Tecnificación de seguridad en las unidades militares

Andrés Gutierrez Giraldo
Hernando Trujillo Amaya

Trabajo de grado para optar al título profesional:
Curso de Estado Mayor (CEM)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2003

FUERZAS MILITARES DE COLOMBIA
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA.

TRABAJO DE FONDO

TECNIFICACION DE SEGURIDAD EN LAS UNIDADES MILITARES.

PARTICIPANTES
MY. ANDRES GUTIERREZ GIRALDO
MY. HERNANDO TRUJILLO AMAYA.

BOGOTA D C 29 DE SEPTIEMBRE DE 2.003.

AGRADECIMIENTO.

Los autores expresan sus agradecimientos a:

Todos los profesionales de **ESCUELA SUPERIOR DE GUERRA,** por todos los conocimientos trasmitidos a través del curso CEM 2.003.

INDICE.

RESPOSABLIDAD DE LOS INVESTIGADORES

El presente trabajo pretende ser una guía de referencia para mejorar la seguridad integral de las Unidades Militares. En efecto se pretende desde el punto de vista académico.

Para la elaboración se investigaron los textos que se relacionan, haciendo énfasis en las experiencias vividas por diferentes Unidades Militares.

NOTA DE ACEPTACION.

_____

_____

_____

_____

_____

_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Bogotá D C 29 de Septiembre de 2.003.

este título debe ir centrado.

INTRODUCCION

Realizando el curso de estado mayor, nace la inquietud de poner en practica los conocimientos adquiridos en la especialización en administración de la seguridad y es así, como en el presente trabajo de fuerza se expondrá a la institución la posibilidad de tecnificar las unidades militares y tratar de aplicar estos conocimientos a todas las unidades o por lo menos darles una luz de información en el nuevo mundo de la seguridad electrónica y técnica que a la postre será la única que tenemos que utilizar; en efecto, se perfila como la mas efectiva, además de ahorrarnos el uso de personal que debemos utilizar en otros sectores.

Es por esta razon que se dará a conocer algunos sistemas de seguridad técnica , además de algunas recomendaciones para adoptar medidas en las unidades militares ubicadas en las diferentes áreas de nuestra nación ;por lo anterior, se busca la aplicación del proyecto presentado, partiendo de un Objetivo General cual es intensificar e incrementar la seguridad física de las unidades militares, para evitar o contrarrestar cualquier acto terrorista, delincuencial y/o la penetración e infiltración a las instalaciones en general ; implementando entonces, los conocimientos específicos adquiridos en el programa académico cursado en la universidad militar y como resultado del trabajo en seguridad.

Por la misma cobertura del proyecto y por la clasificación secreta de los documentos utilizados, no se puede permitir observar todas y cada una de las fuentes utilizadas; sin embargo, se ha tratado de dejar entrever lo importante, necesario e inherente para las estrategias de Seguridad Física en unidades militares; igualmente, se observó lo trascendente en el desarrollo de un conflicto irregular como el que vive nuestro país; en consecuencia, Se espera que trabajo proporcione ideas generales de lo que se debe, realizar.

Maryeno

1. PLANTEAMIENTO DEL PROBLEMA

Los diferentes grupos armados al margen de la Ley que delinquen en Colombia se encuentran en forma permanente empeñados en generar una escalada terrorista de grandes proporciones en pro de urbanizar y profundizar el conflicto y de esta forma desestabilizar el país, obedeciendo al cumplimiento de sus planes estratégicos y centrando las acciones en la realización de actividades terroristas de resonancia, en las cuales se puede encontrar involucrada cualquier unidad militar de nuestro país. Por tal motivo el principal problema es la falta de sistemas tecnicos dentro del sistema de seguridad.

1.1. DESCRIPCIÓN DEL PROBLEMA y la formulación del Problema?

Dentro de los grupos armados al margen de la Ley, que realizan actividades delictivas y terroristas contra la legitimidad del Estado están:

- Las Autodefensas Unidas De Colombia.
- Las FARC.
- El ELN.
- Grupos de narcotraficantes.
- La delincuencia común y organizada

Siendo el objetivo principal desestabilizar el Estado en su estructura, acudiendo al ataque de sus instituciones, entre ellas, las que se encuentren involucradas en forma directa o indirecta con el conflicto mismo ; es previsible entonces, la disposición del enemigo para ejecutar actividades en contra de la seguridad de las unidades militares, entre las que se pueden concretar las siguientes amenazas (1) :

- ❖ Acciones armadas y atentados dinamiteros

- ❖ Ataque con armas de tiro parabólico

- Ataque aéreo
- Sabotaje a instalaciones y medios de comunicación
- Suplantación de personas
- Guerra electrónica e informática
- Ataque químico y/o bacteriológico
- Acción de francotiradores
- Ataque por redes subterráneas
- Atentados al alta mando durante desplazamientos
- Plan Pistoleo.

1.2. JUSTIFICACIÓN

Por lo anterior, se deben replantear y modificar las diferentes medidas de seguridad con que cuentan actualmente las instalaciones militares; en especial, la de contrarrestar el terrorismo que se vive no solamente en Colombia sino a nivel mundial.

Entre las actividades conducentes a minimizar factores de riesgo y actividades de vulnerabilidad (2), están:

- Falta de un sistema integrado de seguridad delas unidades militares.

- Necesidad de mejorar la observación física y electrónica de las áreas circundantes.
- Deficiente control de acceso a las instalaciones y autorización de ingreso mediante ficheros.
- Deficiente organización de dependencias, desde la óptica de la seguridad.
- Falta de capacidad de defensa aérea.
- Falta de un sistema unificado de comunicaciones internas
- Deficiente iluminación y control de áreas perimétricas
- Ineficaz control en los sitios de acceso y corredores de tránsito
- Insuficientes mecanismos de detección electrónica
- Barreras perimétricas deficientes
- Inadecuado control de rutinas obligatorias
- Proliferación de proveedores en áreas no autorizadas y vendedores ambulantes desconocidos en la periferia.
- Rutina en los procedimientos de la seguridad
- Alta rotación del personal responsable de la seguridad
- Falta de evaluación periódica de los procedimientos de selección, enganche.

- Evaluación del personal civil.

- Carencia de contramedidas para proteger la red de comunicaciones y de sistemas.

- Falta de información, medios y capacidad para contrarrestar la acción de terrorismo químico y bacteriológico.

1.2.1. INTERES

La intensificación del conflicto y en especial el incremento de la guerra terrorista, hace necesario la protección tecnificada de las instalaciones militares con el fin de negarle al enemigo la posibilidad de un golpe de opinión ; igualmente, al daño que se pueda ocasionar a nuestros hombres ,instalaciones y equipos.

1.2.2. UTILIDAD

El presente trabajo no solamente es de beneficio para las unidades militares, si no que puede servir en las diferentes instalaciones policiales; de manera similar ,en instalaciones que albergan los diferentes organismos de seguridad del estado.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Modernizar e incrementar la seguridad física en las unidades militares; con el fin, de evitar o contrarrestar cualquier acto terrorista, delincuencial y/o la penetración e infiltración a las instalaciones militares, por parte de integrantes de cualquier Grupo Generador de Violencia.

1.3.2. OBJETIVOS ESPECIFICOS

1. Proveer a las instalaciones militares, de un sistema de seguridad inteligente e integral, con tecnología de punta capaz de garantizar un alto nivel de seguridad.

2. Implementar un sistema de seguridad que integre los diversos equipos y medios de detección, control y comunicaciones ; de tal manera, que se cree una metodología automática que interactúe, alerte y registre oportunamente los eventos rutinarios y de especial suceso en la actividad.

3. Verificar los recursos y mecanismos para actualizar la tecnología de los diferentes medios de seguridad con que cuenta algunas instalaciones militares.

2. ANTECEDENTES

2.1. ANTECEDENTES HISTORICOS

Las Fuerzas Militares de Colombia, se han establecido como una organización sólida, estructurada y altamente capacitada para conducir con eficacia operaciones conjuntas prolongadas en cualquier parte del territorio nacional, tendientes a mantener la soberanía, la independencia, la vigencia de la Constitución, el ejercicio de la ley, el funcionamiento de las instituciones y garantizar la protección de la población y sus recursos ; así como, para participar con fuerzas de otros países en operaciones combinadas de mantenimiento de paz internacional.

El artículo 120 de la Constitución Política de 1886, posteriormente la de 1991, da al Presidente de la República la atribución de dirigir, cuando lo estime conveniente, las operaciones de guerra , supremo de la fuerza publica ; igualmente, la Ley 102 de 1944

fijó al entonces Jefe de Estado Mayor las funciones de órgano de mando del Gobierno, haciéndolo virtualmente un Comandante General, ya que centralizaba en este cargo las funciones del mando de las Fuerzas Militares; posteriormente, el Decreto 835 del 16 de abril de 1951, creó el cargo de Comandante General, asignando las funciones que se habían dado al Jefe de Estado Mayor.

El Comandante General de las Fuerzas Militares será un Oficial General o de Insignia, en servicio activo, nombrado por el Gobierno Nacional, responsable de la instrucción, educación, disciplina, conducta, empleo, conducción y administración de las Fuerzas Militares.

De otra parte, los grupos armados al margen de la Ley se encuentran empeñados en generar una escalada terrorista de grandes proporciones en pro de urbanizar el conflicto, en cumplimiento de sus planes estratégicos; por lo cual, se deduce que dentro de sus propósitos contemplen la realización de una acción terrorista de resonancia, en la que se encuentre involucrado el total de las instalaciones militares.

El rompimiento del Proceso de Paz, la captura de varios miembros de las milicias urbanas y el decomiso de gran cantidad de insumos para la elaboración de artefactos explosivos en diferentes ciudades del país, reflejan el pensamiento e intención del grupo delictivo, especialmente en la capital de la República.

La seguridad de las unidades militares presentan deficiencias que son indispensables corregir. Ellas se pueden concretar en los siguientes aspectos:

- Falta de planeamiento conjunto, dirección unificada y coordinación para la acción integrada entre los elementos de seguridad de las diferentes unidades militares y de policía.

- No hay unidad organizacional ni dispositivo para prevenir o repeler la acción subversiva, las unidades militares y de policía deberían tener una base de datos de todo el personal que labora en las instituciones con el fin de evitar suplantaciones como ha sucedido en muchas unidades.

- La estructura de las dependencias encargadas de la seguridad en las unidades es débil en su estructura física y técnica para disuadir la acción enemiga, no hay en las unidades un control de acceso que permita utilizar tarjetas inteligentes y controlar el ingreso y la permanencia de los visitantes en las unidades encontrándose personal en dependencias que no le son permitidas .

- La seguridad está encaminada fundamentalmente a la seguridad de personalidades y no a la seguridad integral de las unidades.

- Ausencia de coordinación efectiva y normas para la acción integrada entre los planes de seguridad de las unidades de policía, Fuerzas Militares y organismos de seguridad del estado que se encuentran en un área especifica.

- Las unidades no cuentan con censores de movimiento en los muros o mayas ; igualmente, cámaras que sirvan de alerta temprana, permitiendo tanto la entrada como la salida de personal por esos sectores, convirtiéndose en una vulnerabilidad.

- La penetración de algunos miembros activos de las instituciones militares ha permitido el saboteo, el robo de material y los ataques terroristas en las unidades.

- Muchas unidades han recibido durante su existencia varios actos que atentan contra su seguridad física e interna, así como del personal operativo en servicio activo y administrativo del mismo con la finalidad de desestabilizar la institucionalidad y credibilidad del mando general de las Fuerzas Militares; entre los cuales, se encuentran los siguientes ejemplos:

- En 1979 se robaron gran cantidad de fusiles Del Cantón Norte con la construcción de un túnel.

- El intento de toma Al Batallón De Ingenieros Cisneros en la ciudad de Armenia en 1985.

- El lanzamientos de morteros causando gran cantidad de bajas en El Batallón Magdalena En Pitalito En El Año 2001.

- En el 2002 se robaron 02 fusiles de la guardia del batallón M A C suplantando militares.

- 19 de octubre de 1987, un vehículo cargado de dinamita, hizo explosión en el parqueadero de la instalación del comando general de las FFMM., siete personas resultaron lesionadas, dieciséis vehículos semidestruidos y numerosos daños materiales en la edificación.

- En el mes de febrero de 1996 se encontraron seis morteros hechizos emplazados en la zona verde del costado sur del Ministerio de Defensa.

Por lo anterior surge la inquietud por parte de dos alumnos de La Escuela Superior De Guerra, de efectuar la actualización y mejoramiento de la Infraestructura física y logística de las unidades militares, como garantía de su funcionamiento en época de paz y en época de perturbación del Orden y la Seguridad Pública, cuya esencia se fundamenta en la formulación, desarrollo y evaluación de un Proyecto de Mejoramiento de Seguridad a las instalaciones con suficiente soporte presupuestal para su implementación.

Los diferentes grupos armados al margen de la Ley que delinquen en Colombia, se encuentran en forma permanente empeñados en generar una escalada terrorista de grandes proporciones en pro de urbanizar y profundizar el conflicto ; lo anterior, en cumplimiento de sus planes estratégicos; por lo cual, se deduce que dentro de sus propósitos contemplen la realización de una acción terrorista de resonancia, en la que se encuentre involucrada cualquier unidad militar.

