INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA DE ELECTRÓNICA

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD ELECTRÓNICO EN EL DEPARTAMENTO DE FINANZAS DEL ITSA

POR

CBOS. TÉC. AVC. PUETATE RAMÍREZ RODRIGO IVÁN

Trabajo de Graduación como requisito parcial para la obtención de título de:

TECNÓLOGO EN ELECTRÓNICA

MENCIÓN INSTRUMENTACIÓN Y AVIÓNICA

2009

CERTIFICACIÓN

Certifico que el presente Trabajo de Grado fue realizado en su totalidad por el Sr. Cbos. Téc. Avc. Puetate Ramírez Rodrigo Iván, como requerimiento parcial para la obtención del título de **TECNÓLOGO EN ELECTRÓNICA MENCIÓN INSTRUMENTACIÓN Y AVIÓNICA.**

TCrn. Téc. Avc. Ing. Ángel Pérez

DIRECTOR DEL TRABAJO DE GRADO

Latacunga, Febrero 25 del 2009

DEDICATORIA

Quiero dedicarle este trabajo de graduación principalmente a Dios que me ha dado la vida, fortaleza, sabiduría y salud, a mis padres por estar ahí cuando más lo necesite y por el apoyo incondicional; en especial a mi madre por su ayuda y consejos en todo el transcurso de mi vida.

Rodrigo Puetate.

AGRADECIMIENTO

Agradezco a Dios por llenar mi vida de dicha y bendición.

A mis Padres, a quienes agradezco por su amor, cariño y comprensión. En todo momento los llevo conmigo.

Agradezco a mis hermanas por la compañía y el apoyo que me brindan. Se que cuento con ellas siempre.

Agradezco a la Fuerza Aérea por darme la oportunidad de ser mejor cada día.

Agradezco a mis maestros por su disposición y ayuda brindada.

Rodrigo Puetate.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE CONTENIDO

CAPÍTULO I

EL PROBLEMA

CAPÍTULO II

PLAN DE INVESTIGACIÓN

CAPÍTULO III

MARCO TEÓRICO

CAPÍTULO IV

EJECUCIÓN DEL PLAN METODOLÓGICO

CAPÍTULO V

FACTIBILIDAD

CAPÍTULO VI

DESARROLLO DEL TEMA

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

CAPÍTULO IV

EJECUCIÓN DEL PLAN METODOLÓGICO

CAPÍTULO V

FACTIBILIDAD

ÍNDICE DE FIGURAS

CAPÍTULO IV

CAPÍTULO VI

INDICE DE FOTOS

CAPÍTULO VI

ÍNDICE DE ANEXOS

Introducción

El Sistema de Seguridad DSC fue proyectado para proporcionarle la mayor flexibilidad y conveniencia posible.

Este equipo es capaz de monitorear dispositivos de detección de incendio, como detectores de humo y enviar un aviso si una condición de incendio fuere detectado. Una detección de incendio confiable depende de la instalación de una cantidad adecuada de detectores ubicados en puntos apropiados.

También puede monitorear dispositivos de detección de robos, utilizando detectores de movimiento y para que no existan falsas alarmas estos sensores tienen inmunidad contra mascotas de hasta veinte y cinco kilogramos (25Kg.).

Los sistemas de seguridad normalmente son muy confiables, pero podrán no funcionar en todas las condiciones y es muy importante que las personas cuiden sus pertenencias y realicen planes de evacuación en caso de existir algún incendio.

Cabe indicar que el sistema de seguridad no puede prevenir emergencias solamente es un sistema de alerta inmediata de que alguien esta en el departamento o que existe presencia de humo.

HOJA DE VIDA

DATOS PERSONALES

Nombres: Rodrigo Iván.

Apellidos: Puetate Ramírez.

Fecha de nacimiento: El ORO- Piñas, 09 de Febrero de 1987.

Nacionalidad: Ecuatoriano.

CI: 070439667-0.

Domicilio: Quito-Coop. Nuevo Amanecer Mz. 17 Casa 136.

Estado civil: Soltero.

INFORMACIÓN ACADEMICA

Primaria: Escuela Fiscal Mixta “José Peralta”.

Secundaria: Instituto Superior “Nuevo Ecuador”.

Superior: Instituto Tecnológico Superior Aeronáutico.

Cursos y Seminarios:

Suficiencia en el Idioma Inglés

Escuela de Idiomas “INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO”.

Curso de Especialización en Inteligencia

ESCUELA TÉCNICA DE LA FUERZA AÉREA.

Practicas laborales:

EMDA Sección Radares

ITSA Laboratorio de Instrumentación Virtual.

HOJA DE LEGALIZACIÓN DE FIRMAS

Del contenido de la presente investigación se responsabiliza el autor.

Cbos. Téc. Avc. Puetate Ramírez Rodrigo Iván.

DIRECTOR DE LA CARRERA DE ELECTRONICA

Ing. Pablo Pilatasig.

Latacunga, Febrero 25 del 2009

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema.

El Instituto Tecnológico Superior Aeronáutico es una institución de educación superior creada para brindar servicios de carácter educativo en las siguientes carreras: Telemática, Logística y Transportes, Electrónica mención instrumentación y aviónica, Mecánica Aeronáutica-Estructuras, Mecánica Aeronáutica-Motores y Ciencias de la Seguridad mención aérea y terrestre, a estudiantes de todos los sectores del país.

Por el constante crecimiento de la población del ITSA, se ha tornado más vulnerable a las acciones hostiles tales como: robo, fraude o sabotaje, dando lugar a inseguridad de estudiantes y público en general. Por otro lado en la actualidad una de sus debilidades es no contar con los respectivos planes de seguridad para enfrentar desastres tales como: incendios, inundaciones, condiciones climatológicas adversas y otros planes que son necesarios para proporcionar una seguridad integral.

En la actualidad, no existe un modelo único en la organización ni en la gestión de seguridad en el ITSA, lo que provoca que cada uno resuelva sus problemas y demandas con criterios propios produciéndose diferentes tratamientos para los problemas de seguridad.

El Instituto dispone de recursos físicos para el desarrollo de sus carreras, tales como edificios, estacionamientos, equipos, laboratorios, talleres y materiales, mismos que no cuentan con un sistema de seguridad para su resguardo y por tanto están propensos a daños físicos.

Este establecimiento por ser de carácter educativo posee una gran infraestructura y espacios de recreación, los cuales tienen libre acceso a las personas que laboran en esta institución y acceso controlado a las personas ajenas.

Este libre ingreso, ha provocado pérdidas y daños a los bienes del Instituto, sin que se haya identificado a sus causantes, lo que afecta al libre desempeño de los alumnos y personal administrativo que labora en la institución.

Si no se proporciona una solución, seguirá la perdida de recursos económicos, materiales, físicos y personales de los empleados que laboran en la institución provocando un malestar del personal interno y de aquellas personas que visiten la institución y por lo tanto se generaría una mala imagen institucional.

1.2 Formulación del problema

Contribuir a la optimización de la seguridad del I.T.S.A, para precautelar los recursos personales e institucionales y así mantener un normal desarrollo de sus actividades, con una adecuada calidad de vida.

1.3 Justificación e importancia

Según el Manual de Autoevaluación con Fines de Acreditación para los institutos Superiores Técnicos y Tecnológicos del Ecuador emitido por el Consejo Nacional de Evaluación y Acreditación de la educación Superior del Ecuador (CONEA), en el ámbito 4: Bienestar institucional, característica 9: estándar 9.3, en el indicador 9.3.1, indica "Verificación de la existencia de políticas de seguridad institucional. CO.EF.1.4.02 (P)"; y el estándar 9.4, en el indicador 9.4.1 indica "Verificación de que el instituto cuenta con personal especializado y equipos apropiados para su seguridad. RA.TH.1.4.01 (P)"[1]

De acuerdo al Reglamento General de Institutos Superiores Técnicos y Tecnológicos del Ecuador, Capitulo V (De las Estrategias), Art. 9; numeral 5 en donde indica que toda institución educativa debe "Prepara proyectos que permitan prevenir desastres y resolver problemas que afecten a la colectividad."[2]

1 Manual de Autoevaluación con Fines de Acreditación para los Institutos Superiores Técnicos y Tecnológicos del Ecuador.

[2] http://www.conesup.net/descargas/reglamento_institutos.pdf

Es reconocido que el ámbito educativo constituye un escenario particular en materia de necesidades de seguridad, debido a su crecimiento constante, los diferentes colegios de los cuales proceden los alumnos, la variedad de prestaciones de servicios y otros factores que aumentan la probabilidad de que los riesgos se materialicen y que sus consecuencias escapen al control.

Un sistema de seguridad óptimo debe estar compuesto por varios subsistemas, tales como un subsistema de seguridad física que ayude a evitar acciones hostiles como robos, fraudes o sabotajes; un subsistema de contingencia para desastres naturales con sus respectivos planes que ayude informar y prevenir, incendios inundaciones y condiciones climatológicas adversas y otros subsistemas que cumplan funciones adicionales en aporte a la seguridad integral.

Con lo antes indicado se logrará una institución educativa segura, donde se puedan desarrollar las actividades académicas y administrativas en un ambiente de tranquilidad, confianza, así como proyectar una buena imagen institucional.

Se beneficiaran del presente trabajo investigativo los directivos, personal docente administrativo, servicios, alumnos civiles y militares así como la Institución.

1.4 Objetivos:

1.4.1 General

* Analizar la situación actual del sistema de seguridad del ITSA, mediante un plan metodológico para determinar sus puntos críticos y desarrollar diferentes proyectos que permitan mejorar la protección de los recursos personales e institucionales.

1.4.2 Específicos

* Realizar una evaluación del sistema de seguridad actual del ITSA.
* Recopilar información para el buen desarrollo del trabajo investigativo.
* Determinar el sistema de seguridad que requiere el Instituto.

* Instalar un sistema de seguridad electrónico en el departamento de finanzas del ITSA.
* Introducir el concepto de seguridad en la conciencia colectiva e individual de los miembros del instituto mediante exposiciones.

1.5 Alcance

El presente trabajo investigativo abarca el sistema de seguridad del ITSA, que comprende sus tres áreas: administrativa (departamentos, oficinas y servicios), académica (laboratorios, aulas taller, biblioteca y aulas) y recreativa (auditorio, gimnasio, parqueaderos, canchas múltiples y prevenciones), involucrando a directivos, personal docente, administrativo, servicios y alumnos que pertenecen a la institución.

Se orientará la investigación al área administrativa por ser de mayor importancia debido a que un punto medular del instituto, ya que todo tipo de trámite se lo realiza en determinada área y contiene información de gran valor.

CAPÍTULO II
PLAN DE INVESTIGACIÓN

2.1 Modalidad básica de la investigación

* **Investigación de campo.-** Esta investigación se realizará en el sitio donde se encuentra el hecho de estudio, ésta permitirá conocer con profundidad cada uno de los componentes del problema y de esta manera obtener nuevos conocimientos en la realidad social del Instituto (investigación pura), así como analizar su situación actual para diagnosticar necesidades y dificultades.

* **Bibliográfica documental.-** Se utilizará esta modalidad, ya que se necesita revisar documentos, libros e Internet para poder obtener una mayor cantidad de información que contribuya a la realización del proyecto.

2.2 Tipos de Investigación:

* **La investigación no experimental.-** Esta técnica permitirá observar el hecho objeto de estudio sin intervenir en las posibles causas y efectos del problema, puesto que las debilidades del sistema de seguridad están latentes.

* **Investigación cuasi experimental.-** Se tomará este tipo de investigación, por la necesidad de recolectar información del personal que tuvo relación con los sistemas de seguridad anteriormente implantados. Es decir no tomaremos al azar los sujetos a ser investigados.

2.3 Niveles de investigación

* **Exploratoria.-** Se realizará mencionado nivel de investigación, ya que es necesario conocer el entorno donde existe el problema y de esta manera definirlo con una mayor precisión. Un problema bien definido permite dar soluciones efectivas.

* **Descriptiva.-** Este nivel permitirá detallar de manera concreta los componentes del objeto de estudio como es la seguridad del instituto, procurando establecer con mayor claridad los hechos.

* **Explicativa.-** Se utilizará para el análisis de las causas que provocan el problema, así como las consecuencias generadas por el mismo. Es decir se establecerá las relaciones entre causas y sus consecuencias.

2.4 Universo, población y muestra:

* **Universo.-** Será tomado como el universo al Instituto Tecnológico Superior Aeronáutico (ITSA), porque es el lugar en donde realizara la investigación.

* **Población.-** Será el personal administrativo y directivo.

* **Muestra.-** Se establecerá en base a las necesidades de la investigación de manera particular, se seleccionará al personal que haya trabajado en los aspectos de seguridad de la institución.

2.5 Métodos y técnicas de la investigación.

2.5.1 Métodos.

* **Análisis.-** Mediante este método es posible examinar y estudiar de una manera objetiva y sistemática la falta de seguridad existente en la institución.

* **Síntesis.-** Se tomará en cuenta este método para realizar la recolección de varios elementos que pueden encontrarse dispersos y que aportarán con conocimientos importantes para llegar a obtener conclusiones.

* **Deducción.-** Este método nos permitirá partir del objeto hecho de estudio que es la seguridad actual en la institución, para de esta forma determinar las partes o sitios vulnerables y así sacar conclusiones.

2.5.1 Técnicas.

* **Observación.-** Se realizará la técnica de la observación, ya que por medio de esta se tendrá un contacto con la realidad en cuanto a la seguridad del instituto, lo cual se registrará en fichas de observación.

* **Observación de campo.-** Se utilizará esta técnica, debido a que acudiremos al lugar de los hechos o sitio de investigación en donde se produce el problema.

* **Observación documental.**- Se empleará esta técnica, ya que será importante examinar libros, documentos e internet, que contribuirá con información para el marco teórico.

* **Entrevista.**- Esta técnica será utilizada para recopilar información mediante el diseño de instrumentos de investigación que se aplicarán al personal que esta relacionado directamente con el sistema de seguridad anteriormente implantado.

* **Encuesta.**-Se procederá a utilizar esta técnica de investigación, ya que por medio de la misma se recolectará información basada en preguntas concretas. Y se utilizará la encuesta Auto-Administrada, para no dificultar las actividades laborales del personal mediante un cuestionario realizado por el investigador.

2.6 Recolección de datos.

Para la recolección de información se debe tomar en cuenta los datos primarios y secundarios.

Los datos primarios se los obtendrá en base a la observación que se realizará para poder obtener las falencias de seguridad en una realidad permanente y de esta manera se podrá ordenar la información obtenida de una forma lógica, clara y concisa en el diario vivir de las personas que laboran en la institución, estos datos serán tomados en base a unas fichas de observación las cuales serán realizadas para determinar las zonas de vulnerabilidad o de alto riesgo existente en el ITSA.

Los datos secundarios serán obtenidos por las entrevistas y las encuestas que se las realizarán al personal de seguridad y administrativos del ITSA para poder establecer datos verdaderos y confiables.

Otro de los datos secundarios es la información bibliográfica – documental, donde se tomará en cuenta los proyectos realizados por los estudiantes, los cuales nos pueden dar pautas e ideas para la resolución del nuevo proyecto y así poder mejorar los proyectos anteriormente realizados.

2.7 Procesamiento de la información

En este punto se tomará en cuenta la toda la información que se obtenga de las encuestas y entrevistas, la cual será analizada de acuerdo a su importancia y los datos irrelevantes no se los tomarán en cuenta, todo esto nos ayudara en el planteamiento de conclusiones y recomendaciones.

2.8 Análisis e interpretación de resultados.

Para el análisis e interpretación de datos se los realizará de una manera lógica ordenada en base a las preguntas que se realizarán a las personas a ser entrevistadas.

Las encuestas una vez realizadas se analizarán por pregunta y serán representadas gráficamente, lo que facilitará entender de una manera clara y objetiva los problemas que puedan suscitarse en la institución.

2.9 Conclusiones y recomendaciones.

Las conclusiones y recomendaciones se las obtendrá una vez realizada la investigación. Esto contribuirá con mejoras en el rendimiento del sistema de seguridad, en caso de existir algunas otras opciones para aumentar la eficacia del sistema de seguridad se las propondrá dentro de las posibilidades económicas y técnicas.

CAPÍTULO III

MARCO TEÓRICO

3.1 Antecedentes de la investigación.

El Instituto Tecnológico Superior Aeronáutico cuenta con diversas áreas como: Administrativa, Académica y Recreativas, mismas que se encuentran conformadas por: oficinas, talleres, laboratorios, parqueaderos, espacios deportivos, entre otros.

El área administrativa esta conformada por los departamentos de: sistemas, finanzas, docencia, educación a distancia, logística, rectorado y vicerrectorado.

Para estas instalaciones se han realizado diversos proyectos y trabajos que beneficiaron a la institución en el ámbito de la seguridad. El primer trabajo fue realizado en el año 2002 por los estudiantes: Batallas Lorena, Caillagua Gina y Gaucho Cristian, cuyo tema es: "ESTUDIO E IMPLEMENTACION DE UN CIRCUITO CERRADO DE TELEVISION PARA SEGURIDAD DEL ITSA", con la finalidad de "Estudiar e implementar un circuito cerrado de televisión, para brindar mayor seguridad en el control del alumnado e ingreso de personal"[3]

Un segundo trabajo fue desarrollado en el año 2005 por el estudiante Jarrín Urrutia Celso Aníbal, cuyo tema es "IMPLEMENTACIÓN DE CÁMARAS EN UN CIRCUITO CERRADO JUNTO A LA PREVENCION DOS DEL ITSA", cuyo objetivo fue "Implementar cámaras en un circuito cerrado junto a la prevención dos del Instituto Tecnológico Superior Aeronáutico"[4]

Un tercer fue realizado por el Alno. Cayo Osorio Ronaldo Stalin en abril del año 2005, con el tema "IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA EL LABORATORIO DE INGLES DEL ITSA A TRAVEZ DE 2 CAMARAS DE VIDEO", que tuvo como objetivo: "estudiar e implementar un sistema de control de monitoreo de los exámenes ECL para la escuela de idiomas del ITSA, ubicada en el laboratorio

[3] Trabajo realizado por los estudiantes: Batallas Lorena, Caillagua Gina y Gaucho Cristian
[4] Trabajo desarrollado por el estudiante Jarrín Urrutia Celso Aníbal

de ingles en el primer piso”[5].

3.2 Fundamentación teórica.

3.2.1 Seguridad

“La seguridad es una condición necesaria para el funcionamiento de la sociedad y uno de los principales criterios para asegurar la calidad de vida”[6]

El término seguridad proviene de la palabra “seguritas” del latín. Usualmente se representa a la seguridad como el alejamiento de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

En la rama de la Administración Pública cuyo fin es velar por la seguridad de los ciudadanos, se define a la seguridad, como el conjunto de leyes y organismos que tiene como fin proteger contra determinados riesgos sociales: accidentes, enfermedad, paros, vejez, etc.

El concepto de seguridad es, muy amplio y abarca la seguridad social, la ciudadana, la seguridad respecto a los objetos que se poseen, aquella que tiene vinculación con la responsabilidad civil por daños causados a terceros, etc.

En los tiempos complejos y conflictivos de la actualidad, para conseguir la tranquilidad que otorga la seguridad, las leyes han previsto en múltiples disposiciones como obtener esa seguridad total o parcial.

Los expertos afirman que la inversión en materia de seguridad siempre va a ser menor a las pérdidas que podrían sufrir una empresa o cualquier institución que posee bienes materiales.

[5] Trabajo de graduación realizado por el Alno. Cayo Osorio Ronaldo Stalin
[6]“www.guerrero.gob.mx/?P=readart&ArtOrder=ReadArt&Article=301#S”

A continuación se menciona algunos tipos de seguridad:

* Seguridad empresarial.
* Seguridad industrial.
* Seguridad laboral.
* Seguridad pública y protección civil.
* Seguridad privada.
* Seguridad personal.
* Seguridad informática.
* Seguridad física.

3.2.2 Seguridad empresarial.

"La seguridad empresarial puede ser entendida como el conjunto de medidas y estrategias que dispone una empresa ya sea comercial, industrial, etc. para proteger sus recursos materiales, técnicos, humanos y financieros, o sea, su patrimonio, su personal, su dinero así como su mobiliario y equipo (incluyendo software, información y bases de datos)."[7]

Con miras a la seguridad, se deben considerar, entre otras cosas, los siguientes aspectos:

* La ubicación, es decir, que el predio se encuentre en un sitio que ofrezca las condiciones esenciales de seguridad, que el tránsito de vehículos no sea peligroso, que existan todos los servicios municipales, etc.).

* Las dimensiones de oficinas, pasillos, patios y áreas de estacionamiento deben cumplir con los reglamentos o normas correspondientes, a efecto de que provean de aire suficiente, temperatura adecuada e iluminación, además de que los pasillos deben proporcionar la viabilidad necesaria para casos de evacuación emergente.

