINCRONIZACIÓN TIPO CS EN EL ORDINAL 98	2	280,00	560,00
172	SONDA	METÁLICO (A/N) (A/N) (11) DE MEDICION DE TEMPERATURA PARA INMERSIÓN. 7KB9 401-8AB (PUNTAS)	4	70,00	280,00
173	TABLERO	METÁLICO (A/N) (A/N) (36) DE TRANSFERENCIA AUTOMATICA	1	16,28	16,28
174	TABLERO DE CONTROL PRINCIPAL	(78)METÁLICO (A/N) (PLOMO)	10	138,00	1380,00
175	TABLERO DE CONTROL PRINCIPAL	METÁLICO (A/N) (PLOMO) 76) PARA MESAS DE TRABAJO	16	180,00	2880,00
176	TELÉFONO DE MESA	PLÁSTICO (ERISCSSON) (GRIS) (180)	1	15,00	15,00
177	TRANSDUCTOR DE CORRIENTE	METÁLICO (NORMA) (A/N) (47) DE 5 VA/150-300-600 A, TIPO JZ	3	120,00	360,00
178	TRANSFORMADOR	METÁLICO (FOSTER) (A/N) (22) No 5	1	180,00	180,00
179	TRANSFORMADOR	METÁLICO (FOSTER) (A/N) (23) No 23	1	130,00	130,00
180	TRANSFORMADOR	METÁLICO (FOSTER) (A/N) (21) No 1, MONOFASICO	1	150,00	150,00
181	TRANSFORMADOR	METÁLICO (CETEL) (A/N) (101) COUT TRIFASICO, 1.50KVA, COMPUETA DE 2 UNIDADES	1	130,00	130,00
182	TRANSFORMADOR	METÁLICO (FOSTER) (A/N) (20) TRIFASICO	1	210,00	210,00
183	TRANSFORMADOR	MELAMINICO (ZENIT) (A/N) (229) VARIABLES DE CA CON GARRUCHAS	2	1.190,00	2380,00
184	TRANSFORMADOR	METÁLICO (A/N) (A/N) (230) VARIABLES CA, CON GARRUCHAS No 153	2	1.190,00	2380,00

185	TRANSFORMADOR DE CORRIENTE	METÁLICO (GENERAL ELECTRIC) (A/N) (49) DE 800-5A,CAT. 631X33	1	550,00	550,00
186	TRANSFORMADOR DE CORRIENTE	METÁLICO (NORMA) (A/N) (107) 10-25-50 A	5	550,00	2750,00
187	TRANSFORMADOR DE CORRIENTE	METÁLICO (NORMA) (A/N) (48) DE 10-25-50/5 A	3	550,00	1650,00
188	TRANSFORMADOR DE CORRIENTE	METÁLICO (AEG) (A/N) (56) DE 500-5A No 3037583	1	550,00	550,00
189	UNIDAD, AMPLIFICADOR	METÁLICO (A/N) (A/N) (26) DE TRAZO 3A72	1	150,00	150,00
190	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) (17) DE BASE DE TIEMPO	2	170,00	340,00
191	UNIDAD, AMPLIFICADOR	PLÁSTICO (TEKTRONIX) (A/N) (16) DE DOBLE TRAZO	2	100,00	200,00
192	UNIDAD, AMPLIFICADOR	PLÁSTICO (TEKTRONIX) (A/N) (15) DIFERENCIAL DOBLE	2	157,00	314,00
193	UNIDAD,BASE DE TIEMPO	METÁLICO (A/N) (A/N) (27) TIPO 2B67	1	330,00	330,00
194	VATÍMETRO	PLÁSTICO (NORMA) (A/N) (110) DE 5A, 130 - 260-520 V	3	250,00	750,00
195	VATÍMETRO	PLÁSTICO (YEW) (A/N) (8) DE BAJO FACTOR DE POTENCIA 0.2 1/5 A, 30/60 V TIPO 2041	2	250,00	500,00
196	VATÍMETRO	METÁLICO (YEW) (A/N) (4) DE BAJO FACTOR DE POTENCIA 0.2 5/25 A, 120/240 TIPO 2041	2	250,00	500,00
197	VATÍMETRO	METÁLICO (YEW) (A/N) (7) DE POTENCIA 2.0 1/5 A. 120/240 V. TIPO 2041	2	250,00	500,00
198	VATÍMETRO	METÁLICO (YEW) (A/N) (6) DDE FACTOR DE POTENCIA 0.2, 1./5 A, 30/60 V TIPO 2041	2	250,00	500,00
199	VATÍMETRO	METÁLICO (YEW) (A/N) (2) DE POTENCIA 0.2 0.2/1 A 120/240 V TIPO 2041	6	250,00	1500,00
200	VATÍMETRO	METÁLICO (A/N) (A/N) (200) DE PRECISION CA/CC, 240/60/1200/2400 W	2	250,00	500,00
201	VATÍMETRO	METÁLICO (YEW) (A/N) (5) FACTOR DE POTENCIA 0.2, 0.2/4-1 A, 30/60 V TIPO 2041	4	250,00	1000,00
202	VATÍMETRO	METÁLICO (YEW) (A/N) (3) FACTOR DE POTENCIA 0.2 1/5A 120/240V TIPO 2041	8	250,00	2000,00
203	VATÍMETRO MONOFÁSICO	METÁLICO (GOSSEN) (A/N) (6) 1/5 A 120/240/480/600 V	3	240,00	720,00
204	VATÍMETRO MONOFÁSICO	METÁLICO (NORMA) (A/N) (109) DE CA, 5A, 130-260-520 V	6	240,00	1440,00
205	VATÍMETRO TRIFÁSICO	METÁLICO (GOSSEN) (A/N) (7) 5 A, 120/240/480 V	2	270,00	540,00
206	VATÍMETRO TRIFÁSICO	METÁLICO (NORMA) (A/N) (42) 5 A/130-260 V	2	270,00	540,00
207	VATÍMETRO TRIFÁSICO	METÁLICO (YEW) (A/N) (12) DE FACTOR DE POTENCIA 0.1 -1/5 A, 120/240 V TIPO 2042	4	270,00	1080,00
208	VENTILADOR	METÁLICO (TORIN) (A/N) (271) DE 4 1/2", 115 VAC	1	99,00	99,00
209	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (9)CA 65-130-260	5	100,00	500,00
210	VOLTÍMETRO	METÁLICO (WESTOM) (A/N) (245) 0-300 V	1	100,00	100,00
211	VOLTÍMETRO	METÁLICO (AEG) (A/N) (53) CA 2 X 200 V	1	100,00	100,00
212	VOLTÍMETRO	METÁLICO (NORMA) (A/N) (1) BOBINA MOVIL CC 30-120-300-600 V	7	100,00	700,00
213	VOLTÍMETRO	METÁLICO (GOSSEN) (A/N) (1) DC/AC 6/30/120/600 TIPO PANVOLT	4	100,00	400,00
214	VOLTÍMETRO	METÁLICO (YEW) (A/N) (1O) DE CA 300/750 V TIPO 2013	3	100,00	300,00
215	VOLTÍMETRO	METÁLICO (YEW) (A/N) (9) DE CC 30/100/300/1000 V. TIPO 2011	6	100,00	600,00
216	VOLTÍMETRO	METÁLICO (SACI) (A/N) EMPOTRABLES CA ESCALA 0.300 V	4	100,00	400,00
217	VOLTÍMETRO	METÁLICO (AEC) (NEGRO)	2	100,00	200,00
		TOTAL			92.421,57