3. NOCIONES GENERALES

3.1. CONCEPTOS GENERALES

3.1.1 SEGURIDAD

Referencias Bibliográficas

Proviene del Latín Securitas que a su vez se deriva del adjetivo securus, el cual está compuesto por sé, sin y cura, cuidado o procuración, lo que significa sin temor, despreocupado o sin temor a preocuparse.

3.1.2 SEGURIDAD NACIONAL

Es un concepto que ofrece dificultades para definirlo, por lo que cada Estado lo establece en función de las realidades que observa en su desarrollo político, económico, social y militar.

Referencia Bibliográfica

La Seguridad Nacional se generó con la aparición de los primeros grupos humanos, es posible afirmar que nació como una necesidad del ser humano para protegerlo de los peligros provenientes de su relación con el medio ambiente y la sociedad. Entonces, podemos señalar que este fenómeno es el conjunto de acciones hechas por los integrantes de un Estado para obtener y conservar las circunstancias propicias para el logro de su proyecto nacional.

Tomando la definición etimológica, Norberto Bobbio indica que "el fin del Estado solamente es la Seguridad entendida como la certeza de la libertad en el ámbito de la Ley" (3).

Para el Comando Conjunto de las Fuerzas Armadas de los Estados Unidos de América (U.S. CHIEFS OF STAFF). "La seguridad nacional es la condición que resulta del establecimiento y manutención de medidas de protección, que aseguren un estado de inviolabilidad contra actos o influencias antagónicas" (4).

Para la Escuela Superior de Guerra del Brasil, "La seguridad Nacional es el grado relativo de garantía que a través de acciones políticas, económicas, sicosociales y militares que un estado puede proporcionar en una época determinada, a la nación ; con el fin, de garantizar la consecución y salvaguardia de sus objetivos nacionales a despecho de los antagonismos existentes". (5).

Si no acaba el capitulo no tiene por que existir este espacio.

(3) NORBERTO BOBBIO. Liberalismo y democracia. México, F.C.E. Página 26

(4) CO. ALFONSO LITUMA ARIZAGA, Doctrina de Seguridad Nacional. Caracas, Venezuela 1967, Página43

(5) CO. ALFONSO LITUMA ARIZAGA, Doctrina de Seguridad Nacional. Caracas, Venezuela 1967, Página41

El Coronel Alejandro Medina Solís señala en su obra la Doctrina de la Seguridad Nacional ,que ésta se define como "la capacidad del Estado para garantizar su supervivencia, manteniendo su soberanía e independencia material y espiritual, preservando su forma de vida y posibilitando el logro de sus objetivos fundamentales.. " (6)

De este inicio se infieren puntos básicos, de los cuales parten rasgos esenciales que limitan el concepto de la Seguridad Nacional, entre los más destacados tenemos:

- Es una condición política, económica, social y militar
- Se manifiesta como proceso continuo e incesante
- Tiene una dinámica propia
- Es una función estatal
- Nace con la organización del Estado
- Se manifiesta en el pleno ejercicio de la soberanía e independencia
- Su meta básica es la consecución de los objetivos nacionales
- Presenta un estado de garantía
- Capacidad de conservación y supervivencia que posee cada estado

(6)Tomado del compendio de lecturas requeridas, material de seguridad Nacional, Colegio Defensa Nacional Pag. 46

- Se manifiesta en acciones en los cuatro campos del poder nacional
- Busca la estabilidad y consecución de los objetivos nacionales
- Está dirigida a superar los problemas nacionales

NORMATIVIDAD DE SEGURIDAD

Como base de la doctrina de seguridad, las normas emitidas se aplicarán en todas las Instituciones Militares, de manera obligatoria y permanente para :

a. Proteger :

1) La información contra el espionaje.
2) El personal contra la subversión.
3) Las instalaciones y material contra el sabotaje.
4) Las comunicaciones criptográficas contra la acción e interceptación de un posible adversario.

b. Funciones particulares de la Sección de Seguridad Militar, de acuerdo al manual de contrainteligencia para las fuerzas militares

1) Recomienda, ejecuta y adecua los planes existentes y/o necesarios para preservar la seguridad de personas, documentos, información, comunicaciones, electrónica y física, que requiere la Unidad.

2) Atiende lo referente a la instrucción y entrenamiento de seguridad militar.

3) Elabora y mantiene actualizados los Estudios de Seguridad de Personal (E.S.P.).

4) Adelanta Comprobaciones de Lealtad.

5) Ejecuta los procedimientos establecidos para garantizar la seguridad de los documentos y la información clasificada.

6) Adelanta Estudios e inspecciones de seguridad física y técnica.

7) Adelanta pruebas de vulnerabilidad.

8) Ejecuta programas de seguridad para las comunicaciones electrónicas.

9) Propone la designación del personal custodia en cada una de las dependencias de la Unidad, verifica periódicamente el cumplimiento de sus funciones.

10) Ordena la elaboración del plan del buen vecino al personal que habita los alrededores de la Unidad o Instalación Militar.

11) Elaborar las autorizaciones para el manejo de documentación clasificada al personal de las diferentes secciones o dependencias que así lo ameriten.

12) Verifica diariamente que la documentación clasificada llegada o salida sea radicada en un libro destinado para el efecto y que ésta sea empacada en doble sobre y esté correctamente clasificada.

13) Controlar el acceso o empleo de los sellos de clasificación.

14) Constatar el empleo de las canecas de seguridad o picadores de papel en las diferentes dependencias, para los borradores y copias de documentos clasificados, así como su posterior incineración.

15) Verificar en las oficinas el empleo de los archivadores seguros con chapas y candados de buena calidad, así como el empleo de carátulas de seguridad para cubrir documentos en los escritorios que se encuentren en tramitación.

16) Supervisar la reproducción (fotocopias, grabación, reimpresión, etc) de los documentos clasificados y establecer responsabilidad a quienes se les hayan suministrado, llevando un libro Control de Reproducción de Documentos Clasificados.

17) Con el Comité de Seguridad debe supervisar que la clasificación asignada a un documento corresponda al contenido del mismo.

18) Elabora los conceptos de confiabilidad.

19) Elaborar ficheros del personal de la Unidad, para su identificación interna.

20) Verificar que el manejo de documentación cifrada tenga el tratamiento de seguridad que corresponde de igual forma su procesamiento, difusión y archivo(7).

Los valores que regentan la institución se definen como un conjunto de creencias básicas que dan calidad y autordenamiento; igualmente, son fundamentos para la transformación, que orientan el comportamiento y compromiso de los militares y personal no uniformado con algo superior a ellos mismos; manteniendo entonces, los limites aceptables del cambio mostrando aquello que no debe cambiar por ser la esencia de la organización. Entre ellos, se encuentran:

- HONESTIDAD.- En la forma de dar, hablar y realizar las criticas, y el uso de la autoridad y la moral.

- VALOR.- Para cumplir con las tareas y misiones; enfrentar los desafíos y los retos permanentes.
- LEALTAD.- Con la patria, con los ciudadanos, con la institución, con los superiores y con los subalternos.

- COMPETENCIA PROFESIONAL.- Profesionalismo y dedicación en las misiones y tareas asignadas; permitir elevar el desempeño y la obtención de resultados efectivos; liderar a través de la aplicación de conceptos gerenciales y de comandos modernos.

Como Objetivos Estratégicos, la institución determina:

1. Fortalecer la capacidad operacional de las Fuerzas Militares a través de su reestructuración y modernización.
2. Debilitar militarmente los grupos al margen de la ley para llevarlos a aceptar el plan de paz del Gobierno.
3. Debilitar la infraestructura logística y de apoyo económico de los grupos al margen de la ley.
4. Contribuir a la protección de la población civil y sus recursos.
5. Mantener una efectiva capacidad de disuasión tendiente a defender la soberanía e integridad territorial.

4. PLANTEAMIENTO DE UN NUEVO MODELO DE SEGURIDAD DE LAS UNIDADES MILITARES

4.1. ASPECTOS GENERALES.

4.1.1. SEGURIDAD FÍSICA

El concepto de Seguridad Física está determinado como la base fundamental para proteger personas, bienes, valores, documentos, maquinaria, equipos y materias primas mediante una buena vigilancia sobre amenazas y riesgos.

Comprende unas acciones a realizar contempladas en:

1. PLANEAMIENTO.- Que contiene los siguientes interrogantes:

- RIESGOS.- QUÉ
- VULNERABILIDAD.- DÓNDE
- PUNTOS CRITICOS.- DÓNDE
- MEDIOS DISPONIBLES.- CON QUÉ
- CONCLUSIONES.- QUÉ HACER
- RECOMENDACIONES.- CÓMO

Los interrogantes resueltos son plasmados en un Plan de Acción que determina Planes de Seguridad que responde a las preguntas de Cómo y los Programas de Seguridad, que se refieren a Cuándo.

2. ADIESTRAMIENTO.- Es vivir la situación y con mentalidad preventiva, preparar a sus integrantes. Está compuesto por los siguientes elementos:

- Información permanente de la situación
- Funciones a cumplir (Manejo de armas – equipos)
- Ensayos sobre hipótesis

3. EQUIPAMIENTO.- Es el material necesario de cualquier tipo. Su aplicación incide en la seguridad de la empresa. Se compone de:

- FASE ACTIVA – REACTIVA. Es el momento de desencadenar la acción de respuesta ante el intruso.
- FASE CORRECTIVA.- Es, una vez ocurrida, el estudio de aquellas medidas necesarias tendientes a reparar los daños, corregir errores, responder a los cambios,

métodos que debe emplear y sistemas a revaluar. En esta se incluye la investigación del hecho.

4.1.1.1. PILARES DE LA SEGURIDAD FÍSICA.-

La Seguridad Física se sustenta en tres pilares fundamentales:

1. LA PROTECCION

Está constituida por una barrera que separe al delincuente del objetivo de su delito, impidiendo la producción del daño o disuadiéndolo de causarlo. Esas barreras pueden ser tangibles e intangibles. Hacen parte de lo tangible, los vigilantes, escoltas, los grupos de reacción o el apoyo que pueda dar la fuerza publica, en cuanto tienen la capacidad coercitiva para reprimir el delito. También hacen parte de lo tangible los muros, las puertas, las rejas, candados, cercas, verjas, techos, cajas fuertes, bóvedas, sistemas de apertura eléctricos y electrónicos o cualquier otro elemento que dificulte o impida el acceso del delincuente hasta el sitio donde están las personas, los valores o el patrimonio que desea proteger.

Son barreras Intangibles los recursos abstractos que disuaden al delincuente de cometer el delito, como los buenos planes de seguridad, el nivel de entrenamiento del cuerpo de vigilancia, el estado de alerta de la empresa, la proximidad de la fuerza pública de apoyo o la lealtad de los empleados que dificulta la infiltración.

2. LA VIGILANCIA.

Es la capacidad de detectar la proximidad del riesgo con tiempo suficiente para producir una reacción que pueda evitar el daño. La vigilancia implica el uso de personas, sistemas eléctricos o animales que dan aviso cuando se aproxima el peligro.

Los vigilantes y escoltas son al mismo tiempo vigilancia y protección porque pueden detectar el peligro y actuar para evitar el daño.

3. EL CONTROL.

Para garantizar que la vigilancia mantenga su capacidad de alerta y protección e igualmente su capacidad para evitar el daño o disuadir al delincuente ; por lo tanto, resulta necesario ejercer una acción permanente que permita tener la certeza de que siempre se estará en condiciones de actuar adecuadamente frente al riesgo. Esa acción se denomina control.

4.1.1.2. ENEMIGOS DE LA SEGURIDAD FISICA

En forma general, son tres los enemigos de la Seguridad Física:

A. LA SUBVERSION

Está constituida por organismos de presión con una filosofía supuestamente política, que luchan casi siempre clandestinamente contra el régimen político imperante en un Estado. En los países del sistema capitalista democrático, la subversión es de extrema izquierda y actúan contra la paz de una nación haciendo ataques a organismos, instituciones militares o de policía, cuarteles, empresas ; igualmente, a personas de la política contraria a la de sus aspiraciones.

B. LA DELINCUENCIA

Otro enemigo es la Delincuencia, que se caracteriza porque tiene como fin último de su actividad delictiva, el lucro personal o la satisfacción de sentimientos infames como la venganza o la envidia; pasiones estas, que pueden haber nacido en el desarrollo de una incipiente actividad anterior. La delincuencia cuando crece o se vuelve poderosa,

como en el caso del narcotráfico, puede llegar a tomar posición política contra los Gobiernos. Se diferencia de la subversión en el ánimo de lucro personal o del grupo que los impulsa.

C. LA PENETRACIÓN.

La penetración es quizás la actual amenaza mas grande de las instalaciones militares, consiste en efectuar por medios coercitivos, económicos e ideológicos influencia ante un miembro de la institución con el fin que este produzca un daño en la unidad, el material o el personal.

4.1.1.3. RIESGOS DE LA SEGURIDAD FISICA

Los enemigos de la Seguridad Física generan daño ejerciendo acciones en contra de sus componentes, es decir, contra los individuos a su servicio, su patrimonio y su imagen. Cuando el daño está en estado potencial, se denomina RIESGO, y entre los más importantes están:

1.Contra las personas individualmente consideradas.

Atentado: Es una acción violenta para causar muerte o daño físico.