[7] "www.latinoseguridad.com/LatinoSeguridad/SPX/SPX30.shtml"

* La ventilación, alumbrado general, alumbrado de emergencia, materiales de la edificación, los acabados, pisos, barandales, ascensores, los almacenes de sustancias tóxicas, inflamables, explosivas o cáusticas, y las señalizaciones.

* También es necesario proteger los sistemas informáticos y las bases de datos e información contenida en equipo de cómputo a través de sistemas de protección y mantenimiento en red, tales como anti hackers, anti virus, etc. y sistemas anti incendio.

Un punto adicional en el ámbito de la seguridad empresarial es la protección o seguridad a ejecutivos y funcionarios de las empresas, misma que se puede ejercer a través de un elemento que sea un asistente a la vez que un chofer y un guardaespaldas.

3.2.3 Seguridad industrial.

"La seguridad industrial es conceptualizada como el conjunto de principios leyes, normas y mecanismo de prevención de los riesgos inherentes al recinto laboral, que pueden ocasionar un accidente ocupacional, con daños destructivos a la vida de los trabajadores, a las instalaciones o equipos de las empresas en todos sus ramos."[8]

La seguridad industrial puede ser definida como "una obligación que la ley impone a patrones y a trabajadores y para que se organice y funcione dentro de determinados procedimientos".

La seguridad industrial se preocupa de que existan las condiciones adecuadas para que el trabajo se realice con eficiencia y rapidez.

Es por esto que los psicólogos industriales han realizado programas de investigación exhaustiva sobre todos los aspectos del ambiente físico del trabajo, tales como la temperatura, humedad, iluminación, ruido, y jornada laboral, para

[8] "http://www.latinoseguridad.com/LatinoSeguridad/SPX/SPX30.shtml"

establecer las pautas más óptimas de cada uno de esos factores. Con estos programas se evita que exista un ambiente incomodo, el cual ocasione efectos negativos, disminución de la productividad, aumento de errores, mayor índice de accidentes y más rotación de personal.

Cuando se mejora el ambiente laboral haciéndolo más cómodo y agradable la producción se eleva, la compañía obtiene sus metas y el personal está más contento y satisfecho.

3.2.4 Seguridad laboral.

El concepto de seguridad laboral está muy cercano y ligado al de seguridad industrial, toda vez que se trata de la seguridad ocupacional, o sea, una seguridad para los trabajadores.

La seguridad laboral se originó con la aprobación de las leyes laborales y sus posteriores reformas, y “es un sector de la seguridad y la salud pública que se ocupa de proteger la salud de los trabajadores, controlando el entorno del trabajo para reducir o eliminar riesgos.

En este sentido, se podría considerar a la seguridad laboral como la obligación patronal de garantizar la integridad física, mental y material del trabajador, independientemente del tipo de las actividades o funciones que se le hayan encomendado y de que cuente con seguridad social y otras prestaciones que incluyen a las de tipo médico.

3.2.5 Seguridad pública y protección civil.

La seguridad pública equivale a la idea de seguridad integral del público civil, y es uno de los elementos fundamentales y prioritarios del desarrollo de toda sociedad y consecuentemente del Estado, cuya función primaria es la promoción del bien común y de la integridad de todos y de cada uno de sus habitantes.

Los servicios de seguridad pública constituyen un ámbito de esfuerzos comunitarios que están destinados a proteger y preservar el orden y la tranquilidad públicos con el propósito de establecer un contexto de condiciones de entorno que propicien, procuren y promuevan la continuidad y desarrollo armónicos, proactivo y productivos de la dinámica social, así como la consecución de las metas y objetivos comunitarios.

Para estos efectos se tiene que las vertientes funcionales de estos esfuerzos, comprenden, fundamentalmente los siguientes aspectos:

* La protección y preservación de la existencia e integridad de las personas y sus propiedades.
* La vigilancia y preservación del orden público.
* La disuasión, prevención y combate a la delincuencia.
* La contención y anulación de los factores de perturbación del orden social.
* La custodia, rehabilitación y reinserción de los elementos antisociales.

De tal suerte que, las formas de operación que se pueden adoptar para su desempeño, comprenden algunas de las siguientes:

* Servicios médicos de urgencia, bomberos y protección civil.
* Policía.
* Control de tráfico.
* Operación de centros de reclusión y readaptación social.

Protección civil es: “El conjunto de acciones, principios, normas, políticas y procedimientos preventivos o de auxilio, recuperación y de apoyo, tendientes a proteger la vida, la salud y el patrimonio de las personas, la planta productiva, la prestación de servicios públicos y el medio ambiente; realizadas ante los riesgos, emergencias o desastres; que sean producidos por causas de origen natural, artificial o humano, llevados a cabo por las autoridades, organismos, dependencias e instituciones de carácter público, social o privado, grupos voluntarios y en general,

por todas las personas que por cualquier motivo residan, habiten, o transiten en un determinado lugar geográfico.

Seguridad pública y protección civil, teóricamente, podrían parecer conceptos equivalentes o sinónimos; sin embargo, no es así. Normalmente, la noción de seguridad pública se emplea para referir la actividad de la policía y otros organismos especializados en la prevención e investigación del delito. En cambio, protección civil es un término que se emplea para referir la prevención de desastres, ya sean naturales o provocados por el hombre, o el apoyo a la sociedad cuando se presenta uno de ellos"

3.2.6 Seguridad privada.

La calidad de vida tiene que ver con las condiciones adecuadas para que el ser humano pueda realizar todas sus actividades. Esas condiciones implican cuestiones como bienestar material, salud física y psicológica, acceso a la cultura, un medio ambiente sano, justicia social, y también seguridad.

El sector de la seguridad privada está compuesto por dispositivos individuales y organizacionales que brindan servicios de seguridad, vigilancia, protección, investigaciones y otros múltiples conexos a particulares, empresas, instituciones, reparticiones gubernamentales y otros demandantes.

Como la oferta pública no puede dar respuesta completa a la demanda de seguridad ciudadana, en muchos ámbitos las necesidades son cubiertas por la seguridad privada.
Esta demanda social de seguridad persistirá y se profundizará, debido a:

* El incremento de los delitos comunes o tradicionales y el surgimiento de nuevas modalidades de delitos que han superado la capacidad técnica y operativa de las fuerzas policiales tradicionales u oficiales.
* La demanda de seguridad de la ciudadanía es más alta que la expectativa de seguridad que tienen las autoridades gubernamentales.

* La operación y puesta en marcha de un trabajo preventivo, es decir, de prevención del delito, no es algo que las policías oficiales hayan hecho tradicionalmente. Por tanto, su capacidad efectiva es mucho menor en comparación con la de la delincuencia.
* La cobertura real de las policías oficiales es insuficiente ante el crecimiento poblacional urbano industrial y comercial.
* La ciudadanía misma, en consecuencia, y sobre todo los más emprendedores, han tenido que empezar a instrumentar organismos que operen de manera privada para brindar seguridad a la población e incluso a las dependencias gubernamentales, en distintos niveles, sitios y áreas de especialización.
* Es decir, se han creado empresas de seguridad particulares, que se le conoce como seguridad privada.

Por lo anteriormente expuesto podemos definir “seguridad privada” a los servicios integrales de seguridad y protección que ofrecen empresas formadas con capital esencialmente privado y sujetas al régimen legal, fiscal y financiero respectivo, a personas tanto públicas como privadas en áreas diversas y específicas tales como vigilancia, traslado de valores, protección física a individuos, resguardo de bienes muebles e inmuebles, prevención y combate de incendios y contingencias naturales e intencionales, etc.

3.2.7 Seguridad personal.

La época que nos esta tocando vivir empieza a presentar síntomas de una descomposición social que se traduce en una mayor incidencia de hechos delictuosos.

Desgraciadamente los mismos instrumentos masivos de comunicación: prensa, radio, y sobre todo la televisión, son medios para enseñar métodos y sistemas para delinquir.

Bombardeamos las 24 hrs. del día al niño y al adulto con violencia; y si a esto sumamos las carencias propias de una etapa inflacionaria y la falta cada vez mas dramática de valores, nos puede explicar lo que hoy nos pasa: robos, asaltos, secuestros, asesinatos, sabotaje que son consecuencia y no síntoma, de una enfermedad cada día mas grave de nuestra sociedad.

La seguridad personal ha pasado a ser una preocupación de la población en general, y las organizaciones que también emplean personas no pueden ignorar esa ansiedad de sus integrantes, en especial la de aquellos que corren mayores riesgos por su tipo de labor, rutinas, etcétera.

Desde hace mucho tiempo las organizaciones han entendido que la prevención en salud, la seguridad e higiene laboral (accidentes laborales o enfermedades profesionales), la protección de edificios organizacionales son una inversión necesaria para mantener en adecuadas forma a sus colaboradores.

En general se puede decir que el hecho de haber evitado un incidente justifica todo el esfuerzo organizacional en materia de prevención y preparación para actuar ante la delincuencia.

Por ello al igual que en el campo de la salud la prevención es la más económica de las respuestas. Se calcula que de cada dólar invertido en prevención se están ahorrando como mínimo 3 en reparación.

Si bien desde el punto de vista exclusivamente de costos estos riesgos pueden cubrirse con seguros, también debemos pensar en las personas como tales, dado que las organizaciones también tienen que preservar el enfoque humanístico. Además la preservación de la persona también es un buen negocio, para la empresa y para la sociedad si tiene buena calidad de vida, que no solamente consiste en lo estrictamente material.

3.2.8 Seguridad informática.

"Como hemos mencionado anteriormente, seguridad es un sistema (informático o no) libre de peligro o daño. "[9]

Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos del tema el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro.

Para que un sistema se pueda definir como seguro debemos dotarlo de cuatro características:

* Integridad: La información no puede ser modificada por quien no está autorizado
* Confidencialidad: La información solo debe ser accesible para los autorizados
* Disponibilidad: Debe estar disponible cuando se necesita
* Irrefutabilidad: Que no se pueda negar los derechos de autor.

La Seguridad Informática es un tema de dominio obligado por los usuarios de la Internet y de los sistemas informáticos, para no permitir que su información sea robada y usada sin autorización. De esta forma también se la puede definir como una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios.

3.2.9 Seguridad física.

"La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante

[9] "http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica"

amenazas a los recursos e información confidencial. Son los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, edificio o instalaciones. “[10]

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro. [11]

La seguridad física garantiza la integridad de bienes inmuebles tales como: viviendas, edificios, o institutos en caso de cualquier eventualidad, como, por ejemplo, un incendio, corto circuito, fallas en la energía eléctrica, robos o que ningún usuario entre a la empresa sin un carnet que los identifique.

La seguridad física hace referencia, a las barreras físicas y mecanismos de control en el entorno de un sistema de vigilancia, para proteger las instalaciones de amenazas físicas producidas por el hombre o la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo estos bienes pueden ser: Desastres naturales, incendios accidentales, humedad e inundaciones.; amenazas ocasionadas involuntariamente por personas; acciones hostiles deliberadas como robo, fraude o sabotaje.

Son ejemplos de mecanismos o acciones de seguridad física: Cerrar con llave las instalaciones que se quiere controlar; tener extintores por eventuales incendios; instalación de cámaras de seguridad; Guardia humana; control permanente del sistema eléctrico, de ventilación, etc.

3.2.10 Seguridad contra desastres.

Los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes

[10] www.segu-info.com.ar/fisica/seguridadfisica.htm
[11] www.segu-info.com.ar

tipos de riesgos son: Incendios, Inundaciones, Condiciones Climatológicas, Señales de Radar, Instalaciones Eléctricas, Ergometría.

3.2.10.1 Incendios.

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

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

* El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
* El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
* Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
* Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
* No debe estar permitido fumar en el área de proceso.
* Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

* El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

3.2.10.2 Seguridad del equipamiento.

Es necesario proteger los equipos instalados en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

* La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
* Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
* Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

3.2.10.3 Recomendaciones.

* El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
* Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.
* Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.
* Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de

materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

* Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.
* Suministrar información, de la institución, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento esté consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

3.2.10.4 Inundaciones.

Se las define de esta manera a la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

3.2.10.5 Condiciones climatológicas

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, huracanes y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada.

La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa,

permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia.

3.2.10.5.1 Terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

3.2.10.6 Señales de radar.

Los resultados de las investigaciones más recientes indican que las señales muy fuertes de radar pueden inferir en el procesamiento electrónico de la información, pero únicamente si la señal que alcanza el equipo es de 5 Volts/Metro, o mayor.

Ello podría ocurrir sólo si la antena respectiva fuera visible desde una ventana del centro de procesamiento respectivo y, en algún momento, estuviera apuntando directamente hacia dicha ventana.

3.2.10.7 Instalaciones eléctricas

Esta es una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

3.2.10.7.1 Picos y ruidos electromagnéticos.

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en la transferencia de datos.

3.2.10.7.2 Cableado.

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal (UTP) al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

* Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
* Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
* Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

3.2.10.7.3 Cableado de alto nivel de seguridad.

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

3.2.10.7.4 Pisos de placas extraíbles.

"Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo."[12]

3.2.10.7.5 Sistema de aire acondicionado.

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al lugar de trabajo del personal y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

3.2.10.7.6 Emisiones electromagnéticas

Desde hace tiempo se sospecha que las emisiones, de muy baja frecuencia que generan algunos periféricos, son dañinas para el ser humano.

[12]" www.segu-info.com.ar/fisica/ergometria.htm"

Según recomendaciones científicas estas emisiones podrían reducirse mediante filtros adecuados al rango de las radiofrecuencias, siendo estas totalmente seguras para las personas. Para conseguir que las radiaciones sean mínimas hay que revisar los equipos constantemente y controlar su envejecimiento.

3.2.10.8 Ergometría

"La Ergonomía es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible." [13]

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro.

3.2.10.8.1 Trastornos óseos y/o musculares.

Una de las maneras de provocar una lesión ósea o muscular es obligar al cuerpo a ejecutar movimientos repetitivos y rutinarios, y esta posibilidad se agrava enormemente si dichos movimientos se realizan en una posición incorrecta o antinatural.

En resumen, el lugar de trabajo debe estar diseñado de manera que permita que el usuario se coloque en la posición más natural posible. Como esta posición variará de acuerdo a los distintos usuarios, lo fundamental en todo esto es que el puesto de trabajo sea ajustable, para que pueda adaptarse a las medidas y posiciones naturales propias de cada desempeño laboral.

[13] "www.segu-info.com.ar/fisica/ergometria.htm"

3.2.10.8.2 Trastornos visuales.

Los ojos, sin duda, son las partes más afectadas por el trabajo, por ejemplo en computación.

La pantalla es una fuente de luz que incide directamente sobre el ojo del operador, provocando, luego de exposiciones prolongadas el típico cansancio visual, irritación y lagrimeo, cefalea y visión borrosa.

Si a esto le sumamos un monitor cuya definición no sea la adecuada, se debe considerar la exigencia a la que se someterán los ojos del usuario al intentar descifrar el contenido de la pantalla. Además de la fatiga del resto del cuerpo al tener que cambiar la posición de la cabeza y el cuello para acercar los ojos a la misma.

Para prevenir los trastornos visuales en el personal podemos tomar las siguientes precauciones como:

* Tener especial cuidado al elegir los monitores y placas de vídeo de las computadoras.
* Usar de pantallas antirreflejo o anteojos con protección para el monitor, es una medida preventiva importante y de relativo bajo costo, que puede solucionar varios de los problemas antes mencionados.

3.2.10.8.3 La salud mental.

La carga física del trabajo adopta modalidades diferentes en los puestos informatizados. De hecho, disminuye los desplazamientos de los trabajadores y las tareas requieren un menor esfuerzo muscular dinámico, pero aumenta, al mismo tiempo, la carga estática de acuerdo con las posturas inadecuadas asumidas.

Por su parte, la estandarización y racionalización que tiende a acompañar la aplicación de las PCs en las tareas de ingreso de datos, puede llevar a la transformación del trabajo en una rutina inflexible que inhibe la iniciativa personal,

promueve sensaciones de hastío y monotonía y conduce a una pérdida de significado del trabajo.

Además, el estrés causado por la rutina está convirtiéndose en una nueva enfermedad profesional relacionada con el trabajo, provocada por la carga mental y psíquica inherente a la operación con los nuevos equipos.

Los efectos del estrés pueden encuadrarse dentro de varias categorías:

* Los efectos fisiológicos inmediatos, caracterizados por el incremento de la presión arterial, el aumento de la frecuencia cardiaca, etc.
* Los efectos psicológicos inmediatos hacen referencia a la tensión, irritabilidad, cólera, agresividad, etc. Estos sentimientos pueden, a su vez, inducir ciertos efectos en el comportamiento tales como el consumo de alcohol y psicofármacos, el hábito de fumar, etc.
* También existen consecuencias médicas a largo plazo, tales como enfermedades coronarias, hipertensión arterial, úlceras pépticas, agotamiento; mientras que las consecuencias psicológicas a largo plazo pueden señalar neurosis, insomnio, estados crónicos de ansiedad y/o depresión, etc.

La apatía, sensaciones generales de insatisfacción ante la vida, la pérdida de la propia estima, etc., alteran profundamente la vida personal, familiar y social del trabajador llevándolo, eventualmente, al aislamiento, al ausentismo laboral y la pérdida de la solidaridad social.

3.2.10.8.4 Ambiente luminoso.

Se parte de la base que las oficinas mal iluminadas son la principal causa de la pérdida de la productividad en las empresas y de un gasto energético excesivo. Una iluminación deficiente provoca dolores de cabeza y perjudica a los ojos.

3.2.10.8.5 Ambiente climático

En cuanto al ambiente climático, la temperatura de una oficina debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. En todos los lugares hay que contar con sistemas que renueven el aire periódicamente. No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

3.2.11 Seguridad contra acciones hostiles

3.2.11.1 Robo.

"Muchos bienes de valor, tales como las computadoras, proyectores, libros, piezas de stock, etc. e incluso el dinero de las empresas están expuestos."[14]

Inclusive se debería controlar que los operadores no utilicen las computadoras de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina, también en el control de personas ajenas a las áreas de trabajo ya que puede sustraerse bienes pertenecientes a los trabajadores o de la empresa que se encuentren sin vigilancia.

La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

El software, es una propiedad muy fácilmente sustraible y los discos son fácilmente copiados sin dejar ningún rastro.

[14] "http://es.wikipedia.org/wiki/Atraco"

3.2.11.2 Fraude.

"Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines. Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones."[15]

3.2.11.3 Sabotaje

"El peligro más temido en los centros de procesamiento de datos y en los demás departamentos técnicos, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa."[16]

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque los discos estén almacenados en el interior de su funda de protección. Una habitación llena de discos puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos.

Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

3.2.12 Control de accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

[15] "http://es.wikipedia.org/wiki/Fraude_de_ley"
[16] "http://es.wikipedia.org/wiki/Sabotaje"

3.2.12.1 Utilización de guardias

3.2.12.1.1 Control de personas.

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al interior de las dependencias de cualquier empresa ya sea pública o privada. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identification Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc., permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

* Normal o definitiva: para el personal permanente de planta.
* Temporaria: para personal recién ingresado.
* Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
* Visitas.

3.2.12.1.2 Control de vehículos.

Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

3.2.12.1.3 Desventajas de la utilización de guardias.

Es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o egresar de la planta con materiales no autorizados. Esta situación de soborno es muy frecuente, por lo que es recomendable la utilización de sistemas biométricos para el control de accesos.

3.2.12.2 Utilización de detectores de metales.

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

3.2.12.3 Utilización de sistemas biométricos

Definimos a la Biometría como "la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos", además es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

3.2.12.3.1 Los Beneficios de una tecnología biométrica.

Pueden eliminar la necesidad de poseer una tarjeta para acceder. Aunque las reducciones de precios han disminuido el costo inicial de las tarjetas en los últimos años, el verdadero beneficio de eliminarlas consiste en la reducción del trabajo concerniente a su administración.

Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricas de una persona son intransferibles a otra.

3.2.12.3.2 Emisión de calor.

Se mide la emisión de calor del cuerpo (termograma), realizando un mapa de valores sobre la forma de cada persona.

3.2.12.3.3 Huella digital.

Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados.

Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

3.2.12.3.4 Verificación de voz.

La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.).

Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

3.2.12.3.5 Verificación de patrones oculares.

Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse en las mismas enfermedades que en ocasiones se prefiere mantener en secreto.

3.2.12.3.6 Verificación automática de firmas (VAF)

En este caso lo que se considera es lo que el usuario es capaz de hacer, aunque también podría encuadrarse dentro de las verificaciones biométricas.

Mientras es posible para un falsificador producir una buena copia visual o facsímil, es extremadamente difícil reproducir las dinámicas de una persona: por ejemplo la firma genuina con exactitud.

La VAF, usando emisiones acústicas toma datos del proceso dinámico de firmar o de escribir.

La secuencia sonora de emisión acústica generada por el proceso de escribir constituye un patrón que es único en cada individuo. El patrón contiene información extensa sobre la manera en que la escritura es ejecutada.

El equipamiento de colección de firmas es inherentemente de bajo costo y robusto.