LABORATORIO DE ALTO VOLTAJE

N°	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	ACCESORIO	METÁLICO (A/N) (A/N), PARA LOS MEDIDORES DE RESISTIVIDAD DE SUELOS	2	5,70	11,40
2	AISLADOR	CERAMICA (A/N) (A/N), DE SOPORTES	12	3,00	36,00
3	AMPERÍMETRO	PLÁSTICO (WESTINNGHOUSE) (A/N), STYLE 606B690A16	1	100,00	100,00

4	AMPERÍMETRO	PLÁSTICO (AEG) (A/N)	1	100,00	100,00
5	ANALIZADOR DE ESPECTROS	METÁLICO (TEKTRONIX) (A/N)	1	2.050,00	2.050,00
6	ATENUADOR	PLÁSTICO (TEKTRONIX) (CELESTE) DE PASOS DE 50 Ohm	1	1.100,00	1.100,00
7	AUTOTRANSFORMADOR	METÁLICO (GENERAL ELECTRIC) (A/N), VARIABLE DE 3.74 KVA.280 V.	1	200,00	200,00
8	BOMBA DE VACIO	METÁLICO (A/N) (A/N), CON MOTOR AC, 1725 rpm , TIPO BC2514	1	5.200,00	5.200,00
9	CAPACITOR DE CARGA	METÁLICO (A/N) (A/N), CB 1200 pF 140 KV	1	100,00	100,00
10	COMPUTADOR	PLÁSTICO (PREMIO) (A/N) 1.- MONITOR SVGA DE 14 " MARCA PREMIO . P/N P514BA SERIE No 747RL002U01421. 1.- TECLADO MARCA PREMIO. MOD. KPQEA5ZA, SERIE 744N0508*7560. 1.- MOUSE 2 BOTONES MARCA MICROSOFT, P/N 93633, SERIE No 01772327	1	317,58	317,58
11	CONDENSADOR DE MEDIDA	METÁLICO (A/N) (A/N), CON TUBO DE FIBRA DE VIDRIO DE 1.40 cm DE LARGO X 0.25 cm, DE DIAMETRO	1	100,00	100,00
12	DIGITAL TRANSFORMER RATIOMETER	PLÁSTICO (AEMC) (AMARILLO)	1	2.995,00	2.995,00
13	EXTINGUIDOR DE INCENDIOS	METÁLICO (FYR FYTER) (ROJO)	1	150,00	150,00
14	FUENTE	METÁLICO (PERKINS) (A/N) TIPO W20H, ENTRADA 240 V; SALIDA 280 V	1	200,00	200,00
15	FUENTE DE PODER	METÁLICO (FLUKE) (A/N) DE ALTO VOLTAJE	1	200,00	200,00
16	FUNE CUT	METÁLICO (WESTINNGHOUSE) (A/N) TYPE LBU 7.8/13.8 KV .,100 A CON EXTINGUIDOR DE ARCO	1	130,00	130,00
17	FUNE CUT	METÁLICO (WESTINNGHOUSE) (A/N) TYPE LDX 7.8/13 KV., 100A	1	130,00	130,00
18	GENERADOR DE PULSOS	MELAMINICO (HEWLETT PACKARD) (A/N)	1	555,00	555,00
19	IMPRESORA	PLÁSTICO (HEWLETT PACKARD) (BLANCO) DESJET 670C	1	53,00	53,00
20	LUXOMETRO	METÁLICO (GOSSEN) (A/N) DE 1/10/500/2500. CON CELULAS SEPARADAS, TIPO TRILUX, CON MANIJA 454-320	1	180,00	180,00
21	LUXOMETRO	PLÁSTICO (AEMC) (NEGRO) CON PROTEXION DE C AUCHO COLOR AMARILLO	1	250,00	250,00
22	MÁQUINA DE ESCRIBIR	METÁLICO (HERMES STANDART) (A/N) MECANICA CARRO DE 12 " TABULACION AUTOMATICA	1	35,00	35,00
23	MEDIDOR DE RESISTENCIA	METÁLICO (SIEMENS) (A/N) DE SUELDOS	2	111,00	222,00
24	MEGAOMETRO	METÁLICO (HIPOTRONICS) (A/N) PARA MEDIR R. DE AISLANTES DE EUIPOS DE ALTO VOLTAJA, TIPO CS16-117	1	317,00	317,00
25	MEGAOMETRO	METÁLICO (BIDDLE) (A/N) PORTATIL, CON GENERADOR INCORPORADO 5 KV.. CAT. 210400	1	370,00	370,00
26	MEGGER DIGITAL	METÁLICO (METROHM) (A/N)	1	73,95	73,95
27	MILIAMPERÍMETRO	METÁLICO (WESTOM) (A/N) DE DC-50 mA GX-352	1	100,00	100,00
28	MODULOS PARA MEDIR TEMPERATURA	METÁLICO (GOSSEN) (A/N) R1, ESCALAS 20/100/200 GRADOS CENTIGRADOS T FARENGET	1	90,00	90,00
29	MOTOR DE INDUCCIÓN	HIERRO (TRIGE) (A/N) TRIFASICO DE 1.8 HP	1	1.320,00	1.320,00
30	MULTÍMETRO	METÁLICO (SIEMENS) (A/N) MULTIZED AC/CC. A - V - OHMIO,	1	75,00	75,00
31	MULTÍMETRO	PLÁSTICO (FLUKE) (A/N) AUTORANGO 4 1/2 DIGITOS	1	191,00	191,00
32	OSCILÓGRAFO	METÁLICO (HASFELY) (A/N) DE RAYOS CATODICOS, TYPO 75, SERIE, 1 TAMBOR CON CABLE DE RETARDO, 1 ANTENA DE ENCENDIDO	1	224,00	224,00
33	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) TIPO 565	1	2.532,62	2.532,62
34	OSCILOSCOPIO	PLÁSTICO (TEKTRONIX) (AZUL) DE ALMACENAMIENTO	1	2.532,62	2.532,62
35	OSCILOSCOPIO	PLÁSTICO (SIEMENS) (NEGRO) DE 200V.. TYPE Y25-003 No X02-045	1	1.130,00	1.130,00
36	PROBADOR DE ACEITE	METÁLICO (FOSTER) (A/N) DE 0 A 50 KVA, CON RECIPIENTE PARA EL ACEITE DE ELECTRODOS	1	380,00	380,00
37	PROBADOR DE ACEITE	METÁLICO (HIPOTRONICS) (A/N) TIPO CS141705	1	549,00	549,00
38	PROYECTOR	METÁLICO (DA-LITE/BESELER) (NEGRO) DE LAMINAS TRANSPARENTES	1	176,00	176,00
39	PUNTA DE CORRIENTE	METÁLICO (FLUKE) (A/N) TIPO PINZA	1	190,00	190,00
40	PUNTA PARA ALTO VOLTAJE	METÁLICO (FLUKE) (A/N) TIPO LAPIZ	1	430,00	430,00