Secuestro: Es privar a una persona de la libertad, para canjear esa libertad por dinero o toma de decisiones bajo amenazas generalmente de muerte o daño en la persona extorsionada o en alguien cercano a sus efectos o intereses.

Hostigamiento: Persecución continuada a una persona para causar angustia, stress, miedo y aún desesperación con miras a minar la fortaleza moral del individuo.

2.Contra las personas en grupo.

Infiltración: Es el hecho de lograr que personal subversivo o ligado a la delincuencia común o a la competencia desleal, trabaje legalmente en la entidad para causarle daño desde adentro. La infiltración acompañada de otra acción que causa el daño como atentado, el secuestro, el sabotaje y el robo material o documentos clasificados.

Adoctrinamiento Subversivo: Es el que procura ganar para la causa política subversiva a trabajadores o funcionarios, y luego, con apoyo así conquistado, minar las capacidades de la entidad mediante solicitud de exigencias exageradas, impulso a huelgas o paros, en busca justamente de la desestabilización del orden interno de la misma.

Hostigamiento: Igual que el individual, pero manejando grupo de trabajadores o funcionarios, basado en amenazas o reuniones mal intencionadas.

Terrorismo: Son ataques de cualquier tipo que no solamente buscan destruir vidas y patrimonio, sino también, y a menudo especialmente, causan pánico y el desmejoramiento moral de la entidad. El riesgo es tanto para personas como para el patrimonio.

3.Contra las instalaciones y patrimonio.

Sabotaje: Consiste en interrumpir ciclos de producción de bienes y servicios dañando materias primas, mecánicas, maquinaria o instalaciones. También se hace mediante operaciones lentas o huelgas o paros para disminuir o parar la producción o la prestación del servicio. Puede causar pérdidas de vidas y lesiones físicas o morales

Hurto: Es el más frecuente de los riesgos. Se puede realizar mediante engaño o mediante el uso de fuerza pública o moral.

Ataques desde el exterior: No solo pueden generar destrucción patrimonial, sino también pérdidas de vidas e integridad personal y moral de las personas vinculadas a la institución o visitantes o toma de rehenes.

Hurto de material o información clasificada: Es el llamado espionaje industrial que puede ser usado por subversivos, delincuentes y competidores desleales, para planear

y ejecutar delitos contra empresas o instituciones u obtener ventajas de mercadeo y producción.

4.2. PLANTEAMIENTO DE MEJORAMIENTO DE LA SEGURIDAD FÍSICA DELAS UNIDADES MILITARES.

4.2.1. RECOLECCION, CLASIFICACION Y EVALUACION DE LA INFORMACIÓN

Teniendo en cuenta los conceptos generales expuestos, tanto con respecto a la Seguridad y Orden Público General como de Seguridad Física, es necesario empezar a estructurar el Plan de Reestructuración de la Seguridad Física de las unidades militares.

En la Recolección de la información necesaria para realizar las modificaciones pertinentes, se implementó en El Departamento De Seguridad Del Comando General un modelo que puede servir para las unidades militares de todo el país y un formato que tramitado en trabajo de campo, proporcionaría los aspectos sobresalientes de lo existente y por ende, aquellos aspectos que deben ser tenidos en cuenta para implementar, modificar y eliminar dentro de la estructura física de la protección de las unidades.

Se efectúo el siguiente procedimiento:

1. Revisión de las instalaciones construidas actualmente. Se efectúo la consulta sobre los planos del Complejo existentes, adicionando sobre los mismos, las instalaciones de construcción reciente que no se encontraban radicadas en los mismos, así como las modificaciones a los existente en planimetría. Es de advertir que no se adjuntan al proyecto, en vista de constituir material SECRETO.

2. Levantamiento de Inventario de las diferentes medidas de seguridad implementadas, así como su estado de funcionamiento, condiciones de labor y cumplimiento. En este aspecto se relacionó el manejo de un formato, teniendo en cuenta tanto Seguridad Física de Instalaciones, como Personas e Información.

3. Evaluación del desempeño de los procedimientos de control implementados existentes, actuales y en practica. Se efectúo un estudio de los manuales de funciones del personal vinculado al Departamento de Seguridad y por ende, la determinación de diferentes procedimientos de seguridad, implementados con el fin de establecer su estado, cumplimiento y obediencia, así como conveniencia y actualización del mismo.
4. Recolección de inquietudes sobre el tema a base de informes de las diferentes dependencias integrantes del Comando General.
5. Levantamiento de información sobre medidas adoptadas con respecto a la zona y área de influencia del comando General, en el C.A.N., tanto por la institución como por las demás entidades circundantes. Se efectúo un levantamiento fotográfico situacional aéreo de la ubicación del Comando General, sobre la zona, y se determinaron las áreas, zonas y puntos vulnerables y fuertes de la misma. Es parte del anexo SECRETO.

4.2.2. PROYECCION DE AMENAZAS, VULNERABILIDADES Y ACCIONES DE CONTINGENCIA

Recolectada la información, esta fue seleccionada teniendo en cuenta el concepto de seguridad de Instalaciones y los riesgos que las mismas presentan, Seguridad de personas y Seguridad de Información, diseñando el Círculo de Seguridad determinado como las normas, procedimientos, operaciones y responsabilidad de la función de seguridad, y que busca dos objetivos esenciales:

*Reducir la acción, el alcance y el peligro de las amenazas y riesgos reales o potenciales de perdida, perturbación, daño, perjuicio y lesión.

*Eliminar definitivamente los riesgos y amenazas reales y potenciales.

De esta manera, se recomendó una evaluación de la información recogida estructurando los factores de riesgo y amenaza de las instalaciones y personas que comprenden el Comando General para determinar las posibles acciones de protección y seguridad, de la siguiente manera:

Se organizó con la Fuerza Aérea un vuelo en helicóptero para tomar una serie de fotografías donde se establece los diferentes sectores exteriores del Comando General el cual nos permite parámetros específicos de la ubicación con respecto a las instalaciones aledañas al CAN y sus vecinos al norte, sur, oriente y occidente. Extractando estas fotografías los diferentes puntos críticos del sector de una manera más detallada concluyendo las amenazas vulnerabilidades y acciones a ejecutar las cuales me facilitó para concluir el trabajo de campo.

Estas tablas perfectamente pudieron consignarse en los anexos.

TRABAJO DE CAMPO

MENAZA	VULNERABILIDAD	FORTALEZA	ACCIONES A EJECUTAR	OPORTUNIDAD
	❖ Falta de Defensa antiaérea ❖ Ubicación geográfica ❖ Falta sistema	Entrenamiento que poseen los cuadros ; en especial los de seguridad de bases de la fuerza aérea	✓ Colocación de afustes múltiples para ametralladoras punto 50 ✓ Integrar y unificar sistemas de comunicaciones (Centro, Comando y Control)	Apoyo incondicional a todo nivel de toda medida de seguridad tendiente a la conservación de la infraestructura

\QUE REO	unificado de comunicaciones. ❖ Falta de Sistema integrado de seguridad.		✓ Enlazar el sistema de monitoreo de frecuencias aeronáuticas con las defensas en las terrazas (Comando y Control). ✓ Coordinar nuevas notificaciones de tráfico aéreo mínimo NOTAM (Planes). ✓ Coordinar prohibición a tráfico por debajo de 500 pies (Planes)	
HÍCULOS N TEFACTOS PLOSIVOS Y PLOSIVOS CION ENDARIA	❖ Áreas con deficiente control ❖ Falta de iluminación ❖ Falta de control de accesos y tránsitos. ❖ Falta de mecanismos electrónicos. ❖ Barreras perimétricas deficientes ❖ Rutina en los desplazamientos militares. ❖ Alcantarillas en las rutas ❖ Proliferación de	Cuadros expertos en el manejo de explosivos en especial en el arma de ingenieros militares	• Colocar anillos de seguridad apoyados por medios técnicos y humanos. • Coordinación con responsables de la seguridad de entidades aledañas. • Corregir deficiencias de iluminación con censores de movimientos. • Personal de seguridad con mayor capacitación, permanencia y dotación de equipos técnicos y ayuda animal (caninos) . • Construcción de barreras perimétricas. • Equipos de detección de explosivos	Apoyo y exigencia a la implementación de la seguridad tendiente a evitar atentados terroristas en unidades militares

	vendedores Ambulantes y proveedores.		• Suspender recorridos de personal. • Ordenar el tránsito de militares de civil por vías públicas . • Colocación de sellos en las alcantarillas previa autorización de Empresa de Acueducto y Alcantarillado). • Acción de los PORAS (Patrulla de reconocimiento de áreas críticas.	
ATAQUES CON ARMAS DE TIRO PARABOLICO	❖ Áreas con deficiente control ❖ Ubicación geográfica ❖ Falta de mecanismos electrónicos	Experiencia que se ha adquirido por los ataques con cilindros a las unidades militares	• Coordinar con la Policía la integración de carabineros ,campaña de afiches, volantes, calcomanías al vecindario.	Después del ataque al Palacio presidencial ; el apoyo tendiente a evitar esta clase de acciones es total
SUPLANTACION DE PERSONAL	❖ Falta de Control de acceso y tránsitos ❖ Organización de dependencias en planta física. ❖ Falta de mecanismos electrónicos.	Se ha generado conciencia por la ocurrencia constante de esta clase de hechos en tiempos pasados	• • Implementar una base de datos, con el personal de Oficiales, Suboficiales, Soldados, Civiles en actividad o en retiro de las Fuerzas Militares, en donde figure	Exigencias tendientes a restringir el acceso de personal ajeno a las unidades militares

Continuación.....	❖ Carencia de seguridad integrada. ❖ Alta rotación en el personal de seguridad. ❖ Rutina en los procedimientos de seguridad.		nombres y apellidos, número de identificación (cédula y código militar), si se encuentra en actividad o retiro y la Unidad de la cual es orgánico; mencionada la base ésta debe ser manejada por un cuadro y sólo para consulta sin que de allí se pueda modificar la información existente, permanentemente actualizada, complementada con la base de datos del Departamento de Seguridad de ficheros de identificación personal y temporal del Cuartel General, con el montaje de un sistema. • Coordinar con los organismos de seguridad el manejo de información de personal que cuente con	

Continuación..... SUPLANTACION DE PERSONAL			antecedentes judiciales y/o anotaciones de inteligencia. • Construcción de un Centro de atención en el área externa de las unidades militares. • Implementar un Centro Critico de Tele video (CTV), ya sea por sistemas digitales de grabación Y transmisión de imágenes, cámaras digitales, cámaras ocultas o micro cámaras y micrófonos y renovación e incremento de los equipos. • Capacitar al personal de Guardia en lo referente a detectar documentos militares falsos. • Sensibilizar al personal que integra las unidades militares sobre el cumplimiento de las normas de seguridad. • Cambiar los	

			soldados que estén comprometidos con la seguridad, regulares por soldados profesionales. • Disminuir la alta rotación del personal responsable de la seguridad. • En cuanto al control e identificación del personal, hay que basarlo más en el sistema de identificación de documentos y no en el reconocimiento personal.	
INFILTRACIÓN O PENETRACION PRINCIPALMENTE EN LOS SOLDADOS	❖ Falta de mecanismos electrónicos ❖ Falta de control de accesos y tránsitos ❖ Deficiencia en procesos de selección. ❖ Enganche y evaluación. ❖ Alta rotación en el personal de seguridad.	Conciencia de contrainteligencia que se ha adquirido	• Evitar que reinsertados, quienes hayan dejado las armas, bandoleros capturados o desertores tengan libre movimiento por las Dependencias de las unidades, teniendo acceso a la información, conocimiento de personal e instalaciones.	Denuncia constante de la población por recompensa

Continuación INFILTRACION O PENETRACION PRINCIPALMENTE EN LOS SOLDADOS			• El personal que presta sus servicios en las unidades militares debe abstenerse de portar el fichero de identificación personal fuera de las instalaciones. • • Crear una cultura o conciencia de Contrainteligencia que permita contrarrestar el accionar del enemigo al interior de las unidades militares. • Construcción de un centro de atención en el área externa de las unidades. • Coordinar con los organismos de seguridad sobre el manejo de información, de personal que cuente con antecedentes judiciales y/o anotaciones de inteligencia, asimismo, con los Comités encargados para la reinserción y/o	

Continuación INFILTRACION O PENETRACION PRINCIPALMENTE EN LOS SOLDADOS			dejación de armas. • Implementar CTV ya sea por sistemas digitales, de grabación y transmisión de imágenes, cámaras digitales, cámaras ocultas o micro cámaras y micrófonos. • Inspeccionar oficinas, salas de conferencias, salas de guerra y otros locales similares en los cuales se discute información clasificada, para verificar que estén libres de sistemas clandestinos de escucha, grabación o filmación, buscar modificaciones no autorizadas en el equipo. • Modificar el sistema de rotación del personal responsable de la seguridad. • Apoyar el fortalecimiento de las secciones de Contrainteligencia, para que garanticen la neutralización de	

Continuación INFILTRACION O PENETRACION PRINCIPALMENTE EN LOS SOLDADOS			las actividades enemigas. • Crear una cultura o conciencia de contrainteligencia que permita contrarrestar el accionar enemigo al interior de las unidades. • Aplicación de las medidas de seguridad de personal, a saber: ESP preliminar y/o completa, comprobación de lealtad: (preliminar, incidente o por individuo), además adelantando operaciones especiales de Contrainteligencia específicamente de contra subversión. • Pruebas de poligrafía para el personal que ocupa cargos sensibles. • Observar el comportamiento individual y reincidente del personal que se ajuste a las instrucciones que emite el ELN en el	

			Plan Jesús Uribe para someterlos a control y supervisión de la Contrainteligencia.	
GUERRA ELECTRÓNICA E INFORMATICA Continuación	❖ Carencia de contramedidas en información de sistemas.	Conciencia adquirida para evitar sabotajes a la informática, especialmente en las secciones que manejan aspectos restringidos	• Cultura informática, para enfocar estratégicamente la seguridad que surja desde arriba hacia abajo. • La seguridad un tema de todos y no se limita a la información, ni la solución, es únicamente tecnológica. • Capacitación especializada sobre la tecnología de punta al personal de Oficiales de Ingenieros de Sistemas DIINF. • Respaldo a las políticas de seguridad informática establecidas por la Dirección. Ejemplo: No acceso a correos públicos gratuitos, no todo el personal debe	Cantidad de software con componentes de seguridad que se ofrecen en el comercio

GUERRA ELECTRÓNICA E INFORMATICA			tener acceso a Internet. • Efectuar retenes informáticos en la entrada y salida del edificio para verificar qué información entra y sale en diskettes y/o CD Roms. • Asignar personal de Oficiales y Suboficiales profesionales en sistemas a la Dirección de informática para capacitarlos en la guerra contra el ciberterrorismo.	