3.2.12.4 Seguridad con animales.

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el

costo de cuidado y mantenimiento se disminuyen considerablemente utilizando este tipo de sistema.

Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

3.2.12.5 Protección electrónica.

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación.

3.2.12.6 Barreras infrarrojas y de micro-ondas.

Transmiten y reciben haces de luces infrarrojas y de micro-ondas respectivamente. Se codifican por medio de pulsos con el fin de evadir los intentos de sabotaje. Estas barreras están compuestas por un transmisor y un receptor de igual tamaño y apariencia externa.

Cuando el haz es interrumpido, se activa el sistema de alarma, y luego vuelve al estado de alerta. Estas barreras son inmunes a fenómenos aleatorios como calefacción, luz ambiental, vibraciones, movimientos de masas de aire, etc.

Las micro-ondas son ondas de radio de frecuencia muy elevada. Esto permite que el sensor opere con señales de muy bajo nivel sin ser afectado por otras emisiones de radio, ya que están muy alejadas en frecuencia.

Debido a que estos detectores no utilizan aire como medio de propagación, poseen la ventaja de no ser afectados por turbulencias de aire o sonidos muy fuertes.

Otra ventaja importante es la capacidad de atravesar ciertos materiales como son el vidrio, lana de vidrio, plástico, tabiques de madera, revoques sobre madera, mampostería y hormigón.

3.2.12.7 Detector ultrasónico.

Este equipo utiliza ultrasonidos para crear un campo de ondas. De esta manera, cualquier movimiento que realice un cuerpo dentro del espacio protegido, generará una perturbación en dicho campo que accionará la alarma. Este sistema posee un circuito refinado que elimina las falsas alarmas.

3.2.12.8 Detectores con alimentación.

Estos elementos requieren alimentación de 12 Vcd, van conectados a la central de control de alarmas para mandar la información de aviso.

Los siguientes están incluidos dentro de este tipo de detectores:

* Detector de aberturas: contactos magnéticos externos o de embutir.
* Detector de roturas de vidrios: inmune a falsas alarmas provocada por sonidos de baja frecuencia; sensibilidad regulable.
* Detector de vibraciones: detecta golpes o manipulaciones extrañas sobre la superficie controlada.
* Detector de movimiento: censa el calor corporal que emiten las personas por medio de un lente.
* Detector de humo: la presencia de humo en el aire y emite una señal acústica avisando del peligro de incendio.

3.2.12.8.1 Detector de aberturas.

Es un dispositivo que forma parte de una alarma electrónica su utilización es para detectar la apertura de puertas o ventanas.

Contacto Magnético SM-205:

Tiene un tamaño 32 x 7 x 13,5 mm. Autoadhesivo con tornillos para montar sobre superficie plana con dos opciones de instalación: autoadhesivo incluido o tornillos, la solapa está marcada para poder cortarla si es necesario su precableado de 38 cm. extendido desde el lateral del contacto vienen en color marrón y blanco. Abertura: 25 mm.

3.2.12.8.2 Detector de movimiento.

Los detectores de movimiento son fuentes de luz de seguridad que se caracterizan por su conveniencia y eficiencia. La instalación es sencilla. Para la mayoría de los propietarios de casas, instalar una luz activada por el movimiento debe ser un trabajo de no más de un par.

3.2.12.8.3 Detector de humo.

Un detector de humo es un aparato de seguridad que detecta la presencia de humo en el aire y emite una señal acústica avisando del peligro de incendio. Atendiendo al método de detección que usan pueden ser de dos tipos: ópticos o iónicos, aunque algunos usen los dos mecanismos para aumentar su eficacia.

3.2.12.9 Consola de activación/desactivación ó teclado.

Esta consola habitualmente contiene un teclado que permite programar todas las funciones del sistema. Esta interfase de control cuenta con teclas alfanuméricas, como así también otras funciones de señalización de estados, por lo que constituye una pieza importante para el usuario del sistema. Existen señalizadores de dos tipos, los de led o luces, y también los de pantalla de cuarzo líquido. En ambos casos brindan información de cada una de las zonas que están conectadas (áreas de protección exterior, puertas, ventanas, áreas interiores, etcétera). En algunos modelos, la consola de activación/desactivación se encuentra montada en el frente de la central de alarma, aunque esto tiende a caer en desuso. También existen modelos en que se dispone un control remoto por ondas de radio codificadas, que

permite la activación/desactivación de la central, y eventualmente puede accionar las sirenas y hacer llamados telefónicos en caso de asaltos.[17]

3.2.12.10 Sirena.

"Instrumento o aparato que produce un sonido potente y agudo que se oye a gran distancia, como los empleados en vehículos, barcos, fábricas, Etcétera, como señal de alarma o para avisar. "[18]

3.2.12.11 Batería y cargador.

"Estos elementos sirven para proveer un sistema de alimentación eléctrica ininterrumpida (UPS), de manera que ante una falta del suministro eléctrico de red (normal o provocado por un ladrón), el sistema de alarma contra intrusos continúe brindando protección en forma absolutamente normal. "[19]

Sus características técnicas son las siguientes:

* Selladas de plomo-ácido de batería
* Tensión nominal: 12V
* Peso: aprox. 2.58kg (5,68 lbs.)
* Utilizable en cualquier posición
* Larga vida útil

3.2.12.12 Cable UTP o par trenzado.

"Es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común, consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de 1 mm aproximado. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se

[17] "www.arqhys.com/casas/central-alarma.html"
[18] "http://www.elpais.com/diccionarios/castellano/sirena"
[19] "www.arqhys.com/casas/central-alarma.html"

agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multíparas de pares trenzados (de 2, 4, 8,…hasta 300 pares).”[20]

Un ejemplo de par trenzado es el sistema de telefonía, ya que la mayoría de aparatos se conectan a la central telefónica por intermedio de un par trenzado. Actualmente se han convertido en un estándar, de hecho en el ámbito de las redes LAN, como medio de transmisión en las redes de acceso a usuarios (típicamente cables de 2 ó 4 pares trenzados). A pesar que las propiedades de transmisión de cables de par trenzado son inferiores y en especial la sensibilidad ante perturbaciones extremas a las del cable coaxial, su gran adopción se debe al costo, su flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

3.2.12.13 Centrales de alarma.

“La central de alarma suele encontrarse resguardada en un gabinete lo suficientemente protegido como para no poder ser desarmado, el cual, por lo general, suele incluir la batería y su correspondiente cargador.

Estas centrales pueden clasificarse de acuerdo al número de zonas independientes que protegen, por lo tanto podemos encontrar centrales de 2 zonas, 4 zonas, 10 zonas, etc. Cada una de estas zonas puede ser activada y desactivada de forma independiente, lo cual es una gran prestación para hogares con muchas dependencias, ya que es posible proteger las áreas en las que no debería haber presencia humana y desactivar los detectores en aquellas áreas que estén siendo ocupadas por los habitantes de la vivienda.

Existen algunos tipos de centrales como:

* Maxys.
* Power Series.
* Ademco.

[20] “http://html.rincondelvago.com/cable-par-trenzado.html”

* Napco.

En el caso de las alarmas para empresas u oficinas, se han producido grandes avances y es posible contar con sistemas que registran cada activación o desactivación del sistema en un portal de Internet, al cual se puede acceder con un nombre de usuario, contraseña y consultar cada vez que se lo desee.

Dando un paso más allá, y aprovechando el uso que se da hoy en día a los dispositivos móviles, algunas empresas brindan un servicio que, además de posibilitar la consulta de activaciones o desactivaciones."[21]

3.2.12.14 Sonorización y dispositivos luminosos.

Dentro de los elementos de sonorización se encuentran las sirenas, campanas, timbres, etc. Algunos dispositivos luminosos son los faros rotativos, las balizas, las luces intermitentes, etc.

Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente si el estado de alarma es de robo, intrusión, asalto o aviso de incendio.

Se pueden usar transmisores de radio a corto alcance para las instalaciones de alarmas locales. Los sensores se conectan a un transmisor que envía la señal de radio a un receptor conectado a la central de control de alarmas encargada de procesar la información recibida.

3.2.12.15 Circuitos cerrados de televisión.

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para

[21] "www.arqhys.com/casas/central-alarma.html"

ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Todos los elementos anteriormente descriptos poseen un control contra sabotaje, de manera que si en algún momento se corta la alimentación o se produce la rotura de alguno de sus componentes, se enviará una señal a la central de alarma para que ésta accione los elementos de señalización correspondientes.

3.2.12.16 Edificios inteligentes.

La infraestructura inmobiliaria no podía quedarse rezagada en lo que se refiere a avances tecnológicos.

El Edificio Inteligente (surgido hace unos 10 años) se define como una estructura que facilita a usuarios y administradores, herramientas y servicios integrados a la administración y comunicación. Este concepto propone la integración de todos los sistemas existentes dentro del edificio, tales como teléfonos, comunicaciones por computadora, seguridad, control de todos los subsistemas del edificio (gas, calefacción, ventilación y aire acondicionado, etc.) y todas las formas de administración de energía.

Una característica común de los Edificios Inteligentes es la flexibilidad que deben tener para asumir modificaciones de manera conveniente y económica.

3.2.12.16.1 Conclusiones

* Evaluar y controlar permanentemente la seguridad física del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.
* Tener controlado el ambiente y acceso físico permite:
* Disminuir siniestros.
* Trabajar mejor manteniendo la sensación de seguridad
* Descartar falsas hipótesis si se produjeran incidentes
* Tener los medios para luchar contra accidentes

* Las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados.
* Estas decisiones pueden variar desde el conocimiento de las áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

3.3 Fundamentación legal.

Según el Manual de Autoevaluación con Fines de Acreditación para los institutos Superiores Técnicos y Tecnológicos del Ecuador emitido por el Consejo Nacional de Evaluación y Acreditación de la educación Superior del Ecuador (CONEA), en el ámbito 4: Bienestar institucional, característica 9: estándar 9.3, en el indicador 9.3.1, indica "Verificación de la existencia de políticas de seguridad institucional. CO.EF.1.4.02 (P)"; y el estándar 9.4, en el indicador 9.4.1 indica "Verificación de que el instituto cuenta con personal especializado y equipos apropiados para su seguridad. RA.TH.1.4.01 (P)"[22]

De acuerdo al Reglamento General de Institutos Superiores Técnicos y Tecnológicos del Ecuador, Capitulo V (De las Estrategias), Art. 9; numeral 5 en donde indica que toda institución educativa debe "Prepara proyectos que permitan prevenir desastres y resolver problemas que afecten a la colectividad."[23]

De acuerdo a las normas que están dirigidas para la seguridad interna tanto de bienes como personas, para ello el Instituto Tecnológico Superior Aeronáutico, mediante el consejo directivo han decretado y aprobado los artículos desde el Art.1 hasta el Art.22, ver (Anexo A).

En estos artículos no mencionan en absoluto sobre algún sistema de seguridad específico que se deba crear o implementar para brindar mayor seguridad a la institución.

[22] Manual de Autoevaluación con Fines de Acreditación para los Institutos Superiores Técnicos y Tecnológicos del Ecuador.
[23] http://www.conesup.net/descargas/reglamento_institutos.pdf

CAPÍTULO IV
EJECUCIÓN DEL PLAN METODOLÓGICO

4.1 Modalidad básica de la investigación:

* **Investigación de campo.-** El presente trabajo de investigación, para ser ejecutado se ha dividido en tres áreas: administrativa, académica y recreativo, con los que cuenta el Instituto Tecnológico Superior Aeronáutico.

  El área administrativa, comprende las oficinas de: rectorado, vicerrectorado, departamentos de logística, finanzas, secretaria, sistemas, docencia, educación a distancia y recursos humanos.

  El área académica, esta conformada por laboratorios, talleres, biblioteca, aulas taller, coordinación y control, marketing, secretaria académica y aulas.

  El área recreativa, a la que pertenecen: gimnasio, canchas deportivas, patio rojo auditorio, prevenciones.

  La investigación de campo nos permitió obtener la información del sistema de seguridad, mediante un proceso el apoyo de las técnicas de la observación directa, entrevista y encuesta, verificando que existe seguridad física y electrónica.

  La seguridad física que dispone el instituto, se refieren a la confianza humana que realiza el personal militar, que corresponde al servicio de guardia; además se constató que no cuenta con un plan alterno para prevenir desastres.

  Los controles de acceso, aún funcionan bajo el sistema convencional manual (cerraduras, candados y cadenas) pertenecen a una formula caduca de custodiar los bienes.

  La seguridad electrónica (circuito cerrado de televisión), se encuentra en desuso, posiblemente por la falta de mantenimiento y de precaución.

Mediante la observación directa y el diálogo con integrantes del departamento administrativo, hemos podido recopilar información de primera mano la que nos ha conllevado a tener una apreciación mucho mas clara de la problemática sobre seguridad en el Instituto.

Se constató que el ITSA cuenta con poca seguridad física y no cuenta con seguridad anti desastres lo que se pudo constatar al emitir un oficio solicitando estos documentos y obteniendo como respuesta una negativa de la existencia de estos (Anexo B y C)

* **Bibliográfica y documental.-** A través de esta modalidad se obtuvo información en los trabajos realizados por estudiantes anteriores; cabe recalcar que es muy escasa la información bibliográfica relacionada con este tema, aún así hemos podido tener argumentos que han orientado nuestro trabajo.

  Para el desarrollo del marco teórico, recurrimos a la abundante información que posee el Internet, trabajo que nos condujo a realizar una selección de los mejores aspectos a necesitar.

4.2 Tipos de investigación:

* **Investigación no experimental.-** A través de la observación se ha podido describir la existencia de los elementos en cuestión, por lo tanto no se ha profundizado en ningún tipo de experimentación. Dicho de otra forma, el problema nos presenta elementos de verificación sin que esto nos indique una relación de causa y efecto, puesto que el primer proyecto de graduación realizado por la estudiante Batallas Lorena, Caillagua Gina y Gaucho Cristian, cuyo tema es: “ESTUDIO E IMPLEMENTACION DE UN CIRCUITO CERRADO DE TELEVISION PARA SEGURIDAD DEL ITSA” nos sirvió como una pauta para los demás.

* **Investigación cuasi experimental.-** Se aplica esta forma de investigación en el momento en que el grupo de investigadores tiene relación directa con: Subp. Padilla Milton, Subp. Segovia Mario, Sgos. Oyaque Rubén, Sgos. Tulchán Stalin, Sgos. Coello Freddy, de quienes se recaba la información necesaria puesto que el personal mencionado, al momento de realizar el trabajo, cumplían las funciones de: coordinación logística académica, estos profesionales nos entregaron argumentos reales sobre el estado en que se encontraban los sistemas utilizados hasta el momento, conociendo de esta manera que estos medios se encuentran en un estado inactivo.

4.3 Niveles de investigación:

* **Investigación exploratoria.-** Se determinó que existe una seguridad física que no satisface las necesidades actuales, se pudo constatar que la seguridad electrónica que posee esta deshabilitada debido a la falta de mantenimiento y cuidado de los equipos.

  Ya que el espacio físico del instituto es grande por lo que se lo dividió en tres áreas que son: la administrativa (rectorado, vicerrectorado, secretaria académica, departamentos: logístico, docencia, educación a distancia, sistemas, finanzas, recursos humanos), académica (aulas, biblioteca, laboratorios, aulas taller) y de recreación (auditorio, parqueaderos, canchas, gimnasio) las cuales son propensas a sufrir cualquier tipo de acción hostil.

  La seguridad contra desastres del instituto no se lo ha realizado debido a que este no posee un departamento de seguridad quien se encargue de la elaboración de planes de evacuación y desastres.

* **Investigación descriptiva.-** Fue necesario dividir en tres áreas para facilitar la investigación. El área administrativa es la más propensa a sufrir cualquier tipo de acción hostil debido a la gran afluencia de personas propias, ajenas a la institución, a la falta de salidas de emergencia, planes de evacuación y contingencia.

* **Investigación explicativa o correlacional.-** Se descubrió que del área administrativo, en varias ocasiones fueron sustraídos algunos bienes personales e institucionales; situaciones que se han presentado debido a: la falta de precaución, a la facilidad que tienen todas las personas para ingresar a estas dependencias a falta de un plan operativo de control de acceso; es decir estas dependencias por la importancia que tienen en el desarrollo institucional, deberían estar custodiadas por guardias en cada piso, o un sistema electrónico de visión e inclusive se debe optimizar el ingreso y la salida principal del instituto tanto ha visitantes, estudiantes y vehículos.

  En el área educativa se ha registrado un mínimo de robos, ya que en estos lugares no existen materiales o equipos propensos a pérdidas y también debido a que este sector es de uso exclusivo de docentes y dicentes del Instituto.

  Las pérdidas que se han dado en el área recreacional han sido por descuido del personal que hace uso del sector de las canchas deportivas, ya que muchas veces se olvidan de sus pertenencias, tales como: celulares, llaveros, dinero, etc. El sector de los parqueaderos es muy seguro ya que se encuentran a la vista del personal que realiza la guardia en las dos prevenciones del ITSA.

4.4 Universo población y muestra:

El Instituto Tecnológico Superior Aeronáutico, fue considerado como el escenario para realizar la indagación respectiva; esto implica al total de sus integrantes (Autoridades, docentes, administrativos, estudiantes y auxiliares).

En el área administrativa, trabajan cincuenta profesionales, a quienes nos hemos permitido investigarlos mediante las técnicas de entrevista y encuesta. Debido al pequeño número de investigados y de acuerdo a una norma universal (ver tabla 4.1) no es recomendable realizar una muestra, ya que existiría fallas en la obtención de la información.

Tabla 4.1 Fórmula para establecer la muestra.

$n = \frac{Z_{\forall}^{2} * p * q}{e^{2}}$	n = número de elementos que debe poseer la muestra = riesgo o nivel de significación z = puntuación correspondiente al riesgo que se haya elegido. Por ejemplo, para un riesgo del 5%; = 0.05 (Z = 1.96) p = % estimado q = 100-p e = error permitido.

Fuente: Apuntes de la Asignatura de Elaboración de Proyectos.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla 4.2 Tabla de personal administrativo.

INFORMANTES	CANTIDAD
Personal Directivo	7
Personal Administrativo	43
TOTAL	50

Fuente: Investigación de Campo.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

4.5 Métodos y técnicas de la investigación.

4.5.1 Métodos.

* **Análisis.**

Este método permitió reconocer de manera ordenada las áreas vulnerables a sufrir cualquier tipo de desastre o robo. Encontrando que el área administrativa es la prioritaria debido a los documentos y material que se maneja en esta área, también es necesario precautelar el área académica y de recreación ya que con esto se obtendrá una seguridad total del Instituto.

Cabe mencionar que el área administrativa comprende los departamentos de: rectorado, vicerrectorado, secretaria académica,

docencia, educación a distancia, sistemas, finanzas, logístico y recursos humanos, en estos se maneja documentos (reporte de notas, exámenes, planos del instituto, escolástico, carnetización, proyectos de grado, etc.), en los cuales la única seguridad que existe es la protección por parte de los encargados ya que se utiliza un sistema convencional manual(cerraduras, candados, cadenas).

En el área académica se debe dar prioridad a los laboratorios, aulas taller debido a los materiales (líquidos inflamables y hidráulicos) y equipos (computadoras, osciloscopios, multímetro, microprocesadores, etc.), que son utilizados con frecuencia en estos.

El área de recreación necesita la protección de sus equipos (infocus, amplificadores, parlantes, micrófonos, etc.) y materiales (balones, pesas, equipo de heterofilia, etc.), que son utilizados por todos los miembros de la institución.

* **Síntesis.**

Se ha permitido focalizar las áreas vulnerables, llegando a una idea general del estado actual del sistema de seguridad existente y de la distribución de los espacios físicos de la institución, así como también enunciar las posibles alternativas para solucionar estos inconvenientes.

* **Deducción.**

Para este proceso de investigación nos ubicamos en la parte externa de la institución y realizamos una observación de las instalaciones del instituto, encontrando una falta de control del ingreso y salida tanto de personas como de vehículos pertenecientes y ajenos a la institución, dando lugar a que las áreas que se detallo en la síntesis se tornen vulnerable a acciones hostiles.

* **Inducción.**

  La aplicación de este método no fue necesaria, puesto que con la deducción se partió de un problema en general que es la seguridad de instituto hasta llegar a un problema específico que es la falta de seguridad en cada área de la institución.

4.5.2 Técnicas.

* **Observación:**

  Las fichas de observación directa, diseñadas de acuerdo a la necesidad de la investigación, sirvió para recopilar información de lugares, áreas, dependencias, en que estado se encuentran las zonas mencionadas además nos proporciona criterios prospectivos.

  Con el objeto de determinar las áreas o secciones más vulnerables, se realizo fichas de observación mediante las cuales se pudo determinar que el área administrativa y el área académica, son las mas propensas a robos, las cuales fueron consideradas de la siguiente manera: planta baja (ver anexo D), primer piso (ver anexo E), segundo piso (ver anexo F), tercer piso (ver anexo G), áreas anexas del Instituto (ver anexo H).