41	REDUCTOR DE PRESION	METÁLICO (MESSER GREISHEIM) (A/N) CON 2 MANOMETROS, No 03-10.280	1	410,00	410,00
42	REGISTRADOR DE PAPEL	PLÁSTICO (JJ LLOYD INSTRUMENTS) (A/N)	1	6,52	6,52
43	TELÉFONO DE MESA	PLÁSTICO (SONOFON) (AMARILLO)	1	0,06	0,06
44	TRANSFORMADOR	PLÁSTICO (A/N) (A/N) DE 5 KVa, CON GARRUCHAS (TESIS DE GRADO)	1	1.100,00	1.100,00
45	TRANSFORMADOR	PLÁSTICO (A/N) (A/N) MONOFASICOS DE 10 KVA 1 DESARMADO	1	1.100,00	1.100,00
46	TRANSFORMADOR	PLÁSTICO (A/N) (A/N) MONOFASICOS DE 10 KVA 1 DESARMADO	1	1.100,00	1.100,00
47	TRANSFORMADOR	METÁLICO (A/N) (A/N) DE CORRIENTE 300/600/5 A, STYLE 591A286G06	1	1.100,00	1.100,00
48	TRANSFORMADOR	METÁLICO (FEDERATE) (A/N) DE DISTRIBUCION DE 3 KVA TIPO AC	1	1.100,00	1.100,00
49	TRANSFORMADOR	METÁLICO (FEDERATE) (A/N) DE DISTRIBUCION DE 3 KVA TIPO AC	1	1.100,00	1.100,00
50	TRANSFORMADOR	METÁLICO (FEDERATE) (A/N) DE DISTRIBUCION TIPO ASE, SOLO NUCLEO Y TANQUE PARA SER RECONSTRUIDO	1	1.100,00	1.100,00
51	TRANSFORMADOR	METÁLICO (WESTINNGHOUSE) (A/N) MONOFASICO DE DISTRIBUCION DE 12 470/7200/120/240 V, OSP 5 KVA	1	1.100,00	1.100,00
52	TRANSPORTADOR	METÁLICO (A/N) (A/N) PARA OSCILOSCOPIO, CON 1 GAVETA CENTRAL, CON GARRUCHAS	1	100,00	100,00
53	TRASFORMADOR	MADERA (WESTINNGHOUSE) (A/N) DE CORRIENTE DE /2000/4000 a 5 A, STYLE 597A750G13	1	1.100,00	1.100,00
54	UNIDAD CONTADOR DE FRECUENCIA Y TIEMPO UNIVERSAL	METÁLICO (TEKTRONIX) (A/N)	1	258,00	258,00
55	UNIDAD DE CONTROL	METÁLICO (EDWARDS) (A/N) PENNING, DOS43-11-00	1	260,00	260,00
56	UNIDAD DE CONTROL	METÁLICO (EDHSA) (A/N) PIRANI	1	178,00	178,00
57	UNIDAD DE TIEMPO	METÁLICO (TEKTRONIX) (A/N) DE BASE DOBLE	1	178,00	178,00
58	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N)	2	180,00	360,00
59	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) DE DOBLE TRAZO	1	180,00	180,00
60	UNIDAD, AMPLIFICADOR	METÁLICO (TEKTRONIX) (A/N) DE UN SOLO TRAZO	1	180,00	180,00
61	VATÍMETRO	METÁLICO (AEG) (A/N) DE PRECISION, CA/CC 205/600/1200/2440 W	2	250,00	500,00
62	VOLTÍMETRO	METÁLICO (WESTINNGHOUSE) (A/N) DE CA. 0-300 V, TYPE KA 241, STYLE 291B460A10	1	100,00	100,00
63	VOLTÍMETRO	METÁLICO (AEG) (A/N) DE PRECISION, CLASE 0.5 E No 446-012-311-	1	100,00	100,00
64	VOLTÍMETRO	METÁLICO (YEW) (A/N) ELECTROSTATICO AC & DC ALCANCE 25/50 KV	1	100,00	100,00
65	VOLTÍMETRO	METÁLICO (YEW) (A/N) ELECTROSTATICO AC & DC ALCANCE 5 KV, PORTATIL	1	100,00	100,00
66	VOLTÍMETRO	METÁLICO (AEG) (A/N) DE PRECISION, CA/CC 3/6/12/30 V	3	100,00	300,00
67	VOLTÍMETRO DIFERENCIAL	METÁLICO (FLUKE) (A/N)	1	212,00	212,00
		TOTAL			38.518,75