SABOTAJE A LAS COMUNICACIONES	❖ Observación del enemigo ❖ Falta de mecanismos electrónicos. ❖ Carencia de contramedidas e información de sistemas ❖ Deficiencia en procesos de selección, enganche y evaluación.	Autonomia en los sistemas de comunicación (red propia)	• Campaña de telecomunicaciones para usar seguridad de voz. • Organizar las antenas que se encuentran en las unidades.	Oferta de equipos de comunicación cada vez mas seguros

ATENTADO A PERSONALIDADES MILITARES EN DESPLAZAMIENTOS	❖ Observación del enemigo ❖ Áreas con deficiente control ❖ Seguridad Protectiva ❖ Ubicación geográfica. ❖ Rutinas en los desplazamientos militares ❖ Alcantarillas en las rutas ❖ Proliferación de vendedores ambulantes y proveedores. ❖ Rutina en los procedimientos de seguridad.	Entrenamiento de las escoltas	• Modificar rutas, horarios, vehículos, constantemente. • Intensificar la capacitación e instrucción a los Patrulla de Reconocimiento en las Áreas Criticas – PORAS- (combatir la rutina). • Verificar los puntos críticos con caninos antiexplosivos. • Aumentar el número de informantes redes a cubierto, fachadas. • Adquirir mayor número de vehículos blindados. • Capacitar y reentrenar escoltas. • Reforzar los medios de recolección de inteligencia humana (bodoques). • Acceso subterráneo en instalaciones.	Apoyo a la adquisición de equipos que faciliten la seguridad de personajes
Continuación ATENTADO A PERSONALIDADES MILITARES EN DESPLAZAMIENTOS				

ATAQUE BACTERIOLÓGICO Y ENVENENAMIENTO DE LOS ALIMENTOS	❖ Observación del enemigo ❖ Falta de medios para contrarrestar la guerra bacteriológica	Deseo de evitar esta clase de hechos	• Tomar contacto con entidades de sanidad para recibir instrucción, capacitación y adquisición de medios para contrarrestar ese tipo de amenaza. • Adquisición de material como máquinas de Rayos "X", capacitación de personal con experiencia USA, coordinación con Embajada de los Estados Unidos sobre métodos últimamente utilizados para contrarrestar esta amenaza.	La doctrina de cómo manejar esta amenaza a raíz de los ataques con ántrax en los EEUU
ACCION FRANCOTIRADOR	❖ Observación del enemigo ❖ Áreas con deficiente control. ❖ Falta de iluminación	Entrenamiento para evitar esta clase de ataques	• Polarización de vidrios exteriores. • Realizar revistas a los edificios y campos vacíos aledaños a las unidades militares. • Los vehículos del mando en caso de	Apoyo a la implementación de medidas por parte de toda la población en sitios aledaños a las unidades militares

Continuación ACCION FRANCOTIRADOR	❖ Infraestructura débil Arquitectónicamente ❖ Barreras perimétricas. deficientes. ❖ Rutinas en los desplazamientos militares. ❖ Falta de mecanismos electrónicos. ❖ Seguridad protectiva.		riesgo por la entrada principal de las unidades tendrán acceso por otra entada. • Blindaje de vidrios y recubrimiento de paredes. • Verificar la dotación de radios y líneas internas que están ubicadas en las terrazas y antenas de las unidades. • Colocación de una red de teléfonos autoexitados-teléfonos de campaña. • Coordinar con las autoridades para el desalojo total de vendedores ambulantes en un perímetro no menor a 300 mts, de las instalaciones militares. • Adquisición y utilización de chalecos blindados de alto grado de protección.	
Continuación ACCION FRANCOTIRADOR				
	❖ Áreas de deficiente control ❖ Infraestructura	Conciencia por parte de los cuadros de que este ataque se	• Incremento de revistas por parte de los TOPOS,(soldados que	Apoyo por parte de los estamentos para la colocación de dispositivos que eviten esta clase de

ATAQUE SUBTERRANEO	débil arquitectónicamente ❖ Ubicación geográfica. ❖ Alcantarillas en las rutas. ❖ Falta de mecanismos electrónicos. ❖ Rutina en los procedimientos de seguridad.	puede presentar	revisan las alcantarillas) sin rutinizar y no realizarse solo por cumplir la orden. • Instalación de rejas internas en los tubos de aguas negras, ampliar y perfeccionar el sistema de censores. • Ubicación y sellamiento de cajas de desagüe (tapas) • concienciar al personal de conductores y personal civil de esquivar y no pasar sobre las alcantarillas en las rutas.	hechos

4.2.3. LISTADO DE ACCIONES A EJECUTAR

- ✓ Colocación de armas antiaéreas.
- ✓ Integrar y unificar sistemas de comunicaciones
- ✓ Enlazar el sistema de monitoreo de frecuencias aeronáuticas con las defensas en las terrazas.
- ✓ Coordinar nuevas notificaciones de tráfico aéreo mínimo NOTAM.
- ✓ Coordinar prohibición a tráfico por debajo de 500 pies.
- ✓ Ejecutar ejercicios de simulación.
- ✓ Colocar anillos de seguridad apoyados por medios técnicos y humanos.
- ✓ Coordinación con responsables de la seguridad de entidades aledañas.
- ✓ Corregir deficiencias de iluminación con censores de movimiento.
- ✓ Personal de seguridad con mayor capacitación, permanencia y dotación de equipos técnicos y ayuda animal (caninos.
- ✓ Construcción de barreras perimétricas.
- ✓ Equipos de detección de explosivos
- ✓ Suspender recorridos de personal.

✓ Ordenar el tránsito de militares en traje de civil por vías públicas.

✓ Colocación de sellos en las alcantarillas previa autorización de la empresa de alcantarillado y acueducto.

✓ Acción de los PORAS (Patrulla de reconocimiento de las áreas críticas).

✓ Suspender la edición de ficheros a tramitadores y comerciantes.

✓ Coordinar con la policía la integración de carabineros en la seguridad perimétrica, campaña de afiches, volantes, calcomanías al vecindario.

✓ Implementar una base de datos de personal militar (activo y retirado) y civiles que con alta frecuencia deban ingresar a las instalaciones y mantener una interacción con la base de datos del personal con antecedentes judiciales o anotaciones de la unidad militar con la Policía Nacional.

✓ Construcción de un Centro de Atención en el área externa de las actuales edificaciones.

✓ Transformar el CCTV, en centro de Comando y Control con sistemas digitales de grabación y transmisión de imágenes, cámaras digitales, cámaras ocultas o micro cámaras y micrófonos, renovación e incremento de los equipos.

✓ Mejorar el sistema de identificación y control de ingresos (código de barras u otros).

✓ Sensibilizar al personal que integra la unidad militar sobre el cumplimiento de las normas de seguridad.

✓ Cambiar los Soldados regulares que tengan responsabilidad directa en la seguridad de las instalaciones por Soldados profesionales.

✓ Disminuir la alta rotación del personal responsable de la seguridad.

✓ Crear una cultura o conciencia de contrainteligencia que permita contrarrestar el accionar del enemigo al interior de la unidad militar.

✓ Aplicación de las medidas de seguridad de personal, a saber: Estudio Seguridad Personal (ESP) preliminar y/o completa, comprobación de lealtad: (preliminar, incidente o por individuo.

✓ Pruebas de poligrafía para el personal que ocupa cargos sensibles.

✓ Observar el comportamiento individual y reincidente del personal que se ajuste a las instrucciones que emite el ELN en el Plan Jesús Uribe para someterlos a control y supervisión de la Contrainteligencia.

✓ Cultura informática, para enfocar estratégicamente la seguridad.

✓ La seguridad un tema de todos y no se limita a la información, ni la solución es únicamente tecnológica.

✓ Incrementar el uso de medios de uso de seguridad de voz.

✓ Organizar las antenas de comunicaciones.

✓ Tomar contacto con entidades especializadas nacionales y extranjeras para recibir instrucción, capacitación y medios para contrarrestar amenazas de ataque químico y bacteriológico.

- ✓ Adquisición de capacidad técnica como máquinas de Rayos "X".

- ✓ Polarización de vidrios exteriores de los edificios e instalaciones de la unidad.

- ✓ Realizar revistas a los edificios y campos vacíos aledaños a la unidad militar.
- ✓ Blindaje de vidrios y recubrimiento de paredes en oficinas claves.

- ✓ Verificar la dotación de radios y líneas internas que están ubicadas en el la unidad militar que son utilizados por los Centinelas y que hagan parte del sistema integrado de seguridad.

- ✓ Colocación de una red de teléfonos autoexitados – teléfonos de campaña.

- ✓ Coordinar con las autoridades para el desalojo total de vendedores ambulantes en un perímetro de 300 mts de las instalaciones de las unidades militares.

- ✓ Adquisición y utilización de chalecos blindados de alto grado de protección por parte del personal de mayor grado y jerarquía mientras se ejecutan las modificaciones físicas.

- ✓ Incremento de revistas a conciencia por parte de los topos, sin rutinizar.

- ✓ Instalación de rejas internas en los tubos de aguas negras, ampliar y perfeccionar el sistema de censores.

- ✓ Ubicación y sellamiento de cajas de desagüe (tapas.

- ✓ Concienciar al personal de conductores y personal civil para que esquive y no pase sobre las alcantarillas en las rutas al ingreso y salida de las instalaciones.

✓ Incrementar los desplazamientos en traje de civil cuando se exija el uso de uniforme.

✓ Utilizar los medios de comunicaciones existentes (líneas internas, teléfono celular y fija, Internet, relaciones generales, etc.), para estar continuamente recabando las medidas de seguridad personales y avisando inmediatamente cualquier tipo de novedades mediante campañas permanentes.

✓ Efectuar ejercicio y simulaciones sobre la reacción en los diferentes simulacros.

✓ Modificar rutas, horarios y vehículos constantemente.

✓ Intensificar la capacitación e instrucción a los PORAS (combatir la rutina).

✓ Verificar los puntos críticos con caninos antiexplosivos.

✓ Aumentar el número de informantes redes a cubierto, fachadas.

✓ Adquirir mayor número de vehículos blindados.

✓ Capacitar y reentrenar escoltas.

✓ Reforzar los medios de recolección de inteligencia humana – (bodoques).

✓ Acceso subterráneo en las instalaciones militares.

4.2.3.1. IMPLEMENTACION DE AREAS A PROTEGER

Para cumplir con el objetivo determinado en el inicio de esta labor, es necesario, una vez recolectada la información tener en cuenta algunas circunstancias y características estipuladas para implementar el Plan de Seguridad.

La Planeación en materia de Seguridad Física, requiere de la definición cuantitativa y cualitativa del objetivo, como su dimensión, composición, divisiones internas, accesos y además concretar ubicación, actividades que se desarrollan, entorno, climatología y otras, que permiten saber todo lo imprescindible para proteger.
A partir de allí, se debe realizar una lista de amenazas definida como toda causa capaz de producir perdidas o daños las cuales pueden ser agrupadas, como Materiales, entre las que se encuentran los terremotos, inundaciones, deslizamientos, accidentales como incendios, explosiones, contaminación; provocadas, determinadas como sabotaje, intrusión, secuestro, vandalismo, hurto, entre otros. Enumeradas de donde se parte para efectuar la evasión del riesgo, entendida como la probabilidad de que la amenaza se cumpla, teniendo en cuenta los siguientes criterios.

- Criterio de función, entendida como la materialización de la amenaza en las personas y las cosas que puedan alterar de forma diferente la actividad.

- Criterio de sustitución, representa la capacidad de que los bienes sean sustituidos, duplicados o reparados.

- Criterio de profundidad, representa la gradación de la profundidad y los efectos psicológicos por su efecto en la imagen.

- Criterio de extensión determina el alcance de los daños según su amplitud territorial.

- Criterio de agresión, probabilidad de que se produzca un ataque.