  De esta manera se comprobó que el instituto no cuenta con un sistema de seguridad que proteja todas las instalaciones y contribuya a prevenir robos (ver anexo I).

* **Encuesta**

  Aplicada esta técnica, mediante preguntas dicotómicas, el personal administrativo que labora en las dependencias, manifestaron sus requerimientos relacionados con la seguridad, de cuyas respuestas se puede apreciar la urgente necesidad por un nuevo régimen que otorgue

confianza y de esta manera cumplir con satisfacción cada una de sus actividades.(ver anexo J)

* **Entrevista.**

Facilitó establecer un contacto directo con las personas que anteriormente se encontraban relacionadas con los diferentes sistemas de seguridad implantados entre los años 2002 y 2005; este procedimiento fue realizado por los estudiantes de la institución a través de proyectos de graduación.

Para el efecto, se diseñó la entrevista estructurada la que consta de un cuestionario previamente elaborado, aplicado a: Subp. Padilla Milton, Supervisor del Departamento de Logística (ver anexo K). La no estructurada, es aquella que se la realiza de manera espontánea, aplicada a: Subp. (r) Segovia Mario, ex-supervisor de EPAE, Sgos. Oyaque Rubén Técnico de Abastecimientos, Sgos. Coello Freddy Técnico encargado de la seguridad del ITSA, Sgos. Stalyn Tulchán Técnico encargado de la Escuela de Idiomas (ver anexo L).
La conversación establecida con el señor Subp. Padilla Milton, nos permitió conocer la ubicación del circuito cerrado de televisión y el estado en que se encuentra actualmente, es decir inhabilitado.
De igual forma, el señor Subp. Segovia Mario, nos manifestó el estado en que se encontraban los monitores de los sistemas anteriores ubicados en los ingresos principales y perímetros de la institución.

Así mismo, el señor Sgos. Oyaque Rubén, también contribuyo con información relacionada con la fase de este sistema ubicado en los ingresos principales y perímetros de la institución.

El señor Sgos. Stalyn Tulchán, con mayor detalle nos explicó a cerca del circuito cerrado de televisión en la escuela de idiomas y que no funciona porque a su parecer no era necesario.

Del diálogo con el señor Sgos. Coello Freddy, nace la idea de establecer un sistema de seguridad en el área administrativa.

De manera tal que, la técnica de la entrevista contribuyó positivamente con información real, precisa e indispensable para crear un nuevo procedimiento de protección.

4.6 Recolección de datos.

Mediante la observación se logro obtener información acerca de las falencias que existe en la seguridad de la institución, siendo estas: la falta de control de acceso a personas y vehículos, la libertad de acceso a cualquier área, el ingreso y salida de personas por lugares no estipulados.

Se utilizaron fichas de observación para obtener información primaria, estas fueron aplicadas para determinar los tipos de riesgos tales como: desastres (incendios, movimientos telúricos y condiciones climatológicas), acciones hostiles (robo, fraude y sabotaje) a los que se encuentran expuestas las distintas áreas que conforman el ITSA.

Las encuestas y entrevistas ayudaron a obtener datos secundarios verdaderos y confiables de las personas que tuvieron relación con los sistemas de seguridad anteriormente implantados en cuanto a su funcionamiento y las causas de porque fueron deshabilitados, por ejemplo la sustracción de: las cámaras, el cable de alimentación de un monitor.

Los proyectos diseñados sirvieron como guías para el desarrollo del trabajo investigativo, ya que facilitaron información valiosa como es: los antecedentes de la investigación y la importancia de la seguridad que necesita una institución.

4.7 Procesamiento de la información.

Una vez recopilada la información, de acuerdo a lo que consta en el plan metodológico, se tomó en cuenta los resultados obtenidos a través de: la

observación directa, la exploración, las entrevistas y encuestas para posteriormente procesarlas de manera jerárquica.

* Tabulación de datos.
* Codificación de datos.
* Representación gráfica en cuadros y gráficos.

De manera sucinta, globalizamos la información que se ha obtenido por medio de la investigación. Dividimos la institución por áreas; exploramos los sistemas existentes; obtuvimos información a través de entrevistas y encuestas, nos apoyamos, ocasionalmente en proyectos anteriores; receptamos información electrónica.

4.7.1 Análisis e interpretación de la información obtenida.

4.7.1.1 Observación.

* **Planta baja.-** Luego del análisis realizado en la ficha de observación se determinó como puntos vulnerables el área académica (laboratorios y aulas taller) por los equipos y materiales existentes dentro de estas dependencias.

* **Primer piso.-** Esta planta presentó vulnerabilidad en los laboratorios de informática, escuela de idiomas y biblioteca debido al valor del material y equipos encontrados en este piso.

* **Segundo piso.-** Se determinó que el área administrativa es vulnerable, de mayor importancia por la existencia de información de recursos personales e institucionales; debido al ingreso constante de personas a las cuales no se las puede identificar como propias o ajenas a la institución. Sumándose a esta inseguridad la no presencia de señalización en caso de evacuaciones en esta área y la falta de sistemas que alertan de una manera temprana incidentes como incendios.

* **Tercer piso.-** En esta planta únicamente se encontró como un punto critico al laboratorio de sistemas de comunicación.

* **Exteriores.-** Esta por ser el área más concurrida se determinó varios puntos que requieren seguridad como: parqueaderos, gimnasio, prevenciones y auditorio ya que tienen libre acceso de personas propias y extrañas a esta Institución.

4.7.1.2 Encuesta

PREGUNTA 1

¿CONOCE USTED SI EN EL INSTITUTO EXISTE ALGÚN TIPO DE SISTEMA DE SEGURIDAD?

Tabla Nº 4.3 Análisis porcentual primera pregunta.

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
“SI”	15	30	30
"NO"	35	70	70
Total	50	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

Después de realizar un análisis de cada pregunta de las encuestas se determinó el siguiente porcentaje.

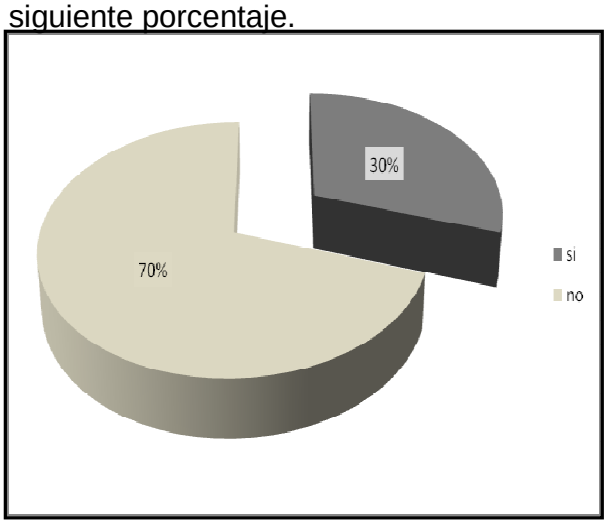


Fig. 4.1 Gráfica porcentual primera pregunta.

Análisis

En el ITSA el 70 % del personal administrativo encuestado desconoce acerca de un sistema de seguridad, esto se debe a la falta de información puesto que solo un 30% del personal conoce sobre este tema.

Interpretación de resultado

Se ha podido constatar que, gran parte del personal que labora en el ITSA desconoce la existencia de algún sistema de seguridad.

PREGUNTA 2

¿DURANTE EL TIEMPO QUE USTED VIENE TRABAJANDO EN LA INSTITUCIÓN, CONOCE DE PÉRDIDAS Y ROBOS SUSCITADOS?

Tabla Nº 4.4 Análisis porcentual segunda pregunta.

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
"SI"	45	90	90
"NO"	05	10	10
Total	50	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

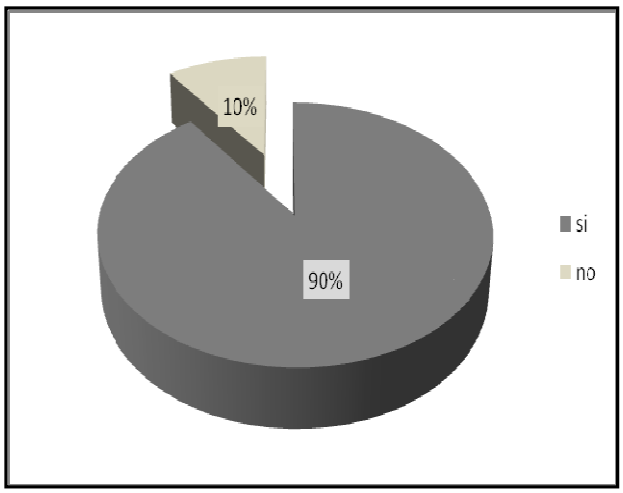


Fig. 4.2 Gráfica porcentual segunda pregunta

Análisis

El 90% del personal conoce sobre pérdidas o robos suscitados dentro del Instituto, esta cifra es alarmante y necesaria para implementar nuestro sistema, en cuanto al 10% no tiene conocimiento exacto de estos hechos por cuanto se encontraba de vacaciones.

Interpretacion de resultados

Como se ha podido observar en las encuestas realizadas existe inseguridad en el área administrativa.

PREGUNTA 3

¿EN SU ÁREA DE TRABAJO HAN EXISTIDO PÉRDIDAS O ROBOS DE OBJETOS Y/O MATERIALES PERSONALES E INSTITUCIONALES QUE SE ENCUENTRAN BAJO SU RESPONSABILIDAD?

Tabla Nº 4.5 Análisis porcentual tercera pregunta.

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
"SI"	26	52	52
"NO"	24	48	48
Total	50	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

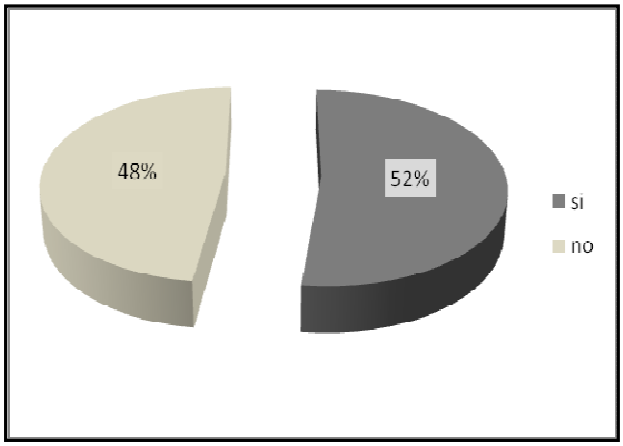


Fig. 4.3 Gráfica porcentual tercera pregunta

Análisis

El 52% de los encuestados manifiestan que en el área administrativa si a existido robos y perdidas personales e institucionales, mientras que el 48% no ha tenido pérdidas.

Interpretación de resultados

Es evidente que sin un sistema de seguridad eficiente no se ha podido contrarrestar las constantes pérdidas materiales que ha sufrido la institución.

PREGUNTA 4

¿QUÉ TIPO DE SEGURIDAD POSEEN LAS INSTALACIONES DONDE USTED TRABAJA ACTUALMENTE?

Tabla Nº 4.6 Análisis porcentual cuarta pregunta.

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
"SI"	44	88	88
"NO"	06	12	12
Total	50	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

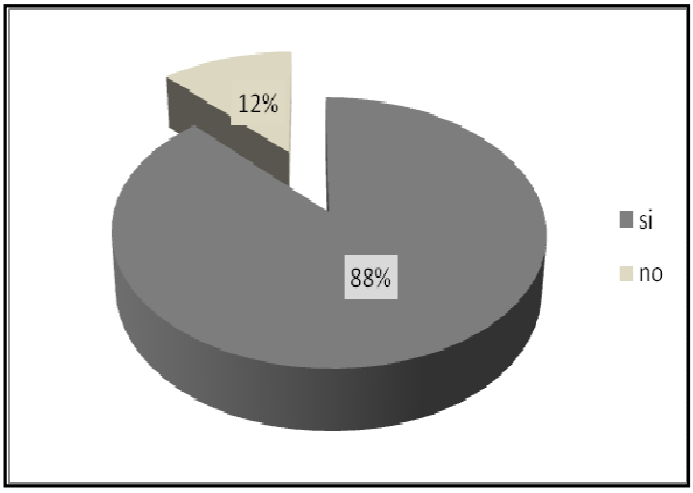


Fig. 4.4 Gráfica porcentual cuarta pregunta

Análisis

El 88% del personal menciona que si existen sistemas de seguridad mínimas en cada una de sus dependencias, y el 12% no conoce ningún sistema de seguridad.

Interpretación de resultados.

Solo las chapas de las puertas en la mayoría y en otra ninguna medida de seguridad.

PREGUNTA 5

¿CONSIDERA USTED QUE LA INFRAESTRUCTURA Y LOS BIENES MATERIALES DE LA INSTITUCIÓN SON MÁS VULNERABLES CON EL CRECIMIENTO DE LA POBLACIÓN ESTUDIANTIL DEL ITSA?

Tabla Nº 4.7 Análisis porcentual quinta pregunta.

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
"SI"	15	30	30
"NO"	35	70	70
Total	59	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

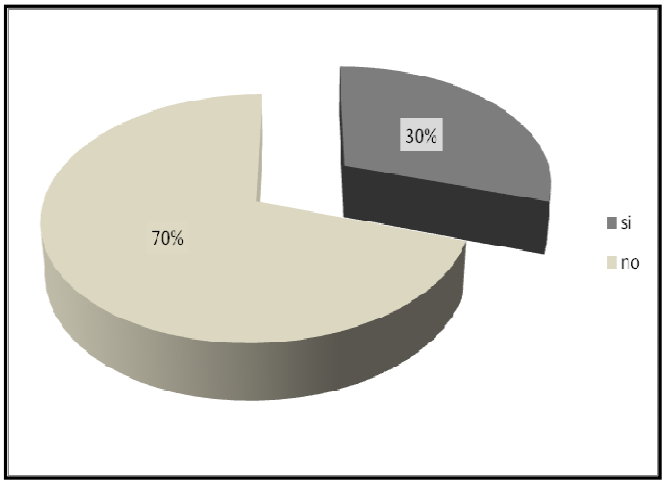


Fig. 4.5 Gráfico porcentual quinta pregunta

Análisis

El 70% del personal encuestado considera que en el Instituto se a incrementado la vulnerabilidad con el incremento de estudiantes y un 30% manifestó que no influye.

Interpretación de resultados

Con el constante crecimiento estudiantil y afluencia de visitantes se torna difícil el control únicamente de la prevención, por lo tanto las instalaciones del ITSA se ven vulneradas frente a hechos de robo.

PREGUNTA 6

¿QUÉ TIPO DE MEDIDAS DE SEGURIDAD HA ADOPTADO PARA EVITAR INCIDENTES O PÉRDIDAS?

Análisis

Cada uno de los empleados a través de sus propios recursos cuida los bienes de los departamentos del área administrativa.

Interpretación de resultados

No existe sistema de seguridad que cumpla medidas eficientes dentro del ITSA.

PREGUNTA 7

¿SEGÚN SU CRITERIO QUE ÁREA, DEPARTAMENTO, SECCIÓN O LABORATORIO CREE QUE ES LA VULNERABLE A ROBOS?

Análisis

El área administrativa es la que más necesita seguridad, según el informe de las encuestas; además, los laboratorios también requieren de un control; estas dos dependencias son muy vulnerables a robos perdidas.

Interpretación de resultados

El área administrativa es la más expuesta a sufrir pérdidas materiales.

PREGUNTA 8

¿CONSIDERA USTED NECESARIO LA IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD QUE AYUDARÍA DE MEJOR MANERA A LA VIGILANCIA Y DESENVOLVIMIENTO DE LAS LABORES QUE SE REALIZA EN LA INSTITUCIÓN?

Tabla Nº 4.8 Análisis porcentual octava pregunta

Válido	Frecuencia	Porcentaje (%)	Porcentaje Válido (%)
"SI"	48	96	96
"NO"	02	04	04
Total	50	100	100

Fuente: Encuesta al personal administrativo
Autor: Cbos. Téc. Avc. Puetate Rodrigo.

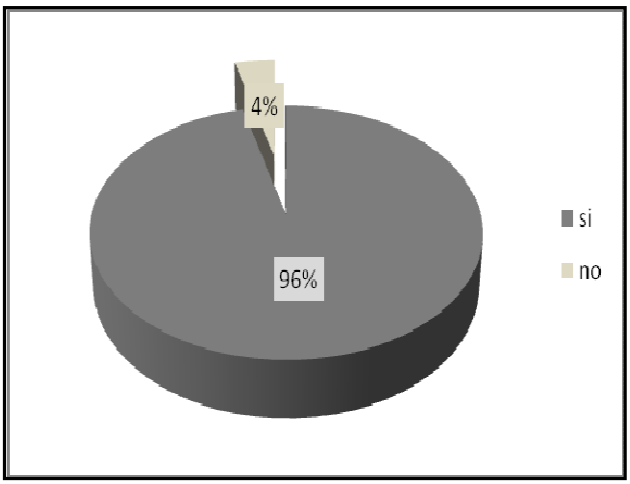


Fig. 4.6 Gráfico porcentual octava pregunta.

Análisis

El 96% de encuestados, considera que es necesaria e imperiosa la instalación de un nuevo sistema de seguridad.

Interpretación de resultados

El personal del ITSA considera que es necesaria la implementación de un sistema de seguridad para otorgar mayor confianza durante el trabajo diario.

4.7.1.3 Entrevistas

Se entrevistó a la persona encargada de la seguridad total del ITSA.

Entrevista

Lugar: Departamento logístico.

Fecha: 21-febrero-2008.

Entrevistado: Subp. Padilla Milton.

Entrevistador: Srta. Puco María.

Tipo de Entrevista: cerrada

Esta entrevista se realizó para obtener los antecedentes de los proyectos anteriores de la institución.

Primera pregunta

¿Cuántos sistemas de seguridad fueron instalados en el ITSA?

Tres proyectos instalados hasta la actualidad.

Segunda pregunta

¿Qué sistemas estaban instalados y cual es su ubicación?

Del primer proyecto fueron cámaras, estuvieron a la entrada principal del edificio, enfocando a la salida, la segunda en la entrada posterior, enfocando a la salida y la tercera que estuvo en la sastrería junto a la prevención dos, fueron robadas a la semana de su colocación.

Del segundo proyecto la cámara estuvo ubicada en la esquina del ITSA, al norte del Hermano Miguel, la misma que también fue robada a la semana.

Los monitores de los dos proyectos anteriores se encuentran almacenados en la bodega del ITSA.

El tercer proyecto se realizó en el laboratorio de ingles para poder monitorear a los alumnos que se encontraban rindiendo exámenes (English Curse Language) ECL se encuentran instaladas en los mismos sitios de su colocación y el monitor de este proyecto se encuentra en la bodega de idiomas.

Tercera pregunta

¿Desde cuándo ya no están en funcionamiento los sistemas de seguridad?
No recuerda exactamente pero más o menos hace un año y medio o dos.

Cuarta pregunta

¿Por qué han dejado de funcionar los sistemas de seguridad?
Nos supo manifestar que fue por la falta de cuidado de estos sistemas pero no tenia toda certeza de estos, para lo que nos sugirió realizar una investigación con el suboficial Mario Segovia y el Sargento Rubén Oyaque quienes fueron encargados principales de este sistema.

Entrevista

Lugar: Departamento logístico.
Fecha: 9-Abril-2008.
Entrevistado: Subp. Segovia Mario.
Entrevistador: Srta. Puco María.
Tipo de Entrevista: abierta

Con esta información se realizó la entrevista vía telefónica al Suboficial Mario Segovia, con respecto al por qué dejaron de funcionar los sistemas de seguridad aludidos, frente a lo cual manifestó:
Que existían dos monitores en la prevención principal, el grande y el pequeño, con respecto al monitor pequeño no tiene conocimiento, pero del monitor grande si; estuvo funcionando correctamente y solo le hace falta el cable del monitor para que funcione.

Entrevista
Lugar: Departamento logístico.
Fecha: 10-abril-2008.
Entrevistado: Sgos. Rubén Oyaque.
Entrevistadora: Srta. Puco María.
Tipo de Entrevista: abierta

La siguiente entrevista se realizó a otro encargado de los sistemas de seguridad, quien manifestó:

El sistema de seguridad que consistía de un circuito cerrado de televisión (CCTV) si funcionaba correctamente, pero como no existió ningún encargado del cuidado de este sistema, se sabe que una persona pidió prestado el cable del monitor grande para ver videos, pero al momento de conectar nuevamente el cable al monitor este ya no funcionó.

Con estas dos entrevistas ya se pudo comprobar que el problema de este circuito fue la falta de control, mantenimiento y cuidado.

Entrevista
Lugar: Escuela de idiomas.
Fecha: 10-abril-2008.
Entrevistado: Sgos. Stalyn Tulchán.
Entrevistadora: Srta. Puco María.
Tipo de Entrevista: abierta

El Sgos. Stalyn Tulchán es encargado de los laboratorios de ingles, el cual explicó que este equipo ya no se encuentra en uso desde hace unos dos años.