CENTRO DE CÓMPUTO GENERAL

Nº	Activo Fijo	Descripción	Cantidad	Precio Unitario $	Total $
1	COMPROBADOR	PLASTICO SINTETICO (B&k PRECISION)	1	115,00	115,00
2	COMPUTADOR	CLON (Monitor LG 14", Mod 454V, 110ACQ4795, teclado, Mouse Genius, CD Writer marca LG, 2 Parlantes)	6	987,00	5.922,00
3	COMPUTADOR	COMPAQ (Monitor de 14", teclado, Mouse) (SERVIDOR)	3	3.693,00	11.079,00
4	COMPUTADOR	CPU SUN (Monitor de 21", Mouse, Teclado, 1 Drive de respaldo) (servidor)	1	18.222,00	18.222,00
5	COMPUTADOR	CPU COMPAQ, Monitor 14", Teclado, Mouse.	1	857,75	857,75

6	EQUIPO	CODEX (De comunicación motorola)	1	312,80	312,80
7	ESCRITORIO	Tipo secretaria de 3 gavetas	1	30,00	30,00
8	EXTINGUIDOR DE INCENDIOS	METALICO (FYR FYTER), rojo de 15 libras	1	25,00	25,00
9	FAX MODEM	PLASTICO SINTETICO (ROBOTICS), EXTERNO, 56 Kbps.	1	150,00	150,00
10	HUB	PLASTICO SINTETICO (CABLETROM), de) puertos, montable en rack.	1	50,00	50,00
11	HUB	PLASTICO SINTETICO (3 Com), de 12 puertos, montable en rack.	2	60,00	120,00
12	MULTIMETRO	PLASTICO SINTETICO (KILTER) DIGITAL	1	30,00	30,00
13	RACK DE PISO	METALICO (ALCATEL), CON PANEL UTP DE 48 PUERTOS RJ45, 2 PATCH PANEL DE FIBRA ÓPTICA DE 18 PUERTOS	1	130,00	130,00
14	REGULADOR DE CORRIENTE	METALICO (SOLA)	2	25,00	50,00
15	RUTEADOR	PLASTICO SINTETICO (CISCO), WIC 2T, 2 PUERTOS SERIALES PARA INTERFAZ, CABLE.	1	2.894,41	2.894,41
16	RUTEADOR	PLASTICO SINTETICO (IBM).	1	2.956,00	2.956,00
17	RUTEADOR	PLASTICO SINTETICO (CISCO).	1	378,00	378,00
18	RUTEADOR	METALICO (CISCO), 2 TARJETAS ETHERNET 10/100 Mbps, 2 TRANSCESIVER COM.	1	600,00	600,00
19	SWITCH	METALICO (IBM), 8 PUERTOS 10BFL, 12 PUERTOS FAST ETHERNET.	1	2.290,00	2.290,00
20	TARJETA	WIC-ETH CON UN PUERTO ETHERNET PARA RUTEADOR, INSTALADO EN RUTEADOR CISCO 2611	1	350,00	350,00
21	UPS	METALICO (SMART 2200)	1	1.274,00	1.274,00
22	HUB	PLASTICO SINTETICO (3 Com), DE 12 PUERTOS, MONTABLE EN RACK.	2	50,00	100,00
23	HUB	PLASTICO SINTETICO (3 Com), DE 6 PUERTOS, MONTABLE EN RACK.	1	24,00	24,00
24	HUB	PLASTICO SINTETICO (3 Com), DE 12 PUERTOS	2	75,00	150,00
25	MONITOR	PLASTICO SINTETICO (COMPAQ)	1	70,00	70,00
26	MOTOROLA	PLASTICO SINTETICO (CODEX)	1	86,26	86,26
27	MULTIMETRO	PLASTICO SINTETICO (TRIPLETT)	1	70,00	70,00
28	TELEFONO DE MESA	PLASTICO SINTETICO (ERICSON)	1	100	10,00
		Total			48.346,22

ANEXO 3.- DIAGRAMAS DEL DISEÑO DEL SISTEMA DE CONTROL DE ACCESO FÍSICO PROPUESTO.