- Criterio de vulnerabilidad, que es el criterio de seguridad o probabilidad de que el ataque produzca daño.

De aquí en adelante se tendrá en cuenta la distribución de los medios, tanto en número suficiente para abastecer las necesidades planteadas, como la optimización de su ubicación, con el fin de atender las zonas de mayor vulnerabilidad. Entre los medios se encuentran los Humanos, que a su vez, se clasifica, en Primarios, que son "aquellos que tienen encomendadas misiones específicas dentro del plan de protección de un determinado objetivo,... Este personal puede tener asignadas funciones de control, observación o vigilancia,... " (8); y Secundarios aquellos que intentan impedir o retardar la entrada en zonas determinadas, o canalizar los flujos de entrada hacia zonas especialmente habilitadas, entre los cuales se encuentran los medios de seguridad electrónica. Los segundos son los medios Organizativos, que se definen como "... el conjunto de estrategias y planes de acción que pretenden adecuar y racionalizar el uso de los medios humanos y técnicos con el fin de garantizar su aprovechamiento ante los incidentes que se puedan producir." (9).

Posteriormente a la determinación de los medios, se deben verificar la viabilidad y eficacia del plan, en cuanto a la viabilidad económica como en el cumplimiento de los objetivos generales planteados. Con respecto a la viabilidad económica, es de tener en cuenta que "Si la disponibilidad económica es inferior al planteamiento inicial, se debe proceder a reducir los medios dispuestos en la cuantía mínima para que de esta manera se adecuen a las posibilidades reales". (10).

Dentro de la filosofía de la Seguridad Física, se encuentra el concepto de líneas de protección o círculos de seguridad, definido como " Normas, Procedimientos, operaciones y responsabilidad de la función de seguridad" que buscan dos objetivos:

*Reducir la acción, el alcance y el peligro de las amenazas y riesgos reales o Potenciales de perdida, perturbación, daño, perjuicio y lesión.

*Eliminar definitivamente los riesgos y amenazas reales y potenciales.

De ello surge la necesidad de dividir la función general en segmentos cuya sumatoria integra el círculo de seguridad: SEGURIDAD DE INSTALACIONES – SEGURIDAD PERSONAL – SEGURIDAD DE INFORMACION.

En el caso objeto de esta labor, han surgido cuatro áreas para tener en cuenta, sobre las cuales se pueden establecer las acciones a seguir, así:

- CONTROL DE ACCESO EN AREAS ESPECIFICAS
- CONTROL DE SEGURIDAD INTERNA
- CONTROL DE SISTEMA ELECTRICO
- CONTROL DE SEGURIDAD PERIMETRAL

4.2.4. IMPLEMENTACION DE ESTRATEGIAS DE CONTINGENCIAS.

4.2.4.1. CONTROL DE ACCESO EN AREAS ESPECIFICAS

Se define control de acceso a un punto de comprobación de la identidad de personas o de la naturaleza de objetos para garantizar que tienen autorizada la entrada a una zona restringida.

---

(8) GUIA DE SEGURIDAD FÍSICA, Profesor Manuel A. Novoa B. 2002 Página 8
(9) GUIA DE SEGURIDAD FÍSICA, Profesor Manuel A. Novoa B. 2002 Página 9
(10) GUIA DE SEGURIDAD FÍSICA, Profesor Manuel A. Novoa B. 2002 Página 9

Tiene como funciones la identificación de personas y comprobación de su autorización de entrada, la inspección de paquetes y correspondencia u el control y requisa de proveedores y mercancías a los que deberá habilitarse un acceso exclusivo por la demora que conlleva efectuar esta labor de modo exhaustivo.

Dependiendo del elemento que sea objeto del control, será el control como tal: de personas, de vehículos y de maquinaria.

De acuerdo a la información recolectada el acceso en áreas específicas, en el caso que nos ocupa, estará conformado de la siguiente manera:

4.2.4.2. SISTEMA DE CONTROL DE ACCESO A GUARDIA Y PORTERIAS PRINCIPALES DE LAS UNIDADES MILITARES.

A) OBJETIVO GENERAL

Diseñar y proponer una solución que permita sistematizar y automatizar por etapas la seguridad en la entrada y salida de las unidades militares, utilizando tarjetas Inteligentes para el acceso no solo a las instalaciones generales de la unidad, sino de igual modo a los diferentes edificios en el interior del mismo. Adicionalmente se desea que en una próxima etapa se pueda utilizar la misma infraestructura tecnológica para otros servicios dentro de las instalaciones como incrementar el control de seguridad a las plantas de cada edificio, a las oficinas, etc.

B) OBJETIVOS ESPECIFICOS

(Que debe cumplir la solución propuesta)

- Distribuir y asignar las tarjetas bajo ambiente controlado, al personal de cada módulo en guardia encargado de la autorización a visitantes.
- Almacenar información histórica de entradas a cada edificio para identificar el comportamiento de cada uno de los visitantes.
- Restringir el tiempo que tiene cada visitante para permanecer dentro de las instalaciones (bien sea en zonas libres o dentro de los edificios) de la Institución.
- Tener una herramienta adicional de control de accesos en las puertas principales de los edificios al interior de las unidades.
- Administrar información de cada uno de los empleados o personas autorizadas a ingresar en la unidad, registrando días y horas de ingreso o salida, tiempo de duración, para obtener reportes estadísticos de: Horas pico, frecuencia y volumen de visitas por dependencia, número de visitantes, intentos de accesos denegados, tiempo promedio que permanece personal ajeno a la institución dentro del recinto, etc.
- Controlar el ingreso máximo de personas ajenas a la Institución en cada uno de los edificios y pisos (topes.
- Saber en cualquier momento cuántos visitantes hay en la unidad.
- Saber en cualquier momento dónde está un visitante en la unidad.
- Retener para recircular, las tarjetas de visitantes en la salida de la unidad por medio de un recolector de tarjetas.
- Manejar listas negras e inhabilitación de tarjetas.
- Imprimir una etiqueta de identificación del visitante

C) FUNCIONAMIENTO

a) Visitantes:

La persona cuando va ingresar al la unidad militar, se acerca a uno de los módulos de la guardia para solicitar la identificación pertinente. Allí mismo se le entrega además de

una tarjeta cargada en su interior con la información del individuo, los accesos a los que tiene derecho y la hora y tiempo máximo autorizado de ingreso.

Posteriormente se dirige hacia uno de los torniquetes a cintura de entrada y presenta la tarjeta. El sistema verifica y almacena la clave de acceso, número de identificación, numero de la tarjeta, hora de entrada y revisa las listas negras (el atributo de inhabilitada, robada o perdida. En caso de encontrarse en estas últimas, el sistema no deja pasar al individuo y genera una alarma visual y sonora.

Al llegar a cada una de las puertas delas edificaciones estas cuentan con un lector de pared, que será paso obligado por todos los portadores de tarjetas. Al acercar una tarjeta por el lector, este verificará la hora de ingreso en guardia para controlar el tiempo máximo que puede durar una persona entre la entrada a las Instalaciones y la entrada específica al edificio. Si la persona se equivoca de departamento o se excede de tiempo el equipo prende una alarma sonora de 5 segundos aproximadamente, prende la luz roja y por el display de cristal líquido le informa qué tipo de inconveniente no le permite accesar. Así pues encenderá una luz verde o roja según sea permitido o denegado el acceso y desplegará un comentario pertinente en el display (además de una alarma sonora sí el caso lo requiere. Puede incluso guardarse el acceso a dos edificios a diferentes horas, pero pensamos que la segunda autorización debe ser validada por un superior.

A la salida se debe acercar la tarjeta nuevamente al lector de pared antes de salir por la guardia, en donde la tarjeta inteligente se inserta por una ranura del torniquete, el sistema verifica que la persona esté saliendo en el tiempo autorizado, o de lo contrario dispara una alarma sonora y visual, además de no dejar salir al individuo. El sistema almacena los datos que ha recolectado la tarjeta y además la hora de salida.

b) Empleados:

La persona cuando va ingresar al la unidad se acerca directamente a los los torniquetes a cintura de entrada y presenta la tarjeta. El sistema verifica y almacena la clave de acceso, número de identificación, número de la tarjeta, hora de entrada y revisa las listas negras (el atributo de inhabilitada, robada o perdida. En caso de encontrarse en estas últimas, el sistema no deja pasar al individuo y genera una alarma visual y sonora.

A la salida, el empleado presenta su tarjeta inteligente en la superficie del torniquete el cual le permite la salida. El sistema almacena los datos que ha recolectado la tarjeta y además la hora de salida.

Se podría también pensar que el empleado pase la tarjeta nuevamente por el lector de salida para registrar los movimientos al interior, pero esta opción en primera fase no representa mayor valor agregado.

D) DETALLES TECNICOS

a). HARDWARE

1.1 Electrónica de los torniquetes

- Entradas Digitales respectivas
- Salidas de Potencia con las cuales se podrán activar los traba pestillos convencionales, cerraduras de seguridad motorizadas, portones, molinetes, barreras
- Salidas de Colector Abierto: para manejar señales luminosas de poco consumo de energía.
- Display de cristal liquido: El sistema muestra la cantidad de entradas que tiene la tarjeta, entrega información e incluso dispara alarmas.
- Puerto de Comunicación RS232: Para la comunicación con el lector de tarjeta Inteligente sin contacto.

- Puerto de Comunicación RS485: Para la comunicación con el computador central y si en algún momento se cae la red, el equipo siga funcionando por que él tiene la capacidad de ser autosuficiente.
- Ingreso por Tarjetas de Inteligentes Proximidad: Es el medio más cómodo y seguro. Debido a que los lectores trabajan por RF (Radio Frecuencia), los mismos están colocados dentro de los torniquetes, reduciendo al máximo los casos de sabotaje o vandalismo. Otra de sus ventajas radica en la imposibilidad de duplicar una tarjeta y la misma puede ser leída, incluso dentro de una billetera o cartera.
- AlarmaAnti-Desarme y PuertaAbierta:

La primera se activa mediante un dispositivo contra desarme si alguien intenta violar el gabinete. La segunda alarma se activa cuando la puerta permanece abierta o mal cerrada durante un lapso mayor al indicado por el supervisor.

- Anti PassBack:

Es posible restringir el acceso a una tarjeta, de modo que no pueda ser usada dos veces en el mismo sentido (una entrada luego de una entrada, o una salida luego de otra.

1.2. Capturador de tarjetas inteligentes

Cuando los visitantes van a salir definitivamente de la institución introducen la tarjeta al equipo (Capturador de tarjetas inteligentes).

Al introducir la tarjeta al equipo este detectará que están introduciendo la tarjeta, activa el motor para entrar la tarjeta hasta posesionarla debajo del lector de tarjeta inteligente sin contacto.

Cuando haya realizado toda la operación programada, el equipo genera una orden que en este caso es capturar la tarjeta.

Lector sin contacto Micro 680 (Ver especificaciones técnicas del Anexo)

Lector sin contacto GemAccess 608 (Ver especificaciones técnicas del Anexo)

1.3.Electrónica del equipo de pared

- Entrada Digitales respectivas
- Salidas de Potencia con las cuales se podrán activar los traba pestillos convencionales, cerraduras de seguridad motorizadas, portones, molinetes, barreras.
- Salidas de Colector Abierto: Son salidas para manejar señales luminosas de poco consumo de energía.
- Display de cristal liquido: Por medio de este display el sistema informa a la persona (visitante, empleado) si puede seguir o no y a qué departamento entra.
- Puerto de Comunicación RS232: Por este puerto se comunica con el lector de tarjeta Inteligente.
- Ingreso por Tarjetas de Inteligentes Proximidad: Es el medio más cómodo y seguro. Debido a que los lectores trabajan por RF (Radio Frecuencia), los mismos están colocados dentro de los torniquetes, reduciendo al máximo los casos de sabotaje o vandalismo. Otra de sus ventajas radica en la imposibilidad de duplicar una tarjeta y la misma puede ser leída, incluso dentro de una billetera o cartera.
- Alarma Anti-Desarme y Puerta Abierta: La primera se activa mediante un dispositivo contra desarme si alguien intenta violar el gabinete. La segunda alarma se activa cuando la puerta permanece abierta o mal cerrada durante un lapso mayor al indicado por el supervisor.
- AntiPassBack: Es posible restringir el acceso a una tarjeta, de modo que no pueda ser usada dos veces en el mismo sentido (una entrada luego de una entrada, o una salida luego de otra.

Lector sin contacto GemAccess 608 (Ver especificaciones técnicas del Anexo)

b). SOFTWARE

1.1 Software de Alto nivel

Software que se encargará de cumplir con TODOS los objetivos específicos de la presente propuesta (Para el PC administrador y los módulos de atención en guardia. Se utilizará un sistema manejador de bases de datos relacionales (SMBD)

1.2 Software de Bajo Nivel

1.2. Software de las máquinas encargado de la comunicación.

c). Tarjetas inteligentes sin contacto, deacuerdo a la necesidad

4.2.5 CONTROL DE SEGURIDAD INTERNA

Se debe implementar teniendo en cuenta los siguientes aspectos:

- Sistema de protección contra incendio
- Sensores de humo
- Sensores térmicos
- Paneles control central integrados al sistema
- de automatización
- Estaciones manuales de incendio
- Cámaras infrarrojas para control de alcantarillas
- Mantenimiento

4.2.6 Control de Sistema Eléctrico

Se debe implementar bajo los siguientes aspectos:

- Sistema de control y monitoreo del alumbrado exterior y puntos fijos donde existan Cámaras
- Software y equipos, adquisición de datos para control de alumbrado
- Software y equipo, adquisición de datos para control de energía

- Software y equipo, adquisición de datos para control de plantas eléctricas.