Aquí hay que mencionar que el Sgos. Stalyn Tulchán fue quien realizó la desconexión de los equipos puesto que ya no ofrecían ninguna utilidad.

Entrevista

Lugar: Departamento Logístico.

Fecha: 11-Marzo-2008.

Entrevistado: Sgos. Freddy Coello.

Entrevistadora: Srta. Puco María.

Tipo de Entrevista: abierta

Esta entrevista se realizó con un claro objetivo de encontrar información sobre la seguridad física que posee y/o requiere la institución.

La siguiente entrevista se realizó a uno de los encargados de la seguridad del ITSA y supo expresar lo siguiente:

El instituto no tiene ningún sistema de seguridad activo hasta el momento, por lo que, sugiere que la institución implemente un sistema de seguridad, que responda a las necesidades institucionales.

A su juicio cree conveniente instalar un sistema de seguridad al ingreso del área administrativa ya que es donde se han producido robos y es necesario darle seguridad electrónica con: Cámaras, Censores con sirena, control de accesos y sugirió un plano para la instalación de los equipos que podrían estar de la siguiente forma:

Uno al ingreso del rectorado, dos al ingreso o salida del área administrativa, tres en el pasillo de las oficinas y la cuarta junto a enfocando a la salida de finanzas, en cuanto a los censores se necesitaría nueve y el control de acceso que se debería colocar en las puertas principales a las áreas.

1. Cámaras
2. Sensores
3. Control de acceso

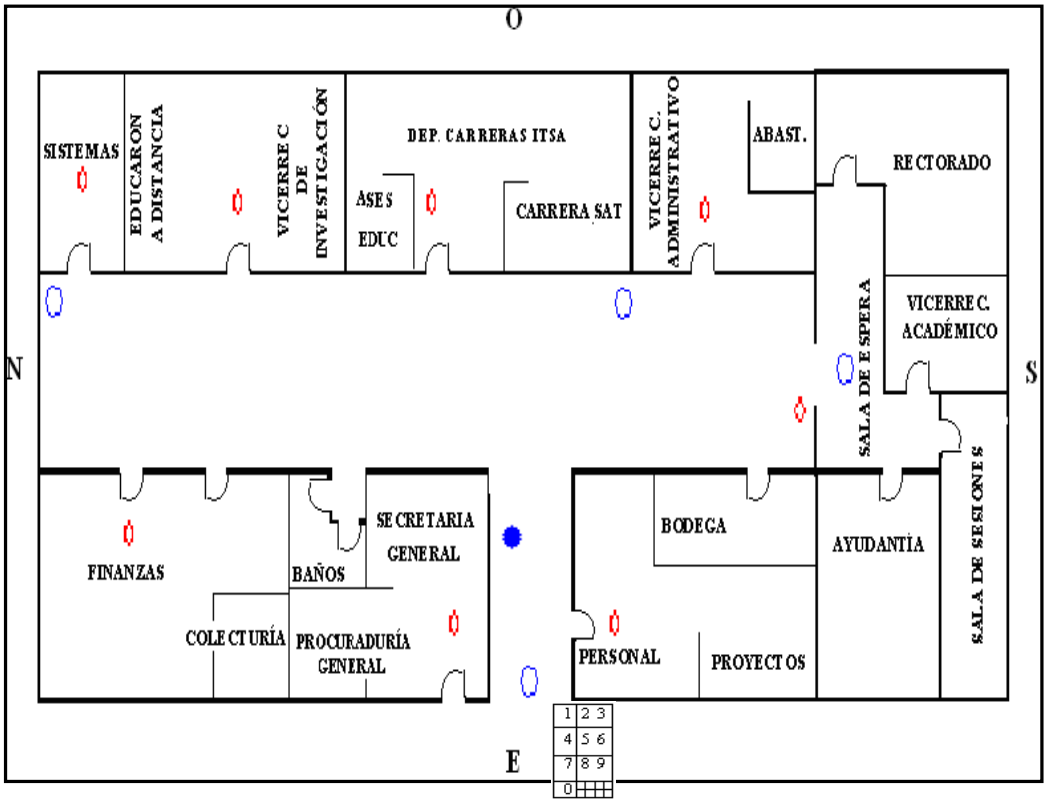


Fig. 4.7 Sugerencia del sistema de alarma para el área administrativa.

En base a las entrevistas se realizo las pruebas de los equipos de seguridad existentes. Se determinó que el monitor grande está en buenas condiciones por lo tanto se lo puede utilizar dando tratamiento necesario, desmintiendo así las versiones anteriormente descritas por las personas que operaban con estos equipos. El monitor pequeño no se pudo determinar su funcionamiento, debido al robo de las cámaras.

4.8 Análisis e interpretación de resultados.

En base a la información obtenida y luego de su respectivo estudio, se ha llegado a determinar que el ITSA no cuenta con un sistema de seguridad adecuado, de forma tal que la incertidumbre persiste en el personal administrativo.

4.9 Conclusiones y recomendaciones.

4.9.1 Conclusiones:

* La seguridad tiene como finalidad garantizar la integridad de personas, objetos y procesos, los cuales deben ser custodiados de cualquier riesgo que implique peligro; con seguridad se puede crear un ambiente laboral en donde las personas se desempeñen con eficiencia.

* El Instituto, actualmente no cuenta con un sistema de seguridad eficiente que brinde la protección adecuada a todas sus dependencias, y por lo tanto a quienes conforman la comunidad del ITSA.

* El ITSA no cuenta con planes para prevenir desastres naturales.

* La seguridad física del instituto no es eficiente para contrarrestar todas las acciones hostiles que se pueden suscitar dentro de esta.

* En base a la utilidad de instrumentos se concluye que las áreas más vulnerables son las: administrativa, laboratorios, aulas taller, auditorio, bloque 42, parqueaderos, biblioteca y gimnasio.

* Los sitios que más necesitan control y protección son los departamentos de sistemas, finanzas, educación a distancia, docencia, logística, rectorado, vicerrectorado y laboratorios, debido a la información que se encuentra en este lugar y al libre acceso de personas a estas dependencias.

* El ITSA hace dos años si disponía de un sistema de seguridad en circuito cerrado, debido a la falta de cuidado y mantenimiento ha hecho que dejen de funcionar estos equipos que eran muy indispensables para la seguridad de la institución.

* Los desastres, siniestros, hurtos son aspectos que se presentan sin aviso

alguno, por lo tanto toda institución debe preveer para no lamentar.

4.9.2 Recomendaciones.

* Implementación de un sistema de seguridad que permita proteger todos los recursos y bienes del ITSA.

* Implementación de un sistema de seguridad contra incendios que pueda evitar cualquier desastre a futuro.

* Elaboración de planes de evacuación y seguridad antidesastres.

* Creación un departamento de seguridad para que haya un control diario del movimiento del personal en el ITSA.

* Recomendamos que a futuro, se complemente el sistema con otros que estén acorde a la tecnología y ubicados en lugares estratégicos, capaz que puedan ser observados y cuidados en caso de atentados.

* Implementación un sistema de seguridad electrónico, en el área administrativa.

* Instalación de un MODEM que permita mantener el control del sistema de seguridad mediante un equipo capacitado para el efecto.

* Implementación de un sistema biométrico para mantener un eficiente control de quienes ingresan y salen del instituto.

* Instalación de un control de acceso mediante tarjetas de proximidad, para todo el personal del ITSA.

* La construcción de garitas en el área perimetral con la finalidad del control del personal por lugares no autorizados.

* Utilización de la entrada principal como único acceso de personas a la

Institución.

* Que en cada piso debe existir un centinela de ronda el cual se encargue del control de visitantes.

* Debido a la afluencia de visitantes, docentes y estudiantes, las garitas deberían tener mínimo dos personas.

* Los pocos implementos del sistema anterior que aún pueden ser rescatados, sugerimos que se realice su reactivación a tiempo a fin de evitar su deterioro total.

* Un sistema de seguridad llega a ser eficiente cuando los perímetros institucionales disponen de muros y cerramientos, consecuentemente aconsejamos construir aquellos que faltan.

* Instalación de cámaras de video en las áreas del parqueadero vehicular.

CAPÍTULO V

FACTIBILIDAD

5.1 Factibilidad del problema.

5.1.1 Factibilidad técnica.

Los sistemas de seguridad que requiere la institución se detallan a continuación:

Tabla No. 5.1 Circuito cerrado de televisión (CCTV).

CIRCUITO CERRADO DE TELEVISIÓN (CCTV).		
Cantidad	**Descripción**	**Características**
8	Cámaras domo de 420 TVL's.	* Modelo DP-914M * Ideal para ambientes interiores. * Pequeño Domo a Color. * Señal del sistema PAL/NTSC * Resolución 420 TV líneas. * Angulo de Visión 70° * Alimentación DC12V ± 10% * Consumo Corriente 100 mA.
26	Cámaras inalámbricas	* Elemento de imagen Sensor CMOS Color de 1/3" * Ángulo de visión 62º. * Resolución 380 líneas de TV. * Frecuencia 1.2 GHz * Alimentación 8 Vcd. * Dimensiones 80mm (alto) x 45mm (ancho) * Alcance sin obstáculos 100 m sin obstáculos.

Fuente: Investigación realizada.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.2 Elemento reproductor y grabador de imagen.

ELEMENTO REPRODUCTOR Y GRABADOR DE IMAGEN		
Cantidad	**Descripción**	**Características**
1	Computador para (CCTV)	**HARDWARE** * Procesador: CPU Intel Pentium IV. * Memoria RAM: 512 Mb en adelante. * Cap. de Disco Duro: 80 Gb o superior. **SOFTWARE** * Sistema Operativo: Microsoft Windows XP Profesional versión 2002
2	Tarjeta de vídeo Capturadora.	* 16 canales MAXDVR.

Fuente: Investigación realizada.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.3 Control de accesos.

CONTROL DE ACCESOS		
Cantidad	**Descripción**	**Características**
1	Central	* PR-112S-A STAND ALON (Enforcer).
2000	Tarjetas de Acceso	* Tarjetas de Proximidad (Enforcer).
2	Cerradura	* Cerradura Electromagnética. * 600 lbrs. de fuerza. * Alimentación de 12 Vcd.
2	Pulsador	* Pulsador Normalmente Cerrado (NC).

Fuente: Investigación realizada.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.4 Sistema de seguridad electrónico.

SISTEMA DE SEGURIDAD ELECTRÓNICO		
Cantidad	**Descripción**	**Características**
2	Central de alarma	* PC 1864 (DSC), 8 zonas expandible a 64 * 8 particiones. * búfer de 500 eventos.
2	Sirena	* Sirena de 30 watts DSC.
2	Transformador	* Transformador de 110 Vac a 12 Vcd
2	Batería	* Batería BD 412 (12 V de 4 A). * Peso: aprox. 2.58kg (5,68 lbs.), de Pb.
11	Teclado	* PC 1555RF de LEDS 8 zonas. * Visualizador de LCD. * 4 teclas programables de funciones. * Botones de fácil identificación para * incendio, emergencia y de pánico.
22	Sensores de movimiento	* Detector infrarrojo pasivo Bravo 6. * Inmunidad contra mascotas hasta de 85 lb. (38 kg) de peso. * Cobertura lateral de 15,2 m. * Cobertura Superior de 18,2 m.
11	Contactos Magnet.	* Contactos Magnéticos Adhesivos. * Color café y blanco.
7	Detectores humo	* Detector de calor, de sensor doble, Incorporado - 135℉ (57 ℃). * Resonador incorporado de 85 dB.
4	Extensores.	* Añade 8 zonas por cableado directo. * Suministro eléctrico auxiliar de 125 mA. * Compatible con los tableros de control Power1832® y Power1864MF

Fuente: Investigación realizada.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

5.1.2 Factibilidad operativa

Estos sistemas de seguridad deberán cumplir con todas las características necesarias de operación y una excelente facilidad por el usuario: además debe ofrece: durabilidad, compatibilidad, fácil manejo, implementación y programación.

5.1.3 Factibilidad económica.

Tabla No 5.5 Costos del circuito cerrado de televisión para el ITSA.

CIRCUITO CERRADO DE TELEVISIÓN (CCTV)			
Cantidad	**Descripción**	**Valor unitario**	**Valor total**
2	Tarjeta de video de 4 canales MAXDVR	200,00	400,00
26	Cámaras domo Sony de 420TVLs.	99,75	2593,50
2	Cámaras inalámbricas	100.00	200,00
12	Rollos de cable coaxial (5E / 75Ω.)	90,00	1080,00
1	Rollo de cable eléctrico	60,00	60,00
48	Conectores (BNC) de video	1,00	48,00
2	Computadores.	700,00	1400,00
		TOTAL:	**$5781,50**

Fuente: Cotizaciones
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.6 Costos del control de acceso para el ITSA.

CONTROL DE ACCESO			
Cantidad	**Descripción**	**Valor unitario**	**Valor total**
1	Control de access STAND ALON	1200,50	1200,50
1000	Tarjetas de Proximidad (Enforcer)	4,00	4000,00
1	Batería	17,00	17,00
1	Rollo de cable gemelo.	60,00	60,00
1	Transformador 110 Vac a 12 Vac	20,00	20,00
2	Cerradura Electromagnética.	100,00	200,00
		TOTAL:	**$5497,50**

Fuente: Cotizaciones.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.7 Costos del sistema de seguridad electrónico para el ITSA.

SISTEMA DE SEGURIDAD ELECTRÓNICA			
Cantidad	**Descripción**	**Valor unitario**	**Valor total**
2	PC 1864 (DSC), 8 zonas hasta 64 z.	210,00	420,00
22	Sensores de movimiento.	17,50	385,00
11	Contactos Magnéticos	3,00	33,00
6	Rollo de cable UTP categoría 5E	150,00	900,00
5	Cinta Aislante de color negro	0,80	4,00
1	Masking	1,00	1,00
7	Detector de humo.	50,00	350,00
1	Software de monitoreo DLS.	400,00	400,00
1	Modem D-12	190,00	190,00
TOTAL:			**$2683,00**

Fuente: Cotizaciones.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla No 5.8 Costos de todos los sistemas requeridos para el ITSA.

COSTO TOTAL.	
DESCRIPCIÓN	**CANTIDAD**
Sistema electrónico de seguridad (S.E.S)	5781,50
Circuito cerrado de televisión (CCTV)	5497,50
Modem de comunicación y monitoreo del (S.E.S)	2683,00
TOTAL:	**$ 13962,00**

Fuente: Cotizaciones
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Se concluye que por el alto costo de todos los sistemas que se requiere para la seguridad del Instituto, únicamente se cubrirá una parte con la utilización de Circuitos cerrados de televisión y sistemas de seguridad electrónica.

5.1.4 Denuncia del tema.

“IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD ELECTRÓNICO EN EL DEPARTAMENTO DE FINANZAS DEL ITSA”

5.2 Factibilidad del tema.

5.2.1 Factibilidad Técnica.

Pese a que “no existe en nuestro país una normativa específica que regule la instalación y utilización de mecanismos de control y vigilancia con videocámaras o micrófonos en los centros de trabajo, por tal razón se tomó como referencia normas implantadas de otros países. Además, tampoco existen leyes al respecto, por lo que pueden ser usados estos sistemas. Pese a que el Estatuto de los Trabajadores permite la utilización de sistemas de vigilancia, también recuerda que debe respetarse la dignidad del trabajador. Además, los sistemas utilizados deben servir sólo para vigilar y no deben captar conversaciones o situaciones que vulneren el derecho a la intimidad.”[24]

Para la implementación del presente proyecto, se observo la necesidad de las siguientes características de los equipos a utilizar:

5.2.1.1 Central de alarma:

* Zonas en la tarjeta 8z expansible a 64 zonas.
* Zonas con cable 64z.
* Zonas inalámbricas 32z.
* Salidas PGM en la tarjeta.
* Teclados 8T.
* Particiones 8P.
* Códigos de usuario 94 mas código maestro.
* Memoria de eventos 500.
* Consumo de corriente 110 mA.
* Baterías alternas.

[24] http://www.belt.es/noticias/2004/octubre/05/camaras_trabajo.htm

5.2.1.2 Extensor de 8 zonas por cableado directo:

* Añade 8 zonas por cableado directo
* Suministro eléctrico auxiliar de 125 mA (protegido)
* Compatible con los tableros de control Power 1832 y Power 1864.

5.2.1.3 Teclado:

* Corriente de trabajo 12 Vcd.
* Conectibilidad con la central de alarma mediante cable.
* Consumo de corriente 22 mA (Normal)/85 mA (máximo).
* Pantalla tipo LCD con símbolos y números.
* 4 Teclas de función programables.
* Luces de estado listo (verde) y armado (rojo).
* Autodesplazamiento por zonas abiertas y de alarma.
* Despliegue de la hora.
* Botones de gran tamaño.
* Botones de fácil identificación para incendio, emergencia y de pánico.
* Detector de baja temperatura incorporado.

5.2.1.4 Sensores de movimiento:

* Inmunidad contra mascotas hasta de 60 lb. (25 Kg.) de peso.
* Cobertura lateral 15,2 m.
* Cobertura de superior 18,2 m.
* Análisis digital de la señal para una capacidad de detección uniforme en todo el área de cobertura.
* Compensación digital de temperatura, para un rendimiento de enganche mejorado a temperaturas críticas.
* Detección más precisa de la energía infrarroja de las personas.
* Óptima flexibilidad en la ubicación y la instalación.
* Puertos de conexión rápida.

5.2.1.5 Detectores de humo.

* Diseño de perfil bajo
* Envía informes de sensibilidad alta / baja
* Detector de calor, de sensor doble, incorporado.
* Compatible con todos los tableros de control DSC.

5.2.1.6 Contactos magnéticos:

* Durabilidad.
* Facilidad de instalación.
* Adaptabilidad.

5.2.1.7 Sirena:

* De tono alternado y fijo
* Potencia 30 (Wattios).
* Voltaje de corriente continua (c. c.) 6-12 v
* Corriente 1100 (mA).

5.2.1.8 Cable:

* Optima transferencia de datos.
* Posee 4 pares trenzados.
* Velocidad de transferencia de datos.

5.2.1.9 Materiales para la instalación:

* Destornilladores (plano y estrella)
* Pinza cortador, multímetro.
* Cautín y estaño.
* Taladro
* Brocas
* Sierra de Metal
* Pistola de Silicón
* Barras de Silicón etc.
* Extensión.

* Cinta aislante.
* Estilete.

5.2.2 Factibilidad operacional.

Este sistema debe ser de fácil manejo y operación para su funcionamiento, que cuente con un manual de usuario en donde se encuentre claramente detallado los pasos de las funciones que cumple el sistema.

Su tiempo de vida deberá ser adecuado, con esto se quiere decir que no se vuelva obsoleto a corto plazo, que al transcurrir determinado tiempo se deberá actualizar el sistema de acuerdo con la tecnología de ese entonces, y que todo cambio en la modernización de los equipos sea compatible con sus versiones anteriores y con la respectiva compatibilidad de los mismos.

5.2.2.1 Centrales de alarma.

Mediante el cuadro que se encuentra a continuación se puede concluir que se tomara como central de alarma la POWER SERIES 1864 por que presta las mejores características de funcionamiento en cuanto a las otras marcas.

Tabla N°5.9 Cuadro comparativo central de alarmas

CENTRAL ALARMA / CARACTERÍSTICAS	POWER SERIES	ADEMCO	NAPCO
Expansibilidad	0.90	0.85	0.70
Duración	0.92	0.80	0.80
Confiabilidad	0.85	0.79	0.75
Trans. De datos.	0.94	0.90	0.80
Programación	0.92	0.80	0.70
TOTAL:	**4.53**	**4.14**	**3.75**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.
Fuente: Investigación de campo.

5.2.2.2 Teclados.

Mediante el siguiente cuadro de comparación se estudiara que marcas de teclados de control de alarma electrónica es el más conveniente y factible utilizar para el proyecto de investigación.

Tabla 5.10 Cuadro comparativo teclados

TECLADOS / CARACTERÍSTICAS	POWER SERIES	ADEMCO	NAPCO
Manipulación	0.90	0.70	0.65
Duración	0.91	0.75	0.65
Confiabilidad	0.94	0.70	0.70
Compatibilidad	0.93	0.90	0.70
TOTAL:	**3.68**	**3.15**	**2.70**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.
Fuente: Investigación de campo.

5.2.2.3 Sensores de movimiento.

Mediante el siguiente cuadro de comparación se estudiara que marcas de teclados de control de alarma electrónica es el más conveniente y factible utilizar para el proyecto de investigación.

Tabla 5.11 Cuadro comparativo sensores de movimientos.

SENSOR MOV. / CARACTERÍSTICAS	POWER SERIES	ADEMCO	NAPCO
Manipulación	0.95	0.80	0.65
Duración	0.92	0.75	0.70
Confiabilidad	0.90	0.70	0.72
Compatibilidad	0.94	0.90	0.70
Sensibilidad	0.92	0.85	0.75
TOTAL:	**4.63**	**4.00**	**3.52**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.
Fuente: Investigación de campo.