SIMBOLOGÍA UTILIZADA

EDIFICIO ANTIGUO EX FACULTAD DE INGENIERÍA ELÉCTRICA

- Planta Segunda
- Planta Primera
- Planta Baja
- Planta Subsuelo

EDIFICIO DE ADMINISTRACIÓN

- Planta Subsuelo

SISTEMA DE CONTROL DE ACCESO VEHICULAR

CUADRO DE DISTRIBUCIÓN DE RED

CUADRO DISTRIBUCIÓN DE RED DEL SISTEMA DE CONTROL DE ACCESO

Ubicación del panel de control de acceso: **Planta Segunda**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-04-03	Lab. Sistemas Digitales
2	P2-01-04-03	Lab. Redes
3	P3-01-04-03	Lab. Postgrado
4	P4-01-04-03	Lab. Comunicaciones
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-04-03	Lab. Sistemas Digitales
2	I2-01-04-03	Lab. Redes
3	I3-01-04-03	Lab. Postgrado
4	I4-01-04-03	Lab. Comunicaciones
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-01-04-03	Lab. Sistemas Digitales
2	C2-01-04-03	Lab. Redes
3	C3-01-04-03	Lab. Postgrado
4	C4-01-04-03	Lab. Comunicaciones

Ubicación del panel de control de acceso: **Planta Segunda**		
Número del panel de control de acceso : **02**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-02-04-03	Lab. Control y Computación
2	B2-02-04-03	Cuarto de Telecomunicaciones
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-02-04-03	Lab. Control y Computación
2	I2-02-04-03	Cuarto de Telecomunicaciones
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-02-04-03	Lab. Control y Computación
2	C2-02-04-03	Cuarto de Telecomunicaciones
3		Libre
4		Libre

Ubicación del panel de control de acceso: **Planta Primera**		
Número del panel de control de acceso : **03**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-03-03-03	Lab. Circuitos Eléctricos
2	P2-03-03-03	Lab. Electrónica
3	P3-03-03-03	Lab. Diseño Electrónico
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-03-03-03	Lab. Circuitos Eléctricos
2	I2-03-03-03	Lab. Electrónica
3	I3-03-03-03	Lab. Diseño Electrónico
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-03-03-03	Lab. Circuitos Eléctricos
2	C2-03-03-03	Lab. Electrónica
3	C3-03-03-03	Lab. Diseño Electrónico
4		Libre

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **04**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-04-02-03	Entrada 2
2	P2-04-02-03	Lab. Electrónica de potencia EL-101
3	P3-04-02-03	Lab. Electrónica de potencia EL-127
4	P4-04-02-03	Lab. Control Industrial
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1		Libre
2	I2-04-02-03	Lab. Electrónica de potencia EL-101
3	I3-04-02-03	Lab. Electrónica de potencia EL-127
4	I4-04-02-03	Lab. Control Industrial
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-04-02-03	Entrada 2
2	C2-04-02-03	Lab. Electrónica de potencia EL-101
3	C3-04-02-03	Lab. Electrónica de potencia EL-127
4	C4-04-02-03	Lab. Control Industrial

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **05**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-05-02-03	Entrada 1
2	P2-05-02-03	Control de acceso vehicular número 3 E/S
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1		Libre
2	I2-05-02-03	Control de acceso vehicular número 3 E/S
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-05-02-03	Entrada 1
2	B2-05-02-03	Control de acceso vehicular número 3 E/S
3		Libre
4		Libre

Ubicación del panel de control de acceso: **Planta Subsuelo**		
Número del panel de control de acceso : **06**		
Nombre de la red de control de acceso : **Edificio Antiguo de Eléctrica**		
Número de lazo de control de acceso : **03**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-06-01-03	Lab. Alto Voltaje
2	P2-06-01-03	Lab. Taller Eléctrico
3	P3-06-01-03	Lab. Máquinas Eléctricas
4	P4-06-01-03	Lab. SEP
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-06-01-03	Lab. Alto Voltaje
2	I2-06-01-03	Lab. Taller Eléctrico
3	I3-06-01-03	Lab. Máquinas Eléctricas
4	I4-06-01-03	Lab. SEP
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-06-01-03	Lab. Alto Voltaje
2	C2-06-01-03	Lab. Taller Eléctrico
3	C3-06-01-03	Lab. Máquinas Eléctricas
4	C4-06-01-03	Lab. SEP

Ubicación del panel de control de acceso: **Planta Subsuelo**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Administración**		
Número de lazo de control de acceso : **06**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-01-06	Centro de cómputo general
2	B-01-01-06	Centro de cómputo general
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-01-06	Centro de cómputo general
2	I2-01-01-06	Centro de cómputo general
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	C1-01-01-06	Centro de cómputo general
2	C2-01-01-06	Centro de cómputo general

CUADRO DISTRIBUCIÓN DE RED DEL SISTEMA DE CONTROL DE ACCESO

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Ciencias Biológicas**		
Número de lazo de control de acceso : **01**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-02-01	Control de acceso vehicular número 1 E
2	P2-01-02-01	Control de acceso vehicular número 1 S
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-02-01	Control de acceso vehicular número 1 E
2	I2-01-02-01	Control de acceso vehicular número 1 S
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	M1-01-02-01	Control de acceso vehicular número 1 E
2	M2-01-02-01	Control de acceso vehicular número 1 S
3		Libre

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Ciencias Nucleares (Casa Mata)**		
Número de lazo de control de acceso : **02**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-02-02	Control de acceso vehicular número 2 E
2	P2-01-02-02	Control de acceso vehicular número 2 S
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-02-02	Control de acceso vehicular número 2 E
2	I2-01-02-02	Control de acceso vehicular número 2 S
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	M1-01-02-02	Control de acceso vehicular número 2 E
2	M2-01-02-02	Control de acceso vehicular número 2 S
3		
4		

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Metalurgia extractiva (Tecnólogos)**		
Número de lazo de control de acceso : **04**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-02-04	Control de acceso vehicular número 4 E/S
2		
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-02-04	Control de acceso vehicular número 2 E/S
2	Libre	Libre
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	M1-01-02-04	Control de acceso vehicular número 2 E/S