4.2.7 Control de Seguridad Perimetral

Los aspectos importantes por el trabajo de campo son:

- Construcción de sala de control e integración del sistema de acceso y seguridad.
- Complementación en control de accesos y circulación en zonas pendientes.
- Control de barreras perimetrales
- Sensores de vibración y fotoeléctricos
- Reconocimiento de rutas (poras)
- Control de operación y mantenimiento de equipos existentes

5. COSTOS Y APROPIACIONES PRESUPUESTALES

De la primera fase y consistente en la implementación del control de acceso en áreas específicas, los costos se solicitaran por licitación publica y varían de a cuerdo con la configuración de la unidad militar y de las diferentes empresas que suministran estos equipos.

5.1. PROPUESTA OTROS ELEMENTOS

De acuerdo con los anexos:

A- Servicios electrónicos de seguridad

B- Sistemas de control de acceso.

C- Subsistema de trasmisión

D- Sistema integrado.

E- Localización automática de vehículos.

F- Equipos especializados.

ANEXO A

SERVICIOS ELECTRONICOS DE SEGURIDAD

Tales como: aparatos de telecomunicaciones, de vídeo, de audio, electromecánicos, etc. que garanticen la máxima eficiencia en la seguridad que vamos a desarrollar.

PRINCIPALES APLICACIONES

Seguridad Perimétrica externa e interna de la planta, local o persona, concertinas, vallas metálicas, cerraduras, candados, puertas, barreras, cristales blindados, chalecos antibalas, sensores sísmicos y de movimiento.

Control de Accesos: barreras microondas, infrarrojos, campos electrónicos, fibra óptica, adosados a la valla (mecánicos, electromecánicos, geofónicos, piezoeléctricos) de subsuelo (sísmicos, magnéticos, cable radiante).

Periféricos: (inerciales, sísmicos, microfónicos, cinta conductora (foil) balance magnético).

Internas: volumétricos, microondas (MW) infrarrojos (PIR) duales (MW-PIR) ultrasonidos, barrera infrarroja, magnético, presión (almohadilla, alfombra).

Control de Accesos:

Seguridad Física

Cabinas Caseta control
Barreras control
Barreras para bloqueo tráfico rodado.
Exclusas, puertas giratorias, barras antipánico.

Detección

Registro
Detectores metales
Detectores explosivos

Equipos Rayos X
Detectores antihurto.

Control Biométricos

Dispositivos, codificación electrónica (cerraduras, llaves, egonométricas, vídeo portero más audio), sus huellas digitales y egonométricos (mano, voz)

Controles de señalización y control. Transmisión (receptores, radios, marcación telefónica automática, fibra óptica, enlaces microondas.

Transmisión de alarmas Antirrobo, antiatraco regidos por computadores (hardware software) CCTV. servicios de monitoreo. Dispositivos avisadores ópticos - acústicos, emergencia médica. Grabación de eventos (vídeo digital)

Observación y vigilancia:

Sistemas convencionales analógicos y digitales
TV. y CCTV. Cámaras, compuertas, energía, monitoreos alámbrico - inalámbrico, vídeo sensores, detectores movimiento, matrices de conmutación, compresores de vídeo (pan-Tilt, rotores, controles transmisores, receptores señales de vídeo (Dow Lock DICAM) interior, exterior, quad, secuenciales, zoom, proyector infrarrojo, grabación VHS/N digital. Protectores. Sistemas digitales: Cámaras alámbricas e inalámbricas, manejadas por tarjetas que se incorporan al computador desde donde se pueden operar por joysticks o tarjetas, graba todos los eventos en disco duro del PC, fecha, hora y evento.

Visión Nocturna: tubo intensificador de luz, cámaras térmicas, grafos (gogeles), cámara infrarrojas. Binoculares giroestabilizados.

Protección de la Información.

Documentación clasificada: destructores, desintegradores, archivadores de seguridad, sistemas control material calificado. Criptografía, codificadores y decodificadores.

Seguridad de la Comunicación.

Internas: rastreo electrónico para detectar grabadoras, micrófonos ocultos, líneas de corriente, blindaje, salas de conferencia, equipos para destruir interferencias telefónicas, espectro, línea corriente, pares aislados.

Exterior: mezcladores analógicos de voz, encriptado digital (banda estrecha - ancha) datos, cifrado analógico de Fax, encriptado digital de Fax, comunicadores lasércos, cajas de seguridad equipo cifrado, equipos protección tempest.

Seguridad informática: equipo de protección físico. Hardware y Software, controladores de acceso a sistemas.

Protección Contra Incendios.

Sistemas detección, sistemas extinción, centralización alarmas, lucha contra incendios, equipos de protección personal, vehículos, brigadas de incendio, entrenamiento vías de evacuación, pruebas periódicas a equipos. Red de agua, clasificación y aplicación extinguidores. Polvos químicos, señalización.

NORMAS DE DIAGRAMACION E INSTALACIÓN DE DISPOSITIVOS ELECTRÓNICOS

La seguridad electrónica como parte de la seguridad pasiva debe cumplir con varios objetivos:

1. Planificación
2. Sencillez
3. Discreción
4. Inmunidad

Planificación. Se requiere que los dispositivos electrónicos se ajusten correctamente a las necesidades del lugar a proteger. Hay que determinar cual tecnología aplica para cada caso. Sensores para uso liviano pueden descalibrarse en ambientes externos.

Sencillez. Debe procurarse no causar mucho deterioro estético con respecto a los acabados y decoración. Facilitar la instalación de los elementos no significa sacrificar en calidad de materiales o en método de cableado. Los materiales e insumos de baja calidad facilitan el aumento en la vulnerabilidad del sistema.

Discreción. Es necesario que la red de alimentación y señales sea lo más discreta posible. Debe evitarse que el cableado sea visible para impedir que haya sabotajes.

Inmunidad. La instalación apropiada de los sensores reducirá las falsas alarmas lo que dará mayor credibilidad a la compañía vendedora del servicio. La ubicación y orientación de los sensores así como su aplicación tienen un papel primordial.

DIAGRAMACION DE UN DISPOSITIVO DE SEGURIDAD

Las instalaciones de niveles I y II deben planificarse por medio de disponer de dos anillos de seguridad.

1. **Cerco de advertencia**. Este anillo protege al perímetro y la periferia. Es necesario cubrir accesos por puertas y ventajas con sensores puntuales y volumétricos (contactos magnéticos y discriminadores de audio). En la zona de acceso principal (con retardo) no es recomendable usar dos tipos de sensores de diferente tecnología.
2. **Cerco de intrusión**. Este es un anillo interior. Lo conforman principalmente sensores volumétricos y de pánico (infrarrojos, ultrasonido, microondas y sensores de presión). Va programado como zonas instantáneas. No es recomendable ubicar sensores volumétricos en el anillo perimetral.

INSTALACIÓN DE DISPOSITIVOS ELECTRÓNICOS

Es importante determinar como se aplican y cómo se cablean los elementos al panel controlado. Deben considerarse factores como altura, profundidad de campo, orientación y ambiente. Al momento de instalar hay que tener en cuenta:

1. Cable a utilizar
2. Contactos magnéticos
3. Sensores infrarrojos
4. Discriminadores de audio

REALIZACIÓN DE PRUEBAS DEL SISTEMA ANTES DE ENTREGARLO

La Estación Central de Monitoreo espera que se realicen ciertas pruebas que den tranquilidad al operador de éstas. Eviten crear confusión con los códigos que se generen.

1. Llamada previa a la realización de las pruebas
2. Activar todas las zonas
3. Activar señales técnicas
4. Probar tiempos del sistema (aperturas y cierres)
5. Activar clave de apertura forzosa
6. Enviar a la central de monitoreo las fichas técnica y operativa completas para su adecuada inscripción en el software

REALIZACIÓN DE PRUEBAS DE MANTENIMIENTO

La estación central de monitoreo espera que se realicen ciertas pruebas que den tranquilidad al operador de ésta y eviten crear confusión con los códigos que se generen.

1. No activar pulsadores de pánico
2. Activar todas las zonas
3. Activar señales técnicas
4. Probar tiempos del sistema (aperturas y cierres)
5. Activar clave de apertura forzosa

Composición de los sistemas de vigilancia de espacios abiertos.

Los sensores de vigilancia, tal como las instalaciones de comando e indicación, son junto a las instalaciones de infraestructura (arquitectura - ingeniería) los componentes más importantes de cualquier sistema de vigilancia.

Seguridad Periférica. Nuestro objetivo es proveer los aparatos, elementos, productos y servicios para sistemas exteriores de seguridad. Ellos pueden ser desde:

a. Sensores de detección, para reducir el riesgo de robos, intrusión, fugas de cárceles y riesgos donde no es viable un guardián o vigilante;
b. Circuitos cerrados de televisión, donde las cámaras (interiores, exteriores u ocultas) son elementos importantes en la seguridad exterior;
c. Sesores de barrera;

d. Sesores de volumen
e. Sensores orientados a las cercas
f. Sensores de movimiento incorporados a caminos
g. Sensores infrarrojos de corto y largo alcance
h. Sensores de iluminación con luz invisible

De acuerdo a los requerimientos de seguridad para cada caso hay diferentes tipos de aparatos para suministrar la seguridad requerida o integrarlos al diseño y automatización del sistema seleccionado.

Sitios a los cuales podemos proteger.
Instalaciones militares tales como del Ejército, Marina, Fuerza Aérea y de Policía. Incluyen estas instalaciones unidades militares, zonas de parqueo, bodegas, campos de entrenamiento, depósitos de armas y municiones, sistemas de defensa, de comunicaciones, centros de seguridad y complejos especiales. Un sistema de seguridad perimetral incrementa la eficiencia de los sitios de vigilancia y da la respuesta necesaria a estos sitios neurálgicos.

Instituciones correccionales o carcelarias.
Un sistema de seguridad diseñado e instalado eficientemente provee una solución ventajosa para prevenir escapes de los reos y garantiza la seguridad de todo el personal tanto de vigilancia, administrativo como los condenados y los visitantes.

Plantas y Torres de Energía. Tratamiento de aguas, procesos químicos, fábricas.

Agencias y Edificios Gubernamentales
Embajadas, residencias importantes, museos, puede ser con luces de seguridad infrarrojos con capacidad de detección muy superior, conectados a torres de cables blindados enterrados sin comprometer o alterar la apariencia de la residencia.

Aduanas y Fronteras
Para proteger el contrabando y el ingreso de ilegales o terroristas.

Aeropuertos
Para proteger toda el área de aeropuertos, pistas aéreas, zonas de carreteo y parqueo, áreas de servicios de equipajes, almacenamiento y servicios de cargue y descargue, rampas, suministro de combustibles y lubricación, parqueaderos públicos y de V.I.P. Puede delimitarse la aviación general con las operaciones comerciales incluidos los

sistemas de detección de explosivos, armas, drogas y valores (billetes).

Centros de comunicación

Esta es una aplicación de alta seguridad, dados los sofisticados sistemas de interferencia electrónica, lo que permite contrarrestarlos sin afectar los sistemas de comunicación, seleccionando adecuadamente los sistemas de seguridad activos, pasivos, cobertura, volumétricos y sensores en línea, para proteger eficientemente las comunicaciones nacionales, internacionales y los sitios de transmisión.

Edificios comerciales, industriales; de almacenamiento y parqueaderos, con aparatos para detectar perímetros de intrusión, detección de rotura o perforaciones de paredes, pisos y techos.

Aparatos a utilizar y dispositivos de seguridad

a. Sistemas de detección de intrusos en perímetros (DTR-2000 Font wine Intrusión Detection Aystem (TWIDS).
b. El YAEL 15 es la combinación, las propiedades de detección con barreras físicas (vallas, alambrados, cercas), lo más avanzado de alta seguridad en sistemas de detección de intrusos (Detectores de estado sólido) (Nogal Group)
c. Detectores de intrusos y cercas con fibra óptica.
d. Electro-barreras (no letales pero que producen una descarga eléctrica y causa pánico al intruso e inmediatamente transmite una alarma al centro de control o seguridad indicando el sitio de intento de intrusión. Puede combinarse con concertinas.
e. Sensores. Adosados e integrados a cercas o barreras metálicas, detectan cortes, escalamientos o levantamientos en las cercas . pueden integrarse a sistemas computarizados desde puertas, cercas, vallados.
f. Sensores de vibración, volumétricos (perimetrales) de intrusión (cables blindados y enterrados) Crean un campo electromagnético que detecta intrusos (Panther 2000). Sensores de campos electrostáticos, sistemas de protección por microondas (locales, tácticos y estratégicos) TMPS.
g. Sistemas de protección pro microondas, consiste en un transmisor (TX) y en un receptor (RX), para diferentes alcances (50 m a 3000 m). Una línea invisible se establece entre el TX y el RX. El receptor (RX) usa un preamplificador que adecua la señal a procesos en los cuales la transmisión se hace a través de cercas o vallas. Se puede incorporar a un sistema de monitoreo
h. Sensores de microonda tácticos portátiles. Son muy eficientes en diversas aplicaciones tales como parqueaderos de aeronaves, hangares, techos o cubiertas,

situaciones de riesgos políticos. Diseñado para detectar accesos aéreos, al proveer detección volumétrica por radar con rangos de cobertura ajustables e ingreso o egresos seleccionables (desde 22 metros hasta 78 metros. Detecta intrusiones entre 1.6 km/h hasta 96 km/h. Comandos inalámbricos remotos.