De la misma manera que el cuadro anterior las características de lo sensores

POWER SERIES son mejores, por lo tanto será tomado como el mas ideal ya que es de fácil manipulación para el usuario.

5.2.2.4 Detector de Humo.

Tabla 5.12 Cuadro comparativo detectores de humo

DETECTOR HUMO / CARACTERÍSTICAS	POWER SERIES	ADEMCO	NAPCO
Manipulación	0.95	0.80	0.65
Duración	0.92	0.75	0.70
Confiabilidad	0.90	0.70	0.72
Compatibilidad	0.94	0.90	0.70
Sensibilidad	0.92	0.85	0.75
TOTAL:	**4.63**	**4.00**	**3.52**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.
Fuente: Investigación de campo.

De igual forma que en los equipos anteriormente estudiados los detectores de humo ideales en este caso también son los POWER SERIES, por esta razón también se utilizarán estos equipos en la implementación del sistema de seguridad.

5.2.3 Factibilidad económica.

Económicamente la implementación del presente proyecto es posible, por lo que resumimos la inversión.

La cantidad que se requiere está al alcance para ejecutar la tarea en los pasos respectivos, razón por la cual se concluye que la tarea es económicamente apta. Existe la relación beneficio costo.

Tabla Nº 5.13 Beneficio costo.

EQUIPOS / DEP. Ó AREAS	INVERSION EN EQUIPOS		PERDIDA DE BIENES	
RECTORADO Y VICE.	3 sensores, 1 teclado	105.00	2 celulares	180.00
DEP DE DOCENCIA	2 sensores, 1 teclado	90.00	1 Laptop	1200.00
FINANZAS	3 sensores, 1 teclado	105.00	1 Laptop	1300 00
SISTEMAS	2 sensores, 1 teclado	90.00	1 cama dig. y carg, 1 RAM, 1 disco dur.	315.00
TOTAL:		**390.00**		**2995.00**

Fuente: Investigación de campo.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Al otorgar seguridad a las instalaciones, mediante un sistema de seguridad electrónica, directamente estamos contribuyendo para que exista confianza en el personal y se pueda desenvolver en cada uno de sus funciones con eficiencia y tranquilidad; estos sentimientos no disponen de valor monetario pero su rédito resulta más positivo en cuanto a la expresión de satisfacción en el cumplimiento de su trabajo diario. De manera tal que si el desempeño es al ciento por ciento, la institución gana económicamente.

5.2.4 Apoyo.

Para la realización de este proyecto, disponemos del soporte de varias personas (TCrn. EMT. Avc. Ing. Angel Pérez, Dr. Córdova, Ing. Narcysa Mena, Ing. Dag Basantes), vinculadas con la Institución, esto conllevara a alcanzar los objetivos propuestos.

5.2.5 Recursos

Tabla Nº 5.14 Talento humano.

N	TALENTO HUMANO	DESIGNACIÓN
1	Cbos. Tec. Avc. Puetate Ramirez Rodrigo Ivan.	Investigador
2	TCrn. EMT. Avc. Ing. Ángel Pérez.	Director

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla Nº 5.15 Recurso material (primario).

Nº	MATERIAL
1	Materiales Necesarios para la ejecución

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Tabla Nº 5.16 Recurso material (secundario).

Nº	MATERIAL
1	Derecho de Grado
3	Impresiones
3	Anillados, empastados e internet
4	Varios(útiles de oficina, transporte)

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

5.2.6 Presupuesto.

5.2.6.1 Costos Primarios.

Tabla Nº 5.17 Costo primario para la implementación.

DESCRIPCION	VALOR UNIT	CANT.	VALOR TOT
Central de alarma PC 1832 (DSC), 8 zonas expandible a 32, transformador de 110 Vac a 12 Vcd, Sirena de 20 watts DSC y batería BD 412 (12 V de 4 A).	$ 190,40	1	$ 190,40
Cable UTP categoría 5E	$ 0,75	200m	$ 150,00
Contactos Magnéticos Adhesivos	$ 4,00	2	$ 8,00
Cinta Aislante de color Negro y Masking	$ 2,00	2	$ 4,00
Detector infrarrojo pasivo Bravo 6.	$ 19,05	3	$ 57,15
Detector De Humo.	$ 47,00	2	$ 94,00
Varios	$ 13,00	1	$ 13,00
SUBTOTAL GASTOS		**$ 516,55**	

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

5.2.6.2 Costos secundarios.

Tabla Nº 5.18 Costos secundarios.

N	MATERIAL	COSTO
1	Derecho de Grado	$ 297,00
3	Impresiones	$ 70,00
3	Anillados, empastados	$ 70,00
4	Internet	$ 40,00
5	Varios(útiles de oficina, transporte)	$14,00
SUBTOTAL GASTOS		**$ 491,00**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

5.2.6.3 Total gastos.

Tabla Nº 5.19 Tabla de resumen.

TABLA GENERAL	
Costos Primarios	$ 516,55
Costos Secundarios	$ 491,00
TOTAL GASTOS	**$ 1007,55**

Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

El presente proyecto de investigación, arrojó como resultados que es factible realizar la instalación de: una central de alarma, tres detectores de movimiento, dos detector de humo, dos contactos magnéticos y un teclado en el departamento de finanzas del ITSA, debido a que contamos con: los materiales, las herramientas, dinero y los conocimientos necesarios para realizar este proyecto y poder cumplirlo con éxito.

CAPÍTULO VI

DESARROLLO DEL TEMA

6.1 Introducción.

Luego del estudio realizado en el presente proyecto se determinó que es necesaria la implementación de un “Sistema de seguridad electrónico en el departamento de Finanzas del ITSA”, debido a que en este se maneja documentos importantes y también se maneja dinero de la institución.

Para la instalación se tomó en cuenta algunos aspectos como: los equipos, herramientas y materiales que son necesarios para la implementación del sistema de seguridad, los beneficiarios directos son los directores de carrera y empleados del instituto.

6.2 Material utilizado en la implementación del sistema de seguridad.

6.2.1 Central de Alarma.- Esta ubicada en el gabinete metálico # 1 en el departamento de Sistemas, se encarga directamente de controlar y procesar todas las señales de alarma que emiten los distintos elemento que conforman el sistema como son los detectores de movimiento, humo, contactos magnéticos y el teclado para luego activar una sirena que nos servirá como un anunciador de que algún evento esta ocurriendo en el lugar ya sea de intrusión o de incendio.

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.1 Central de Alarma

6.2.2 Transformador de Voltaje.- Es básicamente un reductor de voltaje, que se encuentra ubicado dentro del gabinete metálico # 2 junto a la fuente suplementaria, cuya función es regular el voltaje de entrada a la placa electrónica central del sistema la misma que es tomada de la red de voltaje del edificio, la misma que esta comprendida en el rango de los 110 Vac (Voltios de Corriente Alterna) para luego decrementarlos a 16 Vac.

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Puetate Rodrigo.

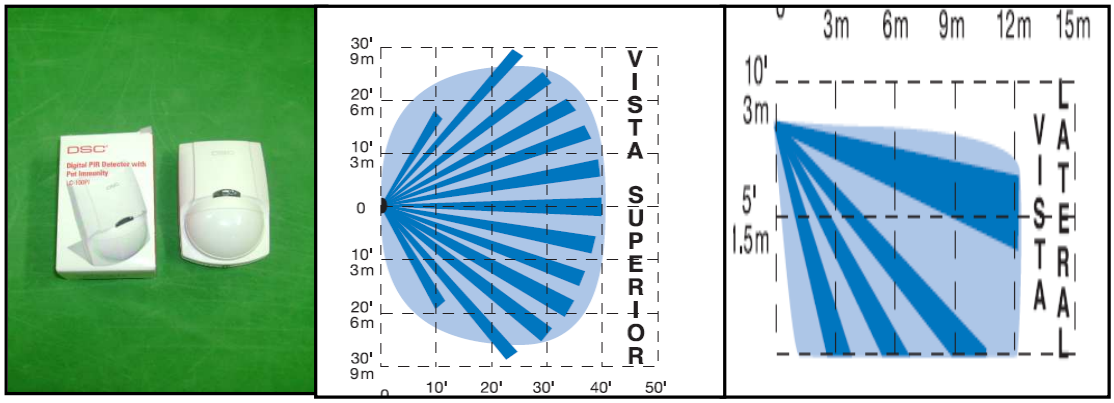
Foto 6.2 Transformador De Voltaje

6.2.2 Fuente de Poder Suplementaria (Batería).- Existe dos fuentes de energía suplementaria o alterna que se encuentran ubicadas en los gabinetes metálicos # 1 y # 2, la una esta conectada a la red de voltaje de 110 Vac. y funciona cuando existe un corte de energía en el edificio, por cuanto el sistema no debe dejar de funcionar, ya que es muy indispensable en la precautelación del lugar a la que se encuentre asignada y de esta forma se transfiere internamente el voltaje de alimentación del Transformador a una batería de 7 Amperios/12Vcd, la misma que dura por un tiempo prudente (Aproximadamente 8 horas) y es la encargada de mantener en funcionamiento del sistema hasta que se restaure el corte de energía inicial, en este momento el sistema interno se encarga de recargar la batería

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.3 Fuente de Poder Suplementaria

6.2.4 Detector de Movimiento.- Es preciso instalarlo en las esquinas del área que se cubrirá, con el fin de que resguarde el mayor espacio físico posible de acuerdo con la foto. 6.4 y de esta manera no dejar puntos de fácil acceso para cualquier intruso, este dispositivo nos alerta de la presencia de intrusos en un área de (18mx12m) y 3m de altura, al encontrarse el personal encargado ausente, este dispositivo esta constituido por los siguientes componentes: Lente intercambiable: Lente de pared a pared (estándar), lente de cortina, lente inmune a las mascotas y lente de pasillo, Interruptor antisabotaje incorporado.

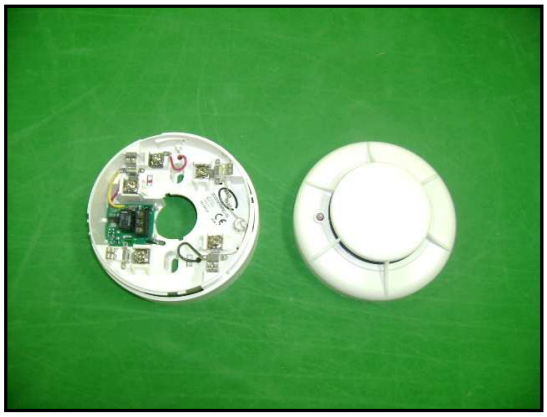


Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto. 6.4 Detector de Movimiento.

6.2.5 Detectores de Humo.- Es el equipo que se encuentra instalado en el centro y en la parte superior del área que se cubrirá, ya que en caso de existir una eventualidad de incendio el humo tiende a subir o dirigirse al centro de cualquier

lugar, mismos que proporcionan un tipo distinto de señal al de intrusión y por ende un sonido distinto en la sirena capas de poder alertar cuando hay un evento de incendio.



Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.5 Detector de Humo.

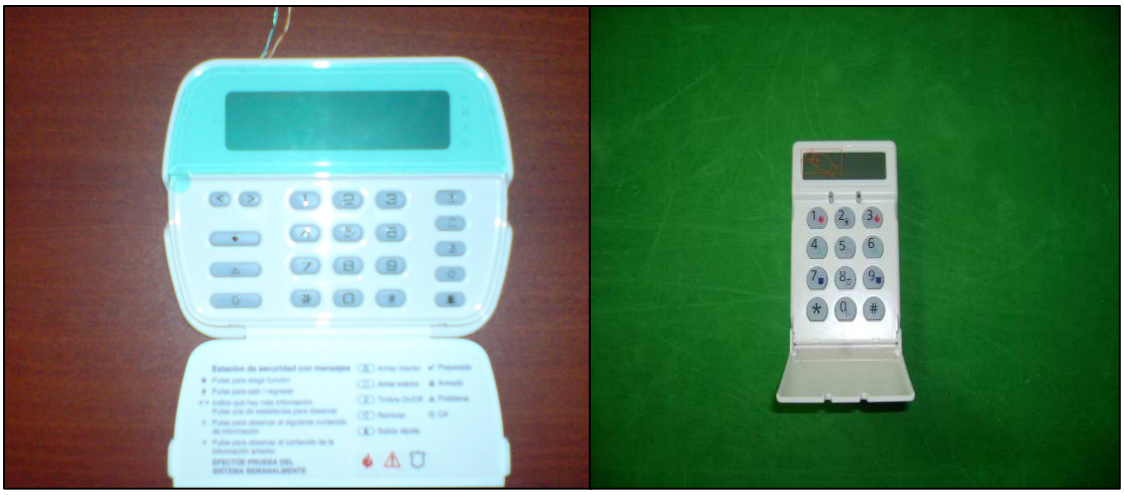
6.2.6 Contactos Magnéticos.- Se encuentran ubicados en las puertas de ingreso al departamento de Finanzas, su funcionamiento empieza cuando la puerta se abre luego de que el sistema se activa, momento en el cual emite un señal de alerta a la central de alarma.

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.6 Contactos Magnéticos.

6.2.7 Teclado Digital de Control.- Esta ubicado al ingreso del departamento de Finanzas y otro se encuentra en el laboratorio de audiovisuales, el mismo que ayudara al reconocimiento de donde sucede cualquier evento de robo o incendio de todo el sistema del área administrativa, mientras que el primero se encarga única y

exclusivamente del control del sistema en el departamento de finanzas.



Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.7 Teclado Digital De Control.

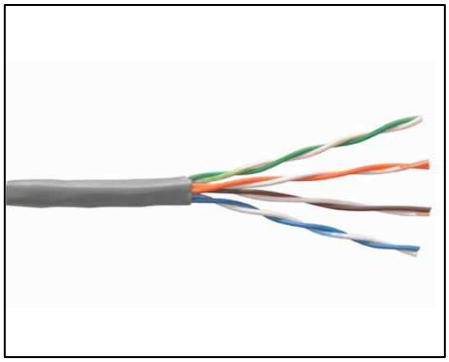
6.2.8 Sirena de 30 Wattios.- Se encuentra ubicada en la parte superior central del edificio, dirigido de forma que el sonido que genere se emita hacia la ciudad, básicamente es un dispositivo de comunicación entre el sistema y el medio exterior.

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.8 Sirena de 30 Wattios.

6.2.9 Cable UTP Cat. 5E.- se encuentran distribuidos en el techo y también por canaletas en el área administrativa, mismos que van desde la central de alarma en el departamento de sistema hasta los dispositivos (detectores de movimiento, humo,

contactos magnéticos, teclado y sirena) que se encuentran en el departamento de Finanzas.



Fuente: www.cableutp5E.com
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Fig. 6.1 Cable UTP Cat. 5E

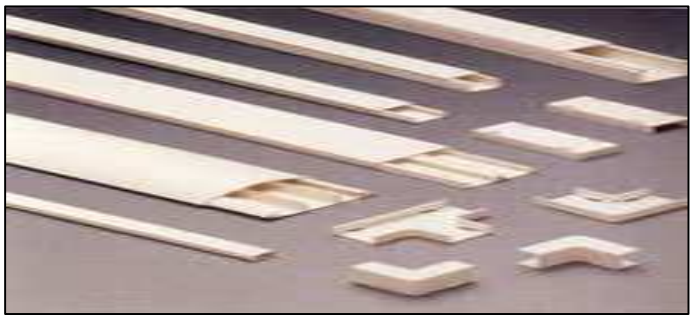
6.2.10 Herramientas Utilizadas.- Son necesarias para la instalación del sistema de seguridad, las cuales brindan facilidad en la colocación y conexión del los dispositivos, las mismas que son:

- ✓ Destornilladores (plano y estrella)
- ✓ Pinza Cortador
- ✓ Cautín
- ✓ Estaño
- ✓ Taladro
- ✓ Brocas
- ✓ Sierra de Metal
- ✓ Pistola de Silicón
- ✓ Barras de Silicón etc.
- ✓ Extensión.
- ✓ Cinta aislante.
- ✓ Estilete.

Fuente: Equipo utilizado en la implementación del sistema de seguridad.
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Foto 6.9 Herramientas Utilizadas.

6.2.11 Canaletas (10x25).- Son los materiales que utilizamos en lugares donde no era accesible el cableado a trabes del techo debido a la existencia de muros, también con lo cual evitaremos el deterioro o daño del mismo.



Fuente: www.canaletas.com
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Fig. 6.2 Canaletas.

6.3 Proceso de Implementación del Sistema de Seguridad.

En el proceso de implementación del sistema, es importante haber distribuido el tiempo de una forma correcta para lograr una optimización del mismo, así como también los recursos económicos y materiales, para lo cual se ha dividido en los siguientes pasos:

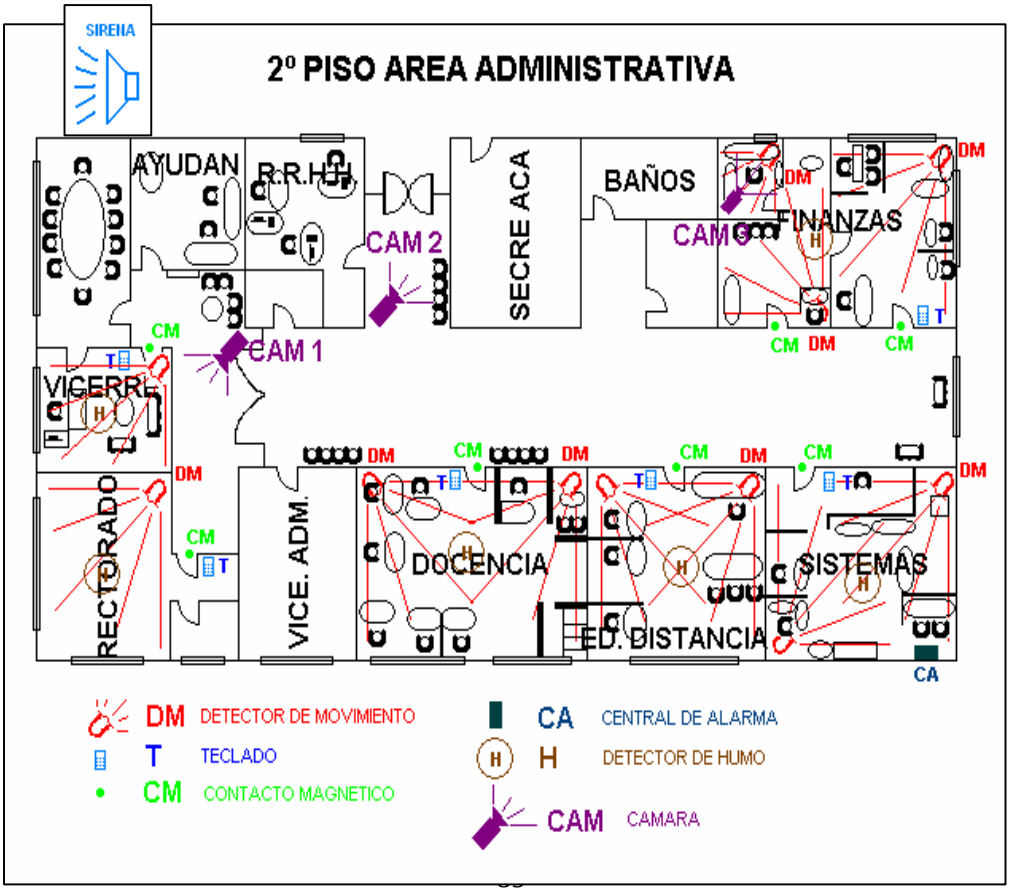
- ✓ Estudio del Plano de Instalación del Sistema de Seguridad Integrado y del Dep. de Finanzas.
- ✓ Cableado del Sistema.

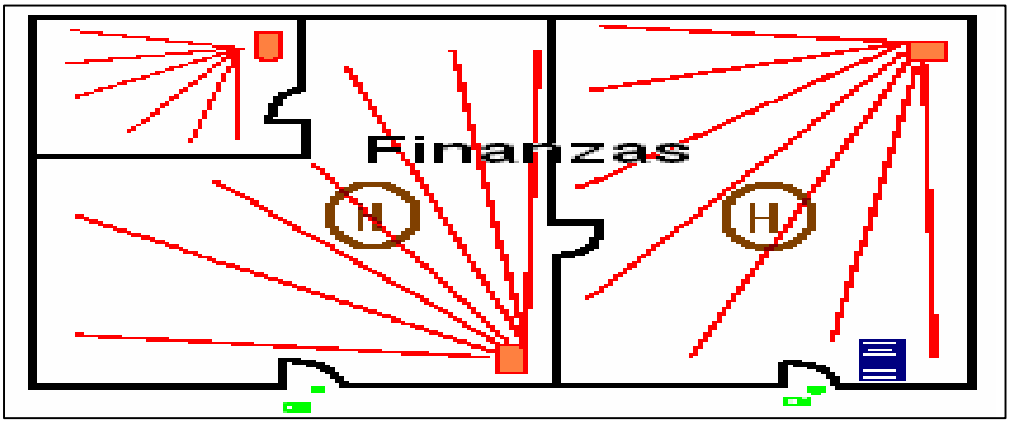
- ✓ Instalación y Conexión de los Equipos.
- ✓ Conexiones de la Central de Alarma.
- ✓ Rotulación del Panel Central.
- ✓ Prueba de Operatividad del Sistema

6.3.1 Estudio del Plano de Instalación del Sistema de Seguridad Integrado y del Dep. de Finanzas.

Este plano fue realizado para representar gráficamente el lugar estratégico de colocación del los dispositivos que conforman el sistema de seguridad para el área administrativa y el departamento de Finanzas.