Ubicación del panel de control de acceso: **Planta Baja**		
Número del panel de control de acceso : **01**		
Nombre de la red de control de acceso : **Edificio Antiguo de Química**		
Número de lazo de control de acceso : **05**		
Lectoras		
Puerto	**Id de cable**	**Nombre del área**
1	P1-01-02-05	Control de acceso vehicular número 2 E
2	P2-01-02-05	Control de acceso vehicular número 2 S
3		Libre
4		Libre
Interruptores		
Puerto	**Id de cable**	**Nombre del área**
1	I1-01-02-05	Control de acceso vehicular número 2 E
2	I2-01-02-05	Control de acceso vehicular número 2 S
3		Libre
4		Libre
Reles de salida		
Puerto	**Id de cable**	**Nombre del área**
1	M1-01-02-05	Control de acceso vehicular número 2 E
2	M2-01-02-05	Control de acceso vehicular número 2 S
3		Libre
4		Libre

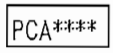
ANEXO 4.- CÓMPUTO DE MATERIALES A SER UTILIZADOS EN LA IMPLEMENTACIÓN DEL SISTEMA DE CONTROL DE ACCESO FÍSICO PROPUESTO.

CÓMPUTO DE MATERIALES

Red de Control de Acceso Antiguo Edificio Eléctrica

Descripción	Unidad Medida	Cantidad	Subsuelo		Planta Baja		Primera Planta		Segunda Planta	
			Calculado	Estimado	Calculado	Estimado	Calculado	Estimado	Calculado	Estimado
Diseño Seguridad										
PUERTAS METALICAS 0.90x2m, C/CERRADURA DE POMO KWIIKSET	u	12	2	2	3	3	1	1	6	6
PUERTAS METALICAS BATIENTES 1,50x2, C/CERRADURA DE POMO KWIKSET	u	4	2	2	0	0	2	2	0	0
GABINETE BYPASS 30A	u	1	1	1	0	0	0	0	0	0
FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	4	1	1	1	1	1	1	1	1
CONTACTOS MAGNETICOS	u	18	4	4	5	5	3	3	6	6
TARJETAS PROXIMIDAD HID	u	200	50	50	50	50	50	50	50	50
CONVERTIDORES RS-485 ETHERNET	u	1	0	0	0	0	0	0	1	1
BRAZOS PEQUEÑOS PARA CERRAR PUERTA	u	18	4	4	5	5	3	3	6	6
SISTEMA ANTENA CLIENTE	u	1	0	0	0	0	0	0	1	1
SOPORTE PARA ANTENAS 2m C/BASE METALICA	u	1	0	0	0	0	0	0	1	1
CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	1		0	0	0	0	0	1	1
CABLE UTP 04 PAR C5E	m	630	74	80	364	380	63	70	99	100
CABLE SPT 2X22 AWG	m	660	148	150	170	180	126	130	198	200
TUBO EMT 3/4" X3M	u	70	15	20	22	25	11	15	8	10
TUBO EMT 1" X3M	u	20	2	5	3	5	0	0	6	10
CANALETA PVC 20X12X2M LISA	u	40	8	10	10	10	8	10	7	10
INTERRUPTOR SIMPLE C/TAPA	u	18	4	4	4	4	3	3	7	7
CAJA PVC 10X5X4CM C. ALMENDRA	u	18	4	4	4	4	3	3	7	7
PC ACCESO (4 PUERTAS)	u	6	1	1	2	2	1	1	2	2
LECTOR DE PROX	u	21	4	4	9	9	3	3	5	5
CERRADURA ELECTROMAGNETICA	u	18	4	4	5	5	3	3	6	6
HAND PUNCH	u	1	0	0	0	0	0	0	1	1
LOOP	u	2	0	0	2	2	0	0	0	0
BRAZO MECANICO	u	1	0	0	1	1	0	0	0	0
CONSUMIBLES										
AMARRAS PLASTICAS 20CM	u	120	30	30	30	30	30	30	30	30
TACO F-6	u	246	71	63	64	68	41	51	49	64
TORNILLO COLEPATO 1X8	u	246	71	63	64	68	41	51	49	64
TORNILLO COLEPATO 1/2X8	u	120	22	26	44	50	20	24	16	20
SILICONA	u	20	5	5	5	5	5	5	5	5

SIMBOLOGÍA UTILIZADA

SIMBOLO	DESCRIPCIÓN
	PERFORACIÓN EN LOZA
	SENTIDO DE ENTRADA SALIDA DE VEHICULOS
	CAJA DE PASO
	TUBERÍA METÁLICA
	CONTROL DE ACCESO VEHICULAR
	IDENTIFICACIÓN DE PANEL DE CONTROL DE ACCESO
	BRAZO MECÁNICO
	LECTOR DE TARJETAS DE PROXIMIDAD
	LOOP
	LECTOR BIOMÉTRICO BASADO EN LA GEOMETRÍA DE LA MANO
	CERRADURA ELECTROMAGNÉTICA
	INTERRUPTOR
	TOMACORRIENTE DOBLE 121 V
	TABLERO DE DISTRIBUCIÓN ELÉCTRICO

PCA0103 Significa Panel de control número 1 de la red de control de acceso número 3