Seguridad Perimetral:

Como sensores de intrusión externos y que desencadenan una señal de alarma existen a disposición los siguientes tipos.

1.3.2. Sensores de Superficie:

- Avisador de terreno. Vigilancia invisible (cable enterrado contra intrusos) del terreno desencadena la señal de alarma cuando se intenta pasar por excavación o por encima del sensor (Excalibur trc/3A anexo).

- Avisador de alambradas: o sensores de barreras. Desencadena la señal de alarma cuando se sobrepasa o se intenta destruir una cerca o alambrada metálica (AEG TELEFUNKEN anexo).

- Barrera luminosa (infrarroja); desencadena la señal de alarma al traspasar esta, por ejemplo cercas de protección perimétrica o portones de entrada.

- Campo eléctrico: lámparas por sensor infrarrojo: prende automáticamente al detectar calor (temperaturas 35* a 37*) y movimiento de personas al entrar en la zona y permanece prendida mientras haya actividad en la misma. Se apaga al suspenderse la actividad. Da alarmas acústicas y visuales.
- Mecánicos (inerciales)
- Electromecánicos (geofonicos piezoeléctricos)
- Cable sensible a deformación.
- Sensores de disturbios en campo electrostático

1.3.3. Sensores de Subsuelo

- Sísmicos magnéticos
- Sísmicos piezoeléctricos, presión diferencial, geofonicos)
- Cable radiante
- Cable micrófono lineal 1000 m.

1.3.4. Sensores de Volumen

Aptos para la percepción de volúmenes en el proceso de movimiento que se ejecutan en el interior de ciertas áreas.

- Barreras de microondas (MW)
- Sensores de campo eléctrico
- Sistemas de alarmas de vídeo
- Fibra óptica
- Duales

Para la identificación se pueden agregar a los citados sistemas de alarma los siguientes sistemas de identificación:

- Fotoregistración mediante cámaras automáticas (detector de movimiento)
- Cámaras de televisión, luz día con iluminación.
- Cámaras de televisión, luz día noche (cámaras de luz residual)
- Avisador de alambradas para la identificación acústica.

Todas las señales de los sensores revelación o de identificación que se encuentra en espacios abiertos, serán elaborados por una central de microprocesadores, para mando y evaluación.

Un componente importante de esta unidad de mando y evaluación es la reproducción a escala del espacio abierto en forma de plano de disposición.

Los intentos de penetración serán indicados por señales luminosas en el plano de disposición y por señales acústicas en la unidad de mando. Es recomendable un sistema doble de energía , 110 VAC y 12 VDC con batería y convertidor o transformador y/o fuente de poder.
Como complemento puede registrarse mediante un aparato registrador el sector, fecha y hora del intento de penetración.

En el mismo instante del aviso de alarma mediante la señal luminosa sobre el plano de disposición, será puesto en funcionamiento el correspondiente sistema de identificación en ese sector. Al utilizar sistema de televisión se reproduce la imagen de la escena en un monitor en la central, de tal manera que el personal de vigilancia sin la presencia en

el lugar de los hechos pueda tomar decisiones con respecto a las medidas apropiadas para la defensa.

(AEG TELEFUNKEN, anexo, Stellar System, anexo, Guardwire anexo)

UNIDAD 2. SUBSISTEMA DE CIRCUITO CERRADO DE TELEVISION.

C.C.T.V. es quizás el mejor medio de supervisión, de producción y vigilancia, siendo un excelente medio disuasivo para el control a propios y extraños dentro y fuera de la Empresa. Actualmente los CCTV. proveen más detalles en la resolución y una imagen más clara, inclusive en condiciones mínimas de iluminación, pues antes estaban diseñados y construidos con tubos y ahora trabajan con procesador electrónico C.C.D. Chip, de casi seis veces de más duración y menor tamaño. Un circuito de 16 cámaras puede registrar todos los eventos en una vídeo grabadora durante 40 días continuos sin necesidad de cambiar la cinta o con activación automática por sensores de movimientos o señales de alarma. También puede transmitir en vivo y al instante a través de línea telefónica (Down Look) celular, móvil o fijo, y radio frecuencia En equipos de radio VHF, UHF o HF. Adicionalmente permiten grabar en el disco duro de un computador o Diskette e imprimir cualquier imagen grabada (TeleSite, Dicam Anexo).

Las nuevas microcámaras C.C.D. poseen las mismas características de las cámaras regulares, tienen un lente PINHOLEy su tamaño es tan solo de 31 mm x 10 mm que facilita su mimetización en cualquier objeto de uso diario en empresas o viviendas. Puede hacercen en gafas, relojes, beepers, corbatas, carteras, etc. y con transmisores inalámbricos alimentados por una pila cuadrada, de 9 V DC de uso corriente o con batería recargable, envía señales de audio hasta de 500 mts.

Las CTV han ido evolucionando en una forma rápida y gracias a las nuevas tecnologías de los microchips y la informática, se han reducido en tamaño y precios; los primeros sistemas eran de grandes volúmenes donde se debían ubicar varios tubos para sus diferentes implementaciones, luego con el micro chip esos fueron eliminados, se redujeron notablemente en tamaño y se pudieron incluir una serie de funciones que con los elementos iniciales no se podían hacer tales como lentes pinhole, rotación, paneo horizontal y vertical (pan/tilt), ***** de pantalla (quad), secuenciador. La última tecnología de informática ha incorporado a los computadores las funciones de pan/tilt, zoom, grabación en el disco duro, con las diferentes imágenes presentadas en el monitor del PC y con la**

reproducción en papel a través de la impresora la toma inmediata, si así lo requieren y con la mejor calidad.

CTV. Sistema de Vigilancia por Video Digital

DMRS, DICAM, TELESITE, DOWN LOOK, G-VISION
Son sistemas completos de vigilancia por video digital, verificación de alarmas y almacenamiento de imágenes digitales.

Los sistemas ofrecen una funcionalidad y flexibilidad única con vigilancia por video tanto local como remoto, alarma y almacenamiento de imágenes para cualquier instalación de CCTV.

CONTROL SOFTWARE
Software para Windows 3.1 x Windows 95 controla hasta 4 puertos simultáneamente en un PC estándar.

Las imágenes pueden ser desplegadas en pantalla completa, dividida en cuatro o dieciséis.

El manejo de las alarmas se lleva a cabo totalmente automático; las alarmas se despliegan sobre la pantalla en tiempo real. Una vez atendida la alarma (de manera automática o manual) el control se revierte a la pantalla principal. El sistema maneja múltiples alarmas simultáneas en un solo PC.

Las imágenes pueden ser tanto almacenadas como reproducidas en el disco duro del PC, en la memoria dentro de la unidad.

RECAM/DI con o en la unidad DI LAPSE. El almacenamiento digital permite la búsqueda instantánea de imágenes por fecha, tiempo, alarmas, lugar/cámara, etc.

Es posible realizar búsquedas, visualizar, mejorar (contraste de luz y zoom digital), imprimir, enviar por fax, exportar y almacenar las imágenes desde el software directamente desde el lugar o vía MODEM en el caso de que la unidad esté conectada remotamente.

Unidad de Transmisión de imágenes digitales y control de alarma
Pueden ser transmitidos por:

- Líneas ordinarias PSTN
- Líneas digitales ISDN
- Teléfonos celulares (CDPD)
- Enlaces de radio
- Enlaces de satélite
- Fibra óptica, etc.

Puede transmitir imágenes de tiempo real comprimidos e imágenes almacenadas. Opcionalmente ofrece un conmutador (joystick) de video para control de vigilancia local y una conexión a una unidad Dilapse para almacenamiento digital indexado por hora y fecha.

Grabación tiempo lapsado
Grabados compacto digital con unidad de respaldo en cinta digital opcional para almacenamiento de imágenes de video digital desde una unidad RECAM o DICON. Es virtualmente libre de mantenimiento.

Una unidad se conecta directamente a una unidad RECAM o DICON y almacena de 250.000 a 500.000 imágenes.

En la actualidad hay sistemas de video digital que pueden controlar hasta 250 cámaras con un solo sistema. Ejemplo: en las Vegas, los grandes hoteles con casinos y múltiples salones de máquinas y juegos diferentes, el centro de monitoreo opera, maneja, dirige, supervisa de 600 a 1200 cámaras, con la posibilidad de ampliación del sistema y todas las funciones de operación (paneo horizontal, vertical, zoom, rotación 360, grabación, exhibición, almacenamiento, quad, secuenciador, revisión eventos anteriores, combinarlos comparativamente, ingreso y egreso activos, ejemplo: Película Ojos de Serpiente con Nícolas Gage).

Con el uso de tarjetas para instalación al computador se pueden manejar hasta 116 cámaras en forma simultánea y manejarlos en forma individual de acuerdo a las necesidades de uso de cada una de ellas.

CCTV DIGITAL

Cómo funciona el sistema CCTV DIGITAL?
Se interconecta una tarjeta en el computador con capacidad para 4-8-12-16 o más cámaras a los cuales se conectan para sus funciones (Ejm: Sistema DMRS, Digital

Monitoring Record System) y con la aplicación del software respectivo se puede manejar desde el PC con el sistema operativo Windows 98; el tiene la facilidad de llevar al monitor el audio y video de cada cámara a través de cableado (coaxial o fibra óptica o UTP), con el fin de ampliar sus funciones de operación. Hay otra tarjeta TPZ que sobre una cámara fija le da funciones de pan/till y zoom. A través de un MODEM, el DRMS le informará y hará ver a ustedes lo que está sucediendo en cada cámara, ya sea vía telefónica, teléfono móvil, celular, beeper, trunking. Mientras tanto el sistema almacenará imágenes en su disco duro para que puedan ser vistas cuando usted lo quiera y los pueda imprimir por fecha o por eventos.

Diferentes software CCTV Digital
Telesite USA INC
GSN VIDEO (Global Security Network)
MICROKEY Software Inc.
DRMS Software
SENSORMATIC SECIRUTY SYSTEMS
DICAM
KALATEZ
ELECTRONIC LINE
TELESITE

2.1. Cámaras, Monitores y Vídeo grabadoras.

Hay diferentes tipos de cámaras de acuerdo a las necesidades, hay a color, en blanco y negro, de alta sensibilidad para un mínimo de iluminación a 0,001 lux, construidas con controles electrónicos de luz para usar con lente auto iris fijo, aceptan también lentes de vídeo tipo auto iris, pueden operar a 12 VDC o a 24 VDC o 110 VDC, con alarmas incorporadas o detectores de movimiento; viene básicamente en medidas referenciales para formatos de 1/3, de 2/3" y de 1", y en la mayoría de los casos vienen sin lentes. Con las medidas anteriores se seleccionan dichos lentes por sus ángulos y focos: gran angular, angular super ancho, estándar, varifocales, semi telefoto, teleobjetivo, zoom, vienen también con selectores de velocidad de 1/60 hasta 1/10.000 segundos. Es necesario seleccionar, de acuerdo a especificaciones de catálogo (anexo) la compatibilidad de cada una de las funciones a realizar de acuerdo a su uso y ubicación.

2.2. Monitores.

Igual como las cámaras, hay pantallas en blanco y negro, a color, desde 4 pulgadas hasta 54", para casos especiales aceptan proyectores sobre pantallas o ecran. Las más usadas son de 9", cuando se usan para la recepción de hasta 4 CCD, para mayor número son las de 12" y pueden ser actividades y operadas manualmente o por secuenciador. Para casos especiales y de mucho control es recomendable varias cámaras en una consola central. Su eficiencia la determina la línea de resolución central de 300, 480, 700 y los pixeles horizontales y verticales. Normalmente viene con los controles en el frente y con soporte para montaje a la pared. Tienen límites en el número de cámaras que pueden recibir, pero hay adaptadores para ampliar su capacidad.

Para un eficiente control del sistema CCTV, es recomendable centralizar la recepción de audio y vídeo en un centro de monitoreo, donde el personal encargado y responsable de su operación, tengan no solo los monitores, si no también los aparatos complementarios para su manejo, tales como control remoto de pan/tilll (horizontal y vertical), de zoom (acercamiento), secuenciadores, quad (división de pantallas) vídeo grabadoras, impresoras, o con los nuevos sistemas computarizados, equipos de recepción y software especiales para pasar el vídeo del monitor al computador, grabarlo en disco duro o diskette o imprimirlo (MULTISCOPE).
Al diseñar un sistema de CCTV, se deberán tener en cuenta diferentes items, cada cual más importante.

Cámaras Exteriores: Ubicación, protector (housing) soporte, seguridad de la cámara, conexión, fuente de energía, tipo de lente foco, luz. Formato autoiris, control temperatura.