También ayudo en el direccionamiento de a donde se debe dirigir el cable para conectar los detectores de movimiento, humo, contactos magnéticos, teclado y sirena, para de esta forma cumplir con un buen desempeño de este sistema de seguridad





Fuente: Plano de el sistema integrado y del departamento de Finanzas
Realizado por: Cbos. Téc. Avc. Puetate Rodrigo.

Fig. 6.3 Plano de Instalación del Sistema Integrado y Dep. Finanzas.

6.3.2 Cableado del Sistema.

Para el cableado se inicio primero levantando el cielo falso (techo) del área administrativa, en el transcurso del mismo que fue desde el departamento de sistemas, lugar donde se encuentra ubicada la central de alarma hacia el departamento de Finanzas, donde se instalarán los dispositivos del sistema, se evitó que los cables se enreden con los del sistema eléctrico o de Internet, en lugares de difícil acceso (columnas, paredes) se coloco canaletas para de esta manera evitar el uso excesivo de cable y la perdida de tiempo en perforaciones, como se puede observar en la (foto 6.10).

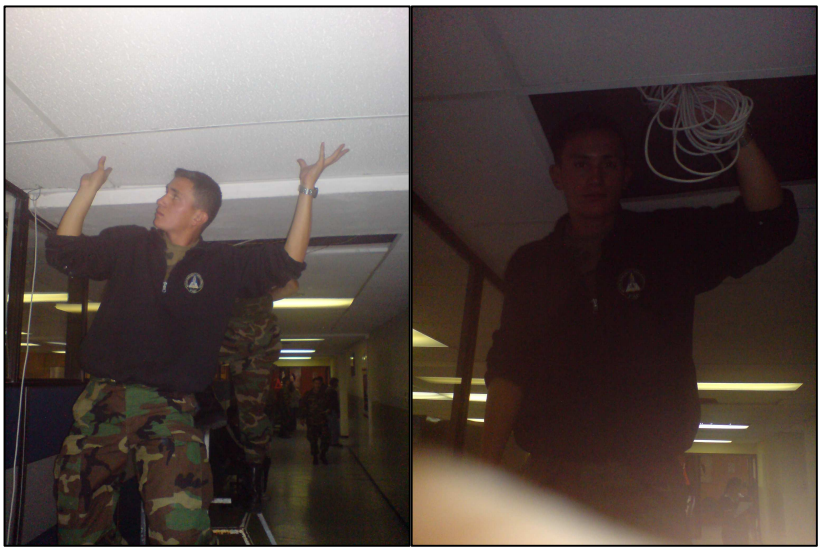


Foto 6.10 Cableado del Sistema.

6.3.3 Instalación y Conexión de los Equipos.

Primero con la ayuda del multímetro nos aseguramos de que los cables no estén rotos midiendo la continuidad, posteriormente con la ayuda de un destornillador y tornillos se procedió a instalar el detector de humo en el centro del techo del departamento de Finanzas, luego de lo cual se utilizó el taladro para alojar los detectores de movimiento en las esquinas del departamento, de la misma manera sucedió con los contactos magnético y teclado, tratando de no dañar los equipos y el cable para que el sistema funcione correctamente sin ningún tipo de inconveniente.

Foto. 6.11 Instalación y Conexión de los elementos

6.3.4 Conexiones de la Central de Alarma.

Una vez ya cableado e instalados todos los dispositivos que forman el sistema en puntos estratégicos, se procedió a realizar las conexiones de la central de alarma, poniendo en práctica las formas y normas de conexión que trae en los catálogos de estos sistemas, ver (Anexo M).

Foto. 6.12 Conexiones de la Central de Alarma.

6.3.5 Rotulación del Panel Central.

Los símbolos y conexiones que identifican a cada uno de los elementos con el módulo, son diseños de fábrica mediante un sistema computarizado con letras de color negro claramente impresas que se encuentra pegado en la tapa del gabinete # 1, con el fin de que el personal autorizado al mantenimiento o en caso de realizar cambios (previo estudio) pueda guiarse.

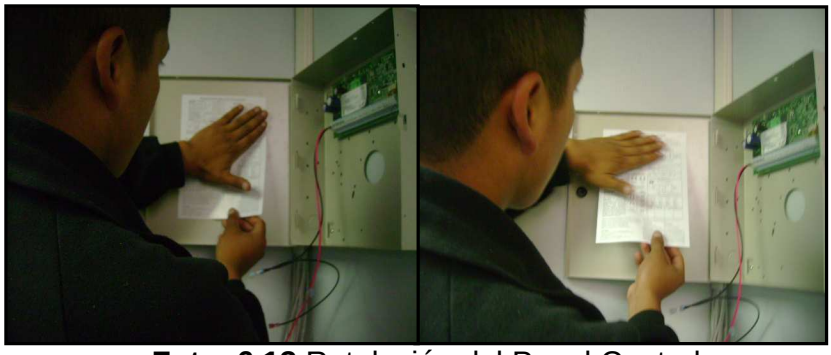


Foto. 6.13 Rotulación del Panel Central.

6.3.6 Prueba de operatividad del sistema.

Luego de haber llevado a cabo todos los procedimientos antes citados en la implementación del sistema, se procede a realizar la prueba de operatividad, mediante los siguientes pasos:

* Conectamos la central de alarma a la red de voltaje de 110 Vac.
* Verificamos que los dispositivos reciban la señal de alimentación.
* Comprobamos que todos los dispositivos estén trabajando según

la función que cumplan.

* Verificamos que el sistema funcione con la fuente de alimentación externa en caso de existir cortes de energía eléctrica.
* Verificamos que al momento de activar y desactivar el sistema de seguridad, no exista ningún inconveniente.
* Comprobamos que en caso de existir un intruso o incendio, la sirena emita los dos diferentes tipos de señal auditiva.

Foto. 6.14 Prueba de Operatividad del Sistema.

6.3.7 Manual del Usuario.

El presente manual contiene información acerca de la manipulación del sistema de seguridad electrónico, el cual facilitara la familiarización y mejor uso al personal que labora en el área administrativa del ITSA.

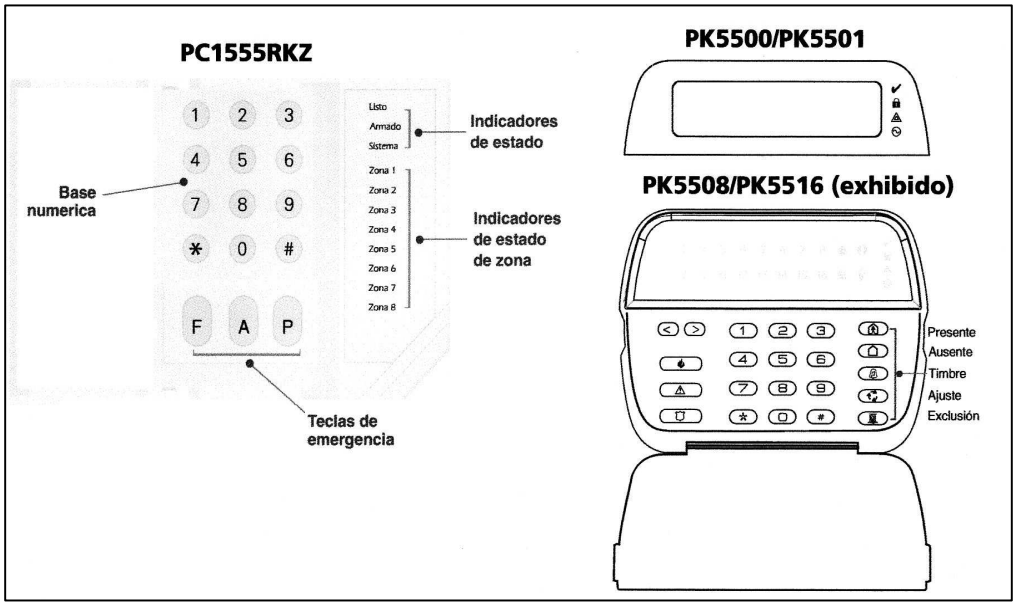


Fig. 6.4 Teclado PK5516

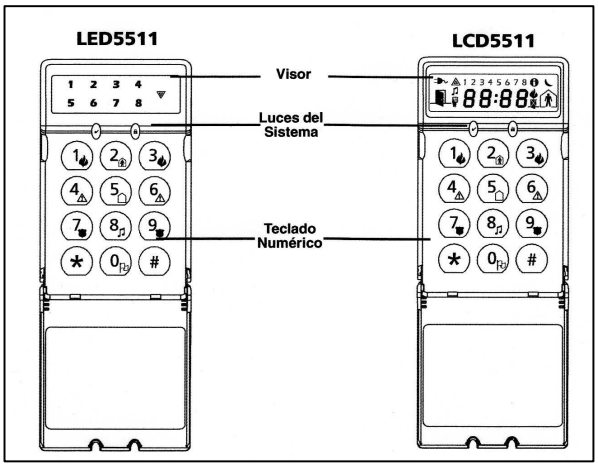


Fig. 6.5 Teclado LCD5511

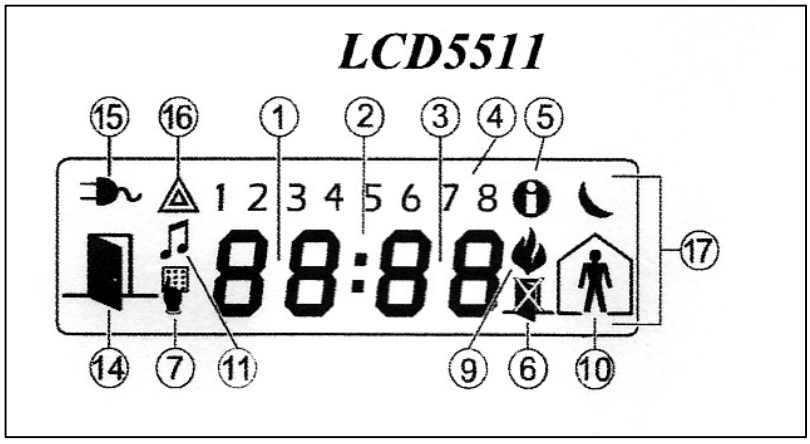


Fig. 6.6 Pantalla del teclado LCD 5511

1 **Dígitos 1,2 del Reloj.-** Estos dos dígitos del reloj de 7 segmentos indica los dígitos de la hora cuando el reloj local está activo e identifican las zonas cuando los íconos OPEN (abierto) o ALARM (alarma) estuvieren activos. Estos dígitos pasan en una zona por segundo, de la zona de número menor, a la de número mayor, cuando estuviese pasando por zonas.

2 **Dos Puntos (:).-** Este icono es el divisor de horas/minutos y se pondrá intermitente una vez por segundo cuando el reloj local estuviese activo.

3 **Dígitos 3,4 del Reloj.-** Estos dos indicadores de 7 segmentos representan los dígitos de los minutos, cuando el reloj local estuviese activo.

4 **1 a 8.-** Estos números identifican problemas.

5 **Memory (Memoria).-** Indica que hay alarmas en la memoria.

6 **Bypass (Inhibición).-** Indica que hay zonas inhibidas automática o manualmente.

7 **Program (Programación).-** Indica que el sistema está en la Programación del Instalador, o el teclado está ocupado.

9 **Fire (Incendio).-** Indica que hay alarmas de incendio en la memoria.

10 **Stay (Presente).-** Indica que el panel está armado en modo Stay. El se armará en el inicio del Retardo de Salida.

11 **Chime (Sonido de la Puerta).-** Este icono se enciende cuando la tecla de función Chime es oprimida para habilitar el Sonido de la Puerta en el sistema. El se apagará cuando la tecla de función chime sea oprimida nuevamente para deshabilitar el Sonido de la Puerta.

14 **Abierto.-** Este icono es utilizado en conjunto con los dígitos 1 y 2 del reloj para indicar zonas violadas (no en alarma) en el sistema. Cuando zonas están abiertas, el icono Abierto se encenderá, y los indicadores 1 y 2 de 7 segmentos pasarán por las zonas violadas.

15 **CA.-** Indica que corriente alterna está presente en el panel principal.

16 **Problema en el Sistema.-** Indica que un problema esta activo en el sistema.

17 **Noche.-** Indica que el panel está armado en Modo Nocturno.

18 **Armado del Sistema.-** Cierre todos los sensores (es decir, paré el movimiento y cierre las puertas). El indicador Ready deberá encenderse. Para armar, oprima su código de acceso, u oprima (*0) para armar rápidamente. Usted ahora tiene

30 segundos para salir del lugar. Para cancelar la secuencia de armar, inserte su código de acceso.

- **Error al Armar.-**Un aviso de error sonará si el sistema no pudiese armarse. Esto ocurrirá si el sistema no estuviese listo para armar(es decir, sensores están abiertos), o si un código de usuario incorrecto fue digitado. Si esto ocurre, certifíquese que todos los sensores estén cerrados, oprima (#) e intente nuevamente.

19 Desarmado del Sistema.- Ingrese su código de acceso para desarmar siempre que el sistema estuviere armado (es decir, el indicador de armado este encendido). El teclado sonará si usted atravesara la puerta de entrada.

- **Error al Desarmar.-** si su código estuviese invalido, el sistema no desarmara, y un aviso de error de 2 segundos sonará. Si esto ocurriere, oprima (#) e intente nuevamente.

20 Cuando la Alarma Suena.- El sistema puede generar dos (2) sonidos de alarma distintos:

- Sirena Continua = Intrusión (Alarma de Robo).
- Sirena Temporal/Pulsante= Alarma de Incendio.

21 Mantenimiento.

- No limpie el equipo de seguridad con paño mojado. Una limpieza ligera con un paño humedecido es suficiente para quitar la acumulación normal de polvo.
- Realice la prueba del sistema verificando las condiciones de la batería. Sin embargo se recomiendo que la batería de emergencia sea sustituida en un periodo de 3 a 5 años.

CAPITULO VII
CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES.-

* Después de haber realizado la investigación, se determinó que el actual sistema de seguridad del ITSA no ofrece condiciones adecuadas para que el personal se encuentre tranquilo en las diferentes áreas de trabajo.

* Para que exista un total control y seguridad dentro del ITSA, es necesario que se coloque un circuito cerrado de televisión en los pasillos del Instituto, biblioteca y el parqueadero; también un sistema de seguridad electrónico en los departamentos de sistemas, educación a distancia, docencia, recursos humanos, logístico, marketing, evaluación y control, audiovisuales, secretaria académica, auditorio, gimnasio, laboratorios, aulas taller y el bloque 42

* La recolección de información durante la investigación fue de gran importancia para la realización de este proyecto y permitió establecer los sistemas más adecuados que requiere la institución.

* Se determinó que la mejor opción es un sistema de seguridad electrónico, debido a que no son fácilmente saboteados o robados sus componentes y además estos no interfieren con el personal que labora en el departamento de Finanzas del ITSA.

* Luego de la implementación del sistema de seguridad electrónico en el departamento de Finanzas se pudo comprobar que brinda confianza y tranquilidad a quienes laboran en esta dependencia.

* El actual proyecto brindará todas las facilidades en cuanto a la manipulación y mantenimiento de este sistema ya que cuenta con guías de prueba y un manual del usuario.

7.2 RECOMENDACIONES.-

* Implementación de un circuito cerrado de televisión en los pasillos del Instituto, biblioteca y el parqueadero; también un sistema de seguridad electrónico en los departamentos de sistemas, educación a distancia, docencia, recursos humanos, logístico, marketing, evaluación y control, audiovisuales, secretaria académica, auditorio, gimnasio, laboratorios, aulas taller y el bloque 42 para que el instituto quede completamente seguro.
* Asignar personal que se encargue continua y estrictamente del control, monitoreo y mantenimiento del sistema de seguridad implantado.
* Verificación periódica para que los cables no sean cortados y que el sistema funcione óptimamente.
* Que se cambie la clave de seguridad periódicamente para que personas ajenas a este departamento no tenga acceso a esta dependencia.
* Cuidar que los sensores de movimiento y detectores de humo no sean saboteados.
* Que se capacite previamente al personal que va a ejercer las funciones de operador del sistema.
* Monitoreo permanentemente del sistema para precautelar su funcionamiento y duración.

GLOSARIO DE TÉRMINOS.

Los conceptos que se muestra a continuación han sido tomados de Microsoft Encarta.

Cibernéticos: Es el estudio del control y comunicación en los sistemas complejos: organismos vivos, máquinas y organizaciones.

Combustión: Es una reacción química en la que un elemento combustible se combina con otro comburente (generalmente oxígeno en forma de O_2 gaseoso).

Cracker: Es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Digital: La palabra Digital puede tener múltiples significados por ejemplo cualquier cosa relacionada con los dedos, señales digitales, circuitos digitales, etc.

Dispositivos: Se utiliza como sinónimo de aparato. En Informática, se utiliza para referirse a los componentes del ordenador. Además, es algo que establece una disposición.

Electromagnéticas: Las ondas electromagnéticas son ondas producidas por la oscilación o la aceleración de una carga eléctrica.

Electrónica: Es el campo de la ingeniería y de la física aplicada relativo al diseño y aplicación de dispositivos, por lo general circuitos electrónicos

Facsímil: Perfecta imitación o reproducción de una firma, de un escrito, de un dibujo, de un impreso, etc.

Fotoeléctricas: Es un dispositivo electrónico que permite transformar la energía luminosa (fotones) en energía eléctrica (electrones) mediante el efecto fotoeléctrico

Infiltraciones: Acción de introducir o introducirse un líquido por los poros o ranuras de un cuerpo sólido hacia su interior.

Informática: Es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales.

Infrarrojas: Es un tipo de luz que no podemos ver con nuestros ojos.

Interferencia: Alteración o perturbación del desarrollo normal de una cosa mediante la interposición de un obstáculo.

Las micro-ondas: Son ondas de radio de frecuencia muy elevada.

Oculares: Es un tipo de lente usada en instrumentos ópticos tales como microscopios y telescopios, que se antepone al ojo del observador para ampliar la imagen del objetivo que éste observa.

Password: Es sinónimo de 'palabra clave' porque en este concurso ante todo, se juega con las palabras y sus significados.

Radiofrecuencias: Es cualquiera de las frecuencias de las ondas electromagnéticas empleadas en la radiocomunicación.

Redes: Es la unión de dos constan de dos o más computadoras conectadas entre sí y permiten compartir recursos e información.

Sensores: Dispositivo formado por células sensibles que detecta variaciones en una magnitud física y las convierte en señales útiles para un sistema de medida o control.

Señales: Es un símbolo, un gesto u otro tipo de signo que informa o avisa de algo.

Sistema: Es un conjunto de elementos cuyas propiedades se interrelacionan e interactúan de forma armónica.

Sistemas biométricos: es un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada.

Software: Se refiere al equipamiento lógico o soporte lógico de un computador digital

Tensión: Es la fuerza interna que actúa por unidad de superficie.

Termograma: Conjunto de líneas que permiten identificar un plástico y su comportamiento con la temperatura.

Virus informáticos: Tienen, básicamente, la función de propagarse, no se replican a sí mismos por que no tienen esa facultad como el gusano informático

Abreviaturas

Volts/m: Voltios / metro

CCTV.- Circuito Cerrado de Televisión

PCs: Personal Communications Service (Servicio de Comunicación Personal).

PIN: Personal Identification Number (Numero de Identificación Personal).

VAF: Verificación automáticas de firmas.

VAC: Voltage Alternating Current (Voltaje de Corriente Alterna).

VCC: Voltage Direct Current (Voltaje de Corriente Continua).

ITSA: Instituto Tecnológico Superior Aeronáutico.

ECL: English Curse Language (Curso de Lenguaje Ingles).

ETFA: Escuela Técnica de la Fuerza Aérea.

EPAE: Escuela de Perfeccionamiento de Aerotécnicos.