SIERRAS	u	8	2	2	2	2	2	2	2	2
CONSUMIBLES CANALETA										
UNION 20X12	u	20	5	5	5	5	5	5	5	5
CONSUMIBLES TUBERIA										
CAJA EMT 12X12CM	u	60	11	13	22	25	10	12	8	10
TAPA CAJA EMT 12X12CM	u	60	11	13	22	25	10	12	8	10
CONECTOR EMT 3/4"	u	140	30	40	44	50	22	30	16	20
CONECTOR EMT 1"	u	40	4	10	6	10	0	0	12	20
UNION EMT 3/4"	u	74	16	21	23	26	12	16	9	11
UNION EMT 1"	u	24	3	6	4	6	1	1	7	11
ABRAZADERA EMT 3/4"	u	210	45	60	66	75	33	45	24	30
ABRAZADERA EMT 1"	u	60	6	15	9	15	0	0	18	30
ALAMBRE GALVANIZADO N°, 18	Kg	4	1	1	1	1	1	1	1	1
CODO EMT 3/4"	u	8	2	2	2	2	2	2	2	2
TOTAL DISEÑO ELECTRICO										
Diseño Electrico										
CABLE TW 08 AWG, MULTIFILAR	m	100	0	0	90	100	0	0	0	0
CABLE TW 10 AWG, MULTIFILAR	m	200	0	0	180	200	0	0	0	0
CABLE TW 12 AWG, MULTIFILAR	m	38	8	10	8	10	8	10	7	8
CABLE TW 14 AWG, MULTIFILAR	m	74	16	20	16	20	16	19	14	15
TOMACORRIENTE TRIPOLAR DOBLE C/PLACA	u	4	1	1	1	1	1	1	1	1
CAJA PVC 10X5X4CM C. ALMENDRA	u	4	1	1	1	1	1	1	1	1
BREAKER 1X20A	u	2	2	2	0	0	0	0	0	0
UPS	u	1	1	1	0	0	0	0	0	0
CENTRO CARGA 04P BIIFASE	u	1	1	1	0	0	0	0	0	0
CONSUMIBLES ELECTRICO										
CINTA AISLANTE 20 YD	u	4	1	1	1	1	1	1	1	1
ETIQUETA CABLE C.VERDE	u	40	10	10	10	10	10	10	10	10
MASKING	u	4	1	1	1	1	1	1	1	1
TACO F-6	u	8	2	2	2	2	2	2	2	2
TORNILLO COLEPATO 1X8	u	8	2	2	2	2	2	2	2	2

CÓMPUTO DE MATERIALES

Control de acceso vehicular número 1 Próximo a Ciencias Biológicas

Descripción	Unidad Medida	Cantidad	Planta Baja	
			Calculada	Estimada
Diseño Seguridad				
FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	1	1	1
TARJETAS PROXIMIDAD HID	u	400	400	400
CONVERTIDORES RS-485 ETHERNET	u	1	1	1
SISTEMA ANTENA CLIENTE	u	1	1	1
SOPORTE PARA ANTENAS 2m C/BASE METALICA	u	1	1	1
CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	1	1	1
CABLE UTP 04 PAR C5E	m	200	180	200
CABLE SPT 2X22 AWG	m	200	180	200
TUBO EMT 3/4" X3M	u	100	90	100
CANALETA PVC 20X12X2M LISA	u	5	4	5
INTERRUPTOR SIMPLE C/TAPA	u	2	2	2
CAJA PVC 10X5X4CM C. ALMENDRA	u	2	2	2
PC ACCESO (4 PUERTAS)	u	1	1	1
LECTOR DE PROX	u	2	2	2
LOOP	u	2	2	2
BRAZO MECANICO	u	2	2	2
CONSUMIBLES				
AMARRAS PLASTICAS 20CM	u	30	30	30
TACO F-6	u	119	106	119
TORNILLO COLEPATO 1X8	u	119	106	119
TORNILLO COLEPATO 1/2X8	u	40	32	40
SILICONA	u	2	2	2
SIERRAS	u	1	1	1
CONSUMIBLES CANALETA				
UNION 20X12	u	5	5	5
CONSUMIBLES TUBERIA				
CAJA EMT 12X12CM	u	20	16	20
TAPA CAJA EMT 12X12CM	u	20	16	20
CONECTOR EMT 3/4"	u	200	180	200
UNION EMT 3/4"	u	101	91	101
ABRAZADERA EMT 3/4"	u	300	270	300
ALAMBRE GALVANIZADO N°, 18	Kg	1	1	1
CODO EMT 3/4"	u	12	10	12
TOTAL DISEÑO ELECTRICO				
Diseño Eléctrico				
CABLE TW 08 AWG, MULTIFILAR	m	200	180	200
CABLE TW 10 AWG, MULTIFILAR	m	400	360	400
BREAKER 1X20A	u	2	2	2
CENTRO DE CARGA BIFASICO	u	1	1	1
CONSUMIBLES ELECTRICO				
CINTA AISLANTE 20 YD	u	1	1	1
ETIQUETA CABLE C.VERDE	u	10	10	10
MASKING	u	1	1	1

COMPUTO DE MATERIALES

Control de acceso vehicular número 2 Próximo a Ciencias Nucleares

Descripción	Unidad Medida	Cantidad	Planta Baja	
			Calculada	Estimada
Diseño Seguridad				
FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	1	1	1
TARJETAS PROXIMIDAD HID	u	400	400	400
CONVERTIDORES RS-485 ETHERNET	u	1	1	1
SISTEMA ANTENA CLIENTE	u	1	1	1
SOPORTE PARA ANTENAS 2m C/BASE METALICA	u	1	1	1
CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	1	1	1
CABLE UTP 04 PAR C5E	m	200	180	200
CABLE SPT 2X22 AWG	m	200	180	200
TUBO EMT 3/4" X3M	u	100	90	100
CANALETA PVC 20X12X2M LISA	u	5	4	5
INTERRUPTOR SIMPLE C/TAPA	u	2	2	2
CAJA PVC 10X5X4CM C. ALMENDRA	u	2	2	2
PC ACCESO (4 PUERTAS)	u	1	1	1
LECTOR DE PROX	u	2	2	2
LOOP	u	2	2	2
BRAZO MECANICO	u	2	2	2
CONSUMIBLES				
AMARRAS PLASTICAS 20CM	u	30	30	30
TACO F-6	u	112	102	112
TORNILLO COLEPATO 1X8	u	112	102	112
TORNILLO COLEPATO 1/2X8	u	40	32	40
SILICONA	u	2	2	2
SIERRAS	u	1	1	1
CONSUMIBLES CANALETA				
UNION 20X12	u	5	5	5
CONSUMIBLES TUBERIA				
CAJA EMT 12X12CM	u	20	16	20
TAPA CAJA EMT 12X12CM	u	20	16	20
CONECTOR EMT 3/4"	u	200	180	200
CONECTOR EMT 1"	u	0	0	0
UNION EMT 3/4"	u	101	91	101
ABRAZADERA EMT 3/4"	u	300	270	300
ALAMBRE GALVANIZADO Nº, 18	Kg	1	1	1
CODO EMT 3/4"	u	5	3	5
TOTAL DISEÑO ELECTRICO				
Diseño Eléctrico				
CABLE TW 08 AWG, MULTIFILAR	m	200	180	200
CABLE TW 10 AWG, MULTIFILAR	m	400	360	400
BREAKER 1X20A	u	2	2	2
CENTRO CARGA 04P TRIFASE	u	1	1	1
CONSUMIBLES ELECTRICO				
CINTA AISLANTE 20 YD	u	1	1	1
ETIQUETA CABLE C.VERDE	u	10	10	10
MASKING	u	1	1	1

COMPUTO DE MATERIALES

Control de acceso vehicular número 4, Próximo a Metalurgia Extractiva

Descripción	Unidad Medida	Cantidad	Planta Segunda	
			Calculada	Estimada
Diseño Seguridad				
FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	1	1	1
CONTACTOS MAGNETICOS	u	4	4	4
TARJETAS PROXIMIDAD HID	u	400	400	400
CONVERTIDORES RS-485 ETHERNET	u	1	1	1
SISTEMA ANTENA CLIENTE	u	1	1	1
SOPORTE PARA ANTENAS 2m C/BASE METALICA	u	1	1	1
CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	1	1	1
CABLE UTP 04 PAR C5E	m	200	180	200
CABLE SPT 2X22 AWG	m	200	180	200
TUBO EMT 3/4" X3M	u	105	100	105
CANALETA PVC 20X12X2M LISA	u	5	5	5
INTERRUPTOR SIMPLE C/TAPA	u	1	1	1
CAJA PVC 10X5X4CM C. ALMENDRA	u	1	1	1
PC ACCESO (4 PUERTAS)	u	1	1	1
LECTOR DE PROX	u	2	2	2
LOOP	u	2	2	2
BRAZO MECANICO	u	1	1	1
CONSUMIBLES				
AMARRAS PLASTICAS 20CM	u	30	30	30
TACO F-6	u	120	115	120
TORNILLO COLEPATO 1X8	u	120	115	120
TORNILLO COLEPATO 1/2X8	u	40	36	40
SILICONA	u	2	2	2
SIERRAS	u	1	1	1
CONSUMIBLES CANALETA				
UNION 20X12	u	5	5	5
CONSUMIBLES TUBERIA				
CAJA EMT 12X12CM	u	20	18	20
TAPA CAJA EMT 12X12CM	u	20	18	20
CONECTOR EMT 3/4"	u	210	200	210
UNION EMT 3/4"	u	106	101	106
ABRAZADERA EMT 3/4"	u	315	300	315
ALAMBRE GALVANIZADO Nº, 18	Kg	1	1	1
CODO EMT 3/4"	u	5	5	5
TOTAL DISEÑO ELECTRICO				
Diseño Electrico				
CABLE TW 08 AWG, MULTIFILAR	m	200	180	200
CABLE TW 10 AWG, MULTIFILAR	m	400	360	400
BREAKER 1X20A	u	1	1	1
CENTRO CARGA 04P BIIFASE	u	1	1	1
CONSUMIBLES ELECTRICO				
CINTA AISLANTE 20 YD	u	1	1	1
ETIQUETA CABLE C.VERDE	u	10	10	10
MASKING	u	1	1	1

COMPUTO DE MATERIALES

Sistema Control de acceso centro de cómputo general

Descripción	Unidad Medida	Cantidad	Planta Subsuelo	
			Calculada	Estimada
Diseño Seguridad				
PUERTAS METALICAS BATIENTES 1,50x2, C/CERRADURA DE POMO KWIKSET	u	1	1	1
FUENTE DE ALIMENTACION DC, 12V / 24V, 5A	u	1	1	1
CONTACTOS MAGNETICOS	u	3	3	3
CONVERTIDORES RS-485 ETHERNET	u	1	1	1
BRAZOS PEQUEÑOS PARA CERRAR PUERTA	u	2	2	2
CORDON CONEXIÓN RJ-45/RJ45 7 PIES C.GRIS	u	1	1	1
CABLE UTP 04 PAR C5E	m	35	28	35
CABLE SPT 2X22 AWG	m	35	28	35
TUBO EMT 3/4" X3M	u	10	9	10
CANALETA PVC 20X12X2M LISA	u	4	2	4
INTERRUPTOR SIMPLE C/TAPA	u	2	2	2
CAJA PVC 10X5X4CM C. ALMENDRA	u	2	2	2
PC ACCESO N-1000-III	u	1	1	1
CERRADURA ELECTROMAGNETICA	u	2	2	2
HAND PUNCH	u	1	1	1
CONSUMIBLES				
AMARRAS PLASTICAS 20CM	u	30	30	30
TACO F-6	u	16	15	16
TORNILLO COLEPATO 1X8	u	16	15	16
TORNILLO COLEPATO 1/2X8	u	10	6	10
SILICONA	u	2	2	2
SIERRAS	u	1	1	1
CONSUMIBLES CANALETA				
UNION 20X12	u	2	2	2
CONSUMIBLES TUBERIA				
CAJA EMT 12X12CM	u	5	3	5
TAPA CAJA EMT 12X12CM	u	5	3	5
CONECTOR EMT 3/4"	u	20	18	20
UNION EMT 3/4"	u	11	10	11
ABRAZADERA EMT 3/4"	u	30	27	30
ALAMBRE GALVANIZADO N°, 18	Kg	1	1	1
CODO EMT 3/4"	u	5	5	5