BIBLIOGRAFÍA

- ✓ Batallas Lorena, Caillagua Gina y Gaucho Cristian, (2002) “Proyecto de Investigación” ITSA.
- ✓ Alno. Jarrín Urrutia, 2005, “Proyecto de Investigación” ITSA.
- ✓ http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- ✓ http://www.wikilearning.com/curso_gratis/seguridad_fisica_como-el_edificio_i/9707-4
- ✓ http://www.pcworld.com.ve/n57/articulos/competencia2.html
- ✓ http://www.segu-info.com.ar/
- ✓ http://es.wikipedia.org/wiki/seguridad_(concepto)
- ✓ Artículo 3º de la Ley general que establece las bases de coordinación del Sistema Nacional de Seguridad Pública
- ✓ http://www.eafit.edu.co/NR/rdonlyres/85EA1937-89BC-4C55-9BFA D396EB702C00/0/Boletin_27_Seguridad_Fisica.doc
- ✓ www.segu-info.com.ar/fisica/ergonometria.html
- ✓ http://es.wikipedia.org/wiki/biometr%c3%ada

Anexos

ANEXO A

REGLAMENTO DE SEGURIDAD INTERNA ITSA

TITULO I

GENERALIDADES

Art.1.- El Instituto Tecnológico Superior Aeronáutico (ITSA) es una Institución de carácter Particular cofinanciada dedicada a la Educación Superior reconocido por el CONESUP.

Art.2.- En vista de que una Institución como es el ITSA, debe tener reglamentaciones a fin de prever futuros inconvenientes legales con infracciones comunes, se ve en la necesario crea el presente Reglamento

TITULO II

DEL PERSONAL Y ESTUDIANTES

CAPITULO I

DEL PERSONAL DE PLANTA Y DOCENTES HORAS CLASE

Art.3.- El personal de planta será todos las personas que tenga una relación laboral con el Instituto.

Art.4.- Además el personal civil contratado y militar por la FAE designado al ITSA.

Art.5.- El personal destinado orgánicamente a la ETFA y EPAE militar o vil contrato o con nombramiento

Art.6.- Los Docentes hora clase que tenga legalizada esta relación por medio de un contrato de Servicios Profesionales.

CAPITULO II

DE LOS ESTUDIANTES

Art.7.- Son aquellos que este legalmente matriculado en las carreras y departamento de Idiomas y que asisten regularmente a los periodos académicos del ITSA, sean estos militares o civiles.

Art.8.- Existe estudiantes que no permanentes a este Instituto, como son los de los cursos especiales que existe en la Escuela de Perfeccionamiento de Aerotécnicos, que funciona en el tercer piso del edificio principal.

CAPITULO III
DE LOS VISITANTES

Art.9.- Son personas no permanentes que están de paso por el Instituto, y que ingresan al mismo a realizar tramites en cualquiera de las dependencias y departamentos sea del Instituto, de la Escuela de Perfeccionamiento de Aerotécnicos o la Escuela Técnica de la Fuerza Aérea

TITULO III

DE LAS MEDIDAS DE SEGURIDAD

CAPITULO I
DE LAS PERSONAS

Art.10.- Todo el personal Militar y Civil de planta deberá utilizar su identificación proporcionada por el Instituto.

Art.11.- Los docentes hora clase deberán utilizar la credencial que los acredite como tales.

Art.12.- Los estudiantes no permanentes de los curso de la ETFA o EPAE, tendrá la obligación de utilizar la credencial militar de Fuerzas Armadas mientras se encuentren en las Instalaciones del Instituto y mantenga la situación de estudiantes de esos cursos.

Art.13.- Los alumnos civiles y militares de las diferentes Tecnologías así como también del Departamento de Idiomas tiene la obligación de utilizar su carnet estudiantil, mientras se encuentre dentro de las Instalaciones de la Institución, caso contrario serán sancionado de acuerdo a lo que señala el Reglamento Interno.

Art.14.- El personal militar y civil de planta o no permanente que tenga vehiculo, deberán adquirir el estiquer de estacionamiento para poder ingresar con el mismo al Instituto.

Art.15.- Se mantendrán dos prevenciones una peatonal y una vehicular, el persona que no acatare las disposiciones del presente reglamento para su uso será sancionado por desacato.

CAPITULO II
DEL USO DE LAS INSTALACIONES

Art.16.- El personal militar y civil de planta estará dispuesto a lo que las autoridades del ITSA, ordenen respecto al cumplimiento de horarios y de guardias según el caso.

Art.17.- Los Estudiantes de las Tecnologías podrán hacer uso de todas las Instalaciones del Instituto desde las 07h00 hasta las 21h00 de lunes y viernes.

Art.18.- El fin de semana y los días feriados los alumnos civiles no podrán ingresar a las Instalaciones del Instituto, con excepción de que tenga recuperación de materias, las mismas que deberán ser autorizadas previamente por el Vicerrector Académico o Directores de Carreras.

Art.19.- Las Áreas verdes y canchas del Instituto podrá ser utilizadas fuera de los horarios establecidos previa autorización del señor Rector del Instituto.

Art.20.- Los estudiantes que viven el las villas del Instituto podrán ingresar a las mismas hasta las 23h00 de lunes a Viernes, el uso de estas instalaciones asignados a los estudiantes el fin de semana y días feriados deberán comunicar al Vicerrectorado Administrativo en el caso de que se queden en ellas.

Art.21.- Se prohíbe a los estudiantes que pagan vivienda al ITSA, realizar ninguna clase de algazaras o escándalo dentro de las villa a ellos asignada, en que caso de hacia hacerlo será sancionado y separado del uso de las villas.

Art.22.- Se prohíbe a los estudiantes que utilizan las villas del ITSA, el ingreso de personas ajenas a las misma, así como el de licor y sustancias psicotrópicas, en caso de incumplimiento será sancionado de acuerdo a lo que estipula el Reglamento Interno.

Anexo B

Latacunga, 24 de septiembre del 2008.

Señor.

Marco Benalcázar Bolaños.

Subt. Téc. Avc.

JEFE DPTO. RR.HH. ITSA.

Yo, Wilman Omar Ortiz Carrillo, portador del número de C.I: 050267468-2, egresado de la Carrera de Telemática, solicito se me haga la entrega del ORGANIGRAMA FUNCIONAL, NOMINAL Y ESTRUCTURAL del departamento de seguridad, además de los planes contra desastres, los cuales requiero para recopilar información en el proyecto de grado que me encuentro realizando.

Atentamente:

_____

A/C Wilman Omar Ortiz
CI: 050267468-2

Anexo C

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

Oficio No. 080234-EX-W (RR.HH.)-O.
Latacunga septiembre 25, 2008

Señor
William Ortiz Carrillo
ALUMNO ITSA
Presente

Asunto: *Ref. oficio S.N.*

De mi consideración:

Referente a su oficio S.N. del 25 de septiembre del 2008, con el presente comunico a usted señor Alumno, que no es posible facilitarle los documentos solicitados, en razón que se encuentran en proceso de elaboración, ya que el Departamento de Seguridad Aérea y Terrestre se está implementando actualmente.

Atentamente,
DIOS, PATRIA Y LIBERTAD,

Marco Benalcázar Bolaños
Sub/ Téc. Avc.
JEFE DPTO. RR.HH. ITSA

cc: Archi.

Elaborado por: Eng. Cadena A.
Supervisado por: Sgos. Tasiguano W.

Dirección: Campus Tecnológico Calle: Javier Espinosa Avenida Amazonas
Teléfonos: 9015089 / 9015093 Fax: 9011608 email: www.itsafaed@itsafas.edu.ec

Anexo D

FICHA DE OBSERVACION

OBJETIVO: Obtener información mediante la observación directa de los posibles sectores vulnerables a acciones que atenten con la seguridad en la planta baja del Instituto.

	HOJA DE INSPECCIÓN PLANTA BAJA.											
	TIPOS DE RIESGOS	FACTORES DE RIESGO	PUESTOS DE TRABAJO									TOTAL.
			Lab. Manto. Motores.	Lab. Instrumentación.	Audiovisuales.	Imprenta.	Aulas.	Lab. Sistemas Digitales.	Lab. Electrónica Básica.	Lab. Electricidad Básica.		
SEGURIDAD CONTRA DESASTRES.	ELÉCTRICOS.	Corriente Continua										
		Corriente Alterna 110V.										
		Corriente Alterna 220V.										
		Variación de Voltaje.										5
		Instalaciones.										
		Equipos.										
	FÍSICOS.	Ruido.										2
		Vibraciones.										
		Radiación.										2
		Temperatura.										
		Iluminación.										1
	DESASTRES	Incendios										8
		Movimientos telúricos.										
		Condiciones climatológicas.										2
SEGURIDAD FISICA.	SEGURIDAD.	Robo.										4
		Fraude.										
		Sabotaje										
		Control de Accesos.										4
	TOTAL		3	5	1	1	1	6	5	6		28

Anexo E

FICHA DE OBSERVACION

OBJETIVO: Obtener información mediante la observación directa de los posibles sectores vulnerables a acciones que atenten con la seguridad en el primer piso del Instituto.

	HOJA DE INSPECCIÓN PRIMER PISO.												
	TIPOS DE RIESGOS	FACTORES DE RIESGO	PUESTOS DE TRABAJO										TOTAL.
			Esc. de Idiomas.	Laboratorio Idiomas.	Biblioteca.	Papelería.	Cont. Transito Aéreo.	Salón Múltiple	Aulas.	Laboratorio Internet.	Laboratorio Redes.	Laboratorio Computación Básica	
SEGURIDAD CONTRA DESASTRES.	ELÉCTRICOS.	Corriente Continua											
		Corriente Alterna 110V.											
		Corriente Alterna 220V.											
		Variación de Voltaje.											4
		Instalaciones.											1
		Equipos.											1
	FÍSICOS.	Ruido.											1
		Vibraciones.											
		Radiación.											
		Temperatura.											
		Iluminación.											5
	DESASTRES.	Incendios.											10
		Movimientos telúricos.											
		Condiciones climatológicas.											
SEGURIDAD FISICA.	SEGURIDAD	Robo.											4
		Fraude.											1
		Sabotaje											2
		Control de Accesos.											4
	TOTAL		1	1	3	4	6	1	1	5	6	6	33

Anexo F

FICHA DE OBSERVACION

OBJETIVO: Obtener información mediante la observación directa de los posibles sectores vulnerables a acciones que atenten con la seguridad segundo piso del Instituto.

	HOJA DE INSPECCIÓN SEGUNDO PISO.														
	TIPOS DE RIESGOS	FACTORES DE RIESGO	PUESTOS DE TRABAJO												TOTAL.
			Aulas.	Recursos Humanos	Ayudantía	Sala de Sesiones	Vicerrectorado	Rectorado.	Carreras.	Educ. a distancia	Información.	Finanzas.	Coordinación y Control	Marketing.	Secretaria General y Procuraduría	
SEGURIDAD CONTRA DESASTRES.	ELÉCTRICOS.	Corriente Continua														1
		Corriente Alterna 110V.														1
		Corriente Alterna 220V.														
		Variación de Voltaje.														1
		Instalaciones.														
		Equipos.														
	FÍSICOS.	Ruido.														1
		Vibraciones.														
		Radiación.														
		Temperatura.														
		Iluminación.														1
	DESASTRE	Incendios.														13
		Movimientos sísmicos.														
		Condiciones climatolog.														
SEGURIDAD FISICA.	SEGURIDAD	Robo.														4
		Fraude.														
		Sabotaje														
		Control de Accesos.														9
	TOTAL		1	2	2	1	2	3	3	2	7	3	1	1	3	31

Anexo G

FICHA DE OBSERVACION

OBJETIVO: Obtener información mediante la observación directa de los posibles sectores vulnerables a acciones que atenten con la seguridad tercer piso del Instituto.

	HOJA DE INSPECCIÓN TERCER PISO.								
	TIPOS DE RIESGOS	FACTORES DE RIESGO	PUESTOS DE TRABAJO						TOTAL
			Aulas.	Laboratorio de Sistemas de Comunicación.	Oficinas ETFA.	Dirección ETFA.	Departamento AET.	Bodega	
SEGURIDAD CONTRA DESASTRES.	ELÉCTRICOS.	Corriente Continua							
		Corriente Alterna 110V.							
		Corriente Alterna 220V.							
		Variación de Voltaje.							**1**
		Instalaciones.							**1**
		Equipos.							**1**
	FÍSICOS.	Ruido.							
		Vibraciones.							
		Radiación.							
		Temperatura.							
		Iluminación.							**1**
	DESASTRE	Incendios.							**6**
		Movimientos sísmicos.							
		Condiciones climatológicas.							
SEGURIDAD FISICA.	SEGURIDAD	Robo.							**1**
		Fraude.							
		Sabotaje							
		Control de Accesos.							**1**
	TOTAL		**1**	**7**	**1**	**1**	**1**	**1**	**12**

Anexo H

FICHA DE OBSERVACION

OBJETIVO: Obtener información mediante la observación directa de los posibles sectores vulnerables a acciones que atenten con la seguridad los exteriores del Instituto.

	HOJA DE INSPECCIÓN EXTERIORES.															
			PUESTOS DE TRABAJO													
	TIPOS DE RIESGOS	FACTORES DE RIESGO	Canchas de basket.	Canchas de Vóley.	Canchas de Fútbol.	Villas Civiles.	Laboratorio Motores.	Laboratorio. Hidráulica.	Patio Marte.	Casino.	Peluquería.	Sastre.	Comedor.	Villas Militares.	Estacionamiento.	TOTAL.
SEGURIDAD CONTRA DESASTRES.	ELÉCTRICOS.	Corriente Continua														
		Corriente Alterna 110V.														
		Corriente Alterna 220V.														
		Variación de Voltaje.														
		Instalaciones.														
		Equipos.														
	FÍSICOS.	Ruido.														2
		Vibraciones.														
		Radiación.														
		Temperatura.														1
		Iluminación.														2
	DESASTRES.	Incendios.														13
		Movimientos sísmicos.														1
		Condiciones climatolog.														
SEGURIDAD FISICA.	SEGURIDAD.	Robo.														7
		Fraude.														
		Sabotaje														3
		Control de Accesos.														9
	TOTAL		1	1	1	4	6	5	2	2	3	3	4	3	3	38

Anexo I

PLANO PERIMETRAL DEL INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO.

Objetivo:

- ✓ Ubicar los puntos vulnerables de las areas que componen el instituto.

Fuente: Departamento Logistico del ITSA.

Modificado: Cbos. Téc. Avc. Puetate Ramirez Rodrigo Ivan.

Anexo J

INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO

CARRERA: Electrónica Mención Aviónica e Instrumentos.

ENCUESTA AL PERSONAL DEL ITSA

OBJETIVOS:

- Comprobar la necesidad real de un sistema de seguridad para el ITSA.

- Realizar el levantamiento de información parar determinar las necesidades especificas del ITSA en relación a su seguridad.

NOTA: Lea cuidadosamemente el contenido de este cuestionario y seleccione la respuesta que usted considere correcta.

PREGUNTAS:

1. ¿Conoce usted si en el Instituto existe algún tipo de sistema de seguridad?

   A.- SI

   B.- NO

2. ¿Durante el tiempo que usted viene trabajando en la Institución, conoce de pérdidas y robos suscitados?

   A.- SI

   B.- NO

   De qué tipo:……..

3. ¿En su área de trabajo han existido pérdidas o robos de objetos y/o materiales personales e Institucionales que se encuentran bajo su responsabilidad?

   A.- SI

   B.- NO

   De qué tipo?……

4. ¿Qué tipo de seguridad poseen las instalaciones donde usted trabaja actualmente?

   .....
   .....
   .....

5. ¿Considera usted que la infraestructura y los bienes materiales de la institución son más vulnerables con el crecimiento de la población estudiantil del ITSA?

   A.- SI
   B.- NO
   Porque?……

6. ¿Qué tipo de medidas de seguridad ha adoptado para evitar incidentes o pérdidas?

   ……
   ……
   ……

7. ¿Según su criterio que área, departamento, sección o laboratorio cree que es la vulnerable a robos, y explique por qué?

   ……
   ……
   ……

8. ¿Considera usted necesario la implementación de un sistema de seguridad que ayudaría de mejor manera a la vigilancia y desenvolvimiento de las labores que se realiza en la Institución?

   A.- SI
   B.- NO
   Porque?……

ANEXO K

INSTITUTO TECNOLÓGICO SUPERIOR AERONÁUTICO

CARRERA DE ELECTRONICA MENCIÓN INSTRUMENTACIÓN Y ÁVIONICA

ENTREVISTA DIRIGIDA

DATOS:

Lugar: Vicerrectorado Académico.

Fecha: 21-Febrero-2008.

Entrevistado: Subp. Padilla Milton.

Entrevistador: Sta. Puco María.

Tipo de Entrevista: cerrada

OBJETIVO:

- Obtener los antecedentes de los proyectos anteriores de la institución.

1. **¿Cuántos sistemas de seguridad fueron instalados en el ITSA?**
   ……
   ……
2. **¿Qué sistemas estaban instalados y que pasó con estos?**
   ……
   ……
3. **¿Desde cuándo ya no están en funcionamiento los sistemas de seguridad?**
   ……
   ……
4. **¿Por qué han dejado de funcionar los sistemas de seguridad?**
   ……
   ……

ANEXO L

INSTITUTO TECNOLOGICO SUPERIOR AERONAUTICO

CARRERA DE ELECTRONICA MENCIÓN INSTRUMENTACION Y AVIÓNICA

ENTREVISTA DIRIGIDA

DATOS:

Lugar:
Fecha:
Entrevistado:
Entrevistador:
Tipo de Entrevista:

OBJETIVO:

- Obtener los antecedentes de los proyectos anteriores de la institución.

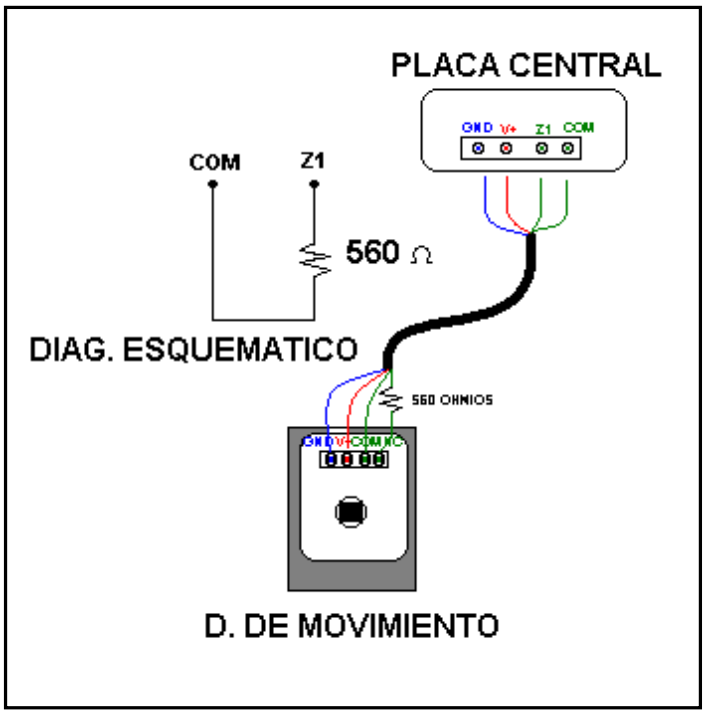
1. ¿Por qué dejaron de funcionar los sistemas de seguridad?

……
……
……
……

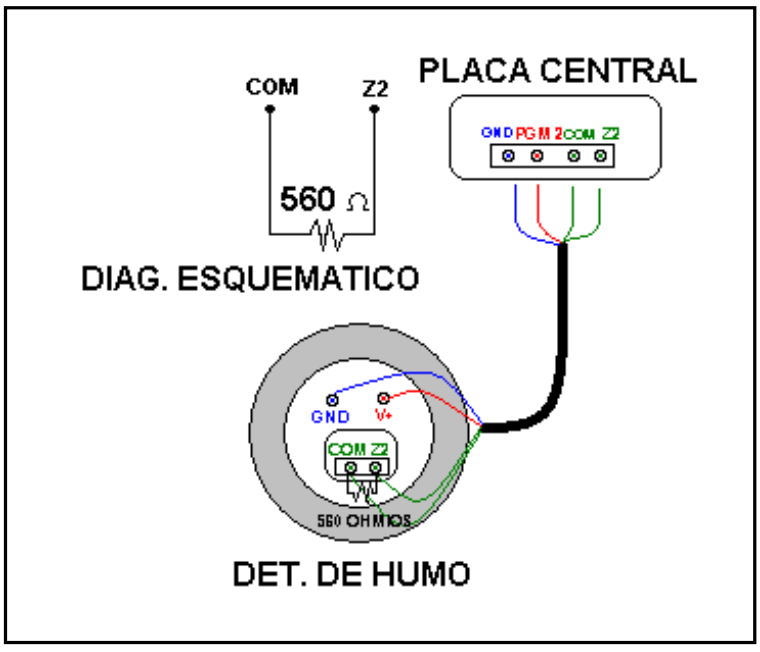
ANEXO M

Modo de conexión de los equipos

1. **Conexión de un detector de movimiento.**



2. **Conexión de un detector de humo.**



3. **Conexión de un teclado.**