Cámara Interiores: Ubicación, blanco y negro o color, tipos de lentes, auto iris o estándar, formato, sensibilidad, resolución, pixeles, soportes, fija o móvil, con motor para zoom y pan/tillt, fuente de energía, consumo, tipo de acople, co cs, para el montaje del lente, sensor de movimiento, inmunidad a golpes o vibraciones, peso, encendido o apagado automático, memoria, conexión al monitor o inalámbrica, y número de cámaras CCD, detector de movimiento.

Monitores: Sitio de trabajo, sensibilidad resolución, formato, número de cámaras que aceptan, fuente de energía consumo, alámbrico o inalámbrico, compatibilidad con las

cámaras blanco y negro o color soporte para montaje, controles de operación (brillo, contraste, color, posición horizontal, vertical) transformador de voltaje. Los últimos modelos vienen con secuenciador incorporado.

2.3. Lentes.

El lente juega un papel importante en la optimización del rendimiento del sistema de CCTV. Lentes con formato de, 1/3", 2/3", y una 1" con monofoco manual, autoiris automático zoom, varifocal, y motorizado (cuadro anexo de especificaciones y equivalencias).

2.4. Equipos Auxiliares.

2.4.1. Secuenciador:

Unidad que selecciona manual o automáticamente paso de la imagen del vídeo de diferentes cámaras a un mismo monitor.

El tiempo es graduable entre 0.2 segundos a 60 segundos. Hay secuenciales que pueden transmitir la imagen de 4,6 y hasta 24 cámaras a un solo monitor. Algunos vienen con alarma.

DIVISOR DE PANTALLA

2.4.2. QUAD

Equipo que permite partir la pantalla en 4,6,8,9,16 cuadrantes de acuerdo a la marca. En caso de alarma lleva a la pantalla plena la imagen de lo que sucede, varios tienen zoom.

2.4.3. Vídeo Grabadoras

Los hay en blanco y negro, a color, tiempos de grabación automáticos de 2 a 960-1920 horas, formato en VHS, hora/fecha incluida, velocidad de control y memoria, graban desde 1 hasta 99 imágenes, de una cámara a más de 12 cámaras, adaptadas a 12 VDC programables para grabar desde 2 segundos al activarse la alarma de tiempo

lapsado.

2.4.4. Conmutadores/Controladores

Incorporan controles automáticos a secuenciadores, Pan/Tilt, zoom desde 8 cámaras hasta 2048 cámaras y pares, ubicación de eventos rápidos o lentos, control de rotores.

2.4.5. Iluminadores Infrarrojos

Desde 6,3 vatios hasta 1000 vatios, para interiores o exteriores, con voltajes de 12 VDC, a 110 VAC.

2.4.6. Protectores (housing)

Para la protección de las cámaras CCD en usos exteriores, evitan la humedad haciéndolas impermeables. Hay de diferentes tipos y formas, lo mismo que pesos lo cual debe ser considerado para seleccionar el soporte o base de anclaje. Pueden escogerse discretas como l□mparas o faroles o domos térmicos

2.4.7. Rotor y Control

Este elemento consiste en un pequeño motor que permite el giro de la cámara en forma horizontal con un ángulo hasta 355 grados a través de un control de rotor manual o automático.

2.4.8. Amplificador de Vídeo

Cuando hay grandes instalaciones o distancias entre cámaras y el centro de monitoreo, se debe usar el amplificador el cual genera una alta ganancia en vídeo y audio al recuperar la resolución pérdida por el cableado. Asegura una imagen clara en la pantalla todo el tiempo, sistema a color compatible con NTSC y el PAL.

2.4.9. Pan / Tilt - Zoom

Son los aparatos que al interconectarse con las cámaras CCTV permiten manual o automáticamente o a distancia moverlas lateralmente (Pan) verticalmente (Tilt) y acercar o alejar (zoom) la imagen captada por la c□mara.

2.5. Sistemas de Transmisión de Audio y Vídeo a Computador (DICAM)

Gracias a las últimas investigaciones y desarrollos tecnológicos, se han diseñado y fabricado equipos de transmisión de las imágenes captadas por cámaras CCD a través de línea telefónica vía RF (radio VHF, UHF, HF) celular móvil o fijo a un equipo de CDPD recepción interconectado a un computador con un Software permitiendo ver en el monitor, grabar en el disco duro o diskette y oír el audio captado en el lugar de los hechos, y luego imprimir las imágenes necesarias o programadas en la impresora correspondiente. Pueden quedar en diskettes como reportes de actividades y controles de vigilancia.

Con los recursos económicos y equipos anteriores necesarios, se puede diseñar y configurar un sistema CCTV, totalmente confiable y eficiente.

2.6. Equipos Inalámbricos

Los sistemas de CCTV inalámbricos ofrecen lo último en tecnología audio vídeo. La cámara de CCD tiene un micrófono incorporado y un lente gran angular, el cual ofrece una excelente imagen aún en lugares oscuros, puede dar imagen en casi oscuridad total. El monitor portátil puede ser trasladado a oficinas, almacenes, bodegas, a exteriores, ofreciendo rápida libertad de movimiento y audio y vídeo inmediato. Hay sistemas que ofrecen la posibilidad de conectarse a un televisor comercial para obtener una imagen en pantalla grande.

ANEXO B

UNIDAD 3. SISTEMAS DE CONTROL DE ACCESO

Los altos costos operacionales de los sistemas convencionales, la limitada confianza y responsabilidad del personal encargado (vigilantes y porteros 24 horas) sumados a la imposible supervisión de los mismos, hace indispensables los sistemas de control de acceso, manejados independientemente o por computadores con un programa de fácil operación y m□xima seguridad, restringiendo cualquier mala utilización ya que posee diferentes niveles de accesos controlados por códigos (Password).

3.1. Diferentes Tipos de Control de Acceso

El sistema de control de acceso permite el manejo seguro del ingreso del personal en áreas restringidas. Su facilidad de manejo y alta eficiencia son las características que deben tener en cuenta.

3.2. Componentes de Controles de Acceso

LECTORA SIN TECLADO

LECTORA CON (PUERTAS CAJEROS)

TECLADO (CAJEROS)

LECTORA SIN TECLADO = PUERTA CAJEROS

Boca adicional

LECTORA CON TECLADO = EXPENDEDOR DE DINERO

Banda infrarroja / Magnética / Aproximación

TARJETA STANDAR
Banda infrarroja
Banda invisible
Banda magnética
Banda por aproximación

LECTORA DE SALIDA 3A

3.3. Seguridad Física

- Vigilantes
- Cabinas - casetas de control.
- Barreras de control.
- Barreras de bloqueo de tráfico rodado.
- Esclusas
- Barras antipánico
- Puertas giratorias y de molinete (esclusas)

3.3.1. concertinas
3.3.2. vallados Metálicos
3.3.3. Cámaras Acorazadas
3.3.4. Cerraduras, Candados
3.3.5. Cristales Blindados
3.3.6. Puertas Blindadas / Automáticas
3.3.7. Vídeo - Porteros

3.4. Detección y Registro

3.4.1. detectores de Metales (Manuales guantes)
3.4.2. detectores de Explosivos
3.4.3. Detectores de Rayos X
3.4.4. Detectores de Antihurto
1.4.5. Detectores Carta Bomba
1.4.6. Sillas detectoras partes íntimas (Boss)

3.5. Controladores Electrónicos

3.5.1. Lectores de Tarjeta de Código de Barras, Infrarrojo (ir) de Alta Seguridad

(invisible)

3.5.2. Tarjeta de Barras Magnéticas(PTA. CAJEROS)

3.5.3. Controles de Teclado Para Digitar Claves Personales en Areas de Alta Seguridad.

3.5.4. Sistemas de Aproximidad

3.5.4.1. Sistemas de control de acceso por aproximación sin contacto (tarjeta de aproximación y el lector de aproximación)

3.5.4.2. Sistema de (transmisión digital) interpreta el código de la tarjeta para permitir el ingreso del personal autorizado.

Características Técnicas

Los controles de acceso básicamente constan de las siguientes partes.

- CPU. PRINCIPAL. Con 64 k de memoria EPROM 64 K. de RAM, IBM para las autorizaciones 20 MB para el archivo de movimiento y reloj de tiempo real para manejo de autorizaciones y la red de comunicaciones con el computador.
- Interfase de comunicaciones RS 232.
- Puerto de comunicaciones de protocolo especial.
- Fuente de alimentación.
- Backup de batería para la memoria RAM y reloj del tiempo real.
- Controles de acceso (con teclado y sin teclado)
- Control de salida.
- Controlador de acceso múltiple SCAM.
- Software adicional, opcional solo cuando instalen SCAM.
- Sistema administrador de tiempo ELECTIME modelo de liquidación de tiempo. Modelo control cafeterías.
- Cantonera para puertas.
- Electroimán impulsador cierre y apertura
- Tendido de cables y ductos.
- Softime.
- Interfase entre el computador y reloj.

3.6. Sistemas de Accesos Biométricos que Identifican Personas.

Técnicas de seguridad que utiliza las características o rasgos del comportamiento humano para distinguir un individuo de otro.

3.6.1. Exploración dactilar
3.6.2. Escaneo de iris/retina
3.6.3. Volumétrico
3.6.4. Análisis de voz
3.6.5. Geometría de la mano (egonométricos)
1.6.6. Firma
1.6.7. Reconocimiento facial
1.6.8. Otros sistemas biométricos exóticos: exploración del cuerpo humano, patrones de venas de la mano, reconocimiento oreja y olor corporal

CUIDADOS E INSPECCION

- Estado físico de cada sensor, soportes y montajes.
- Cableado y ductos.
- Apariencia externa del sensor, unidad de control, conexiones, equipos, y accesorios.
- Fuente de energía, electricidad, convertidor, (cargador) batería.

LIMITACIONES: COSTO - BENEFICIO

Tarjetas +/- us $1000 por puerto
Huella dactilar + / - us $3500 a 6000
Escaneo de iris/retina + / - us $4500
Análisis de voz + / - us $1200
Geometría de la mano + / - us $2100

SOLO PARA TUS OJOS
De la ciencia ficción a la realidad: la identificación por el iris.

El desarrollo de las máquinas IRIOSCOPICA se debe a dos oftalmólogos que trabajan actualmente para la empresa IRIS CAM en Monut Launel New Jersey, USA, son Leonard Flom y Aran Safir igualmente se trabaja en esta nueva técnica en Inglaterra y en el Japón la firma OKL quien ha ganado el liderazgo de los avances de esta novedosa técnica de identificación.

Los doctores Flom y Safir demostraron que el complejo patrón de estrías y estructuras fílmicas del iris, ofrecen un método de identificación más preciso que el sistema

dactiloscópico actual que se basa en el conjunto, relativamente más sencillo de espirales y curvas que se encuentran en una huella digital. Las formas que se hallan en el iris de una persona, incorporan 260 valores independientes, en tanto que las huellas digitales solo contienen cerca de 35. por otra parte, el exclusivo patrón de líneas del iris no se altera en el transcurso de la vida de la persona, como si lo hace el diseño de las huellas digitales y otros factores biométricos, como pueden ser las líneas de los nudillos, el timbre de la voz y los olores corporales. Adicionalmente, el iris es una de las partes más visibles del cuerpo y gracias a ello, puede ser fácilmente revisado por una cámara.

El desarrollo que permitió convertir esa idea en una tecnología fue un conjunto de fórmulas patentadas por John DAUGMAN en la Universidad de Cambridge en 1994. dichas fórmulas le permiten a una cámara de video localizar el iris en la imagen de un ojo y luego escudriñan la estructura textural de dicho iris, codificando sus rasgos distintivos en una pequeña "forma" electrónica que es almacenada en un archivo de computador para su futura referencia. Cuando se requiere identificar a una persona, el sistema simplemente selecciona el item del archivo de referencia que corresponde a la fórmula detectada en la persona que se quiere identificar.

Al ser tan pequeños (tiene 256 bytes, es decir, menos información que la que hay en este párrafo) los códigos microscópicos del doctor DAUGMAN utilizan poco espacio en la memoria del computador, gracias a ello se facilita la búsqueda de archivos. Utilizando un PC personal estándar pueden compararse 100.000 registros por segundo y la tasa de error es menos de uno en 100.000. semejante exactitud parece ser cientos de veces superior a la de los demás medios biomédicos de identificación.

Se ha licenciado dicha tecnología a las firmas IRISCAN, SENSAR y OKI del Japón. Por eso es que esta manera rápida y amigable de verificar la identidad de una persona podría ahorrarle sendos problemas a muchos.

TERMINALES DE COMPROBACIÓN DE IDENTIFICACIÓN DE HUELLA DIGITAL

El sistema utiliza verificación biométrica (cada firma tiene su patente) para proveer identificación personal irrefutable, solo personal autorizado tiene acceso permitido a áreas restringidas o el registro de entradas o salidas.

VENTAJAS Y CARACTERÍSTICAS

- Asegura rapidez y fácil acceso al personal autorizado
- Elimina el registro hecho pro compañeros

- Verifica positivamente la identidad del usuario sin necesidad de tarjetas, códigos, insignias, llaves u otras formas de ID.
- Cualquiera de los 10 dedos pueden registrarse
- Programación de 30 restricciones de zona por día
- Ideal para ubicaciones remotas o no supervisadas.
- Registra el tiempo de cada persona que llega o sale; el sistema no se puede engañar
- Genera y mantiene un registro de tiempo de todas las transacciones
- Opera en modo autónomo o en configuraciones de red
- Fácil configuración y operación directa en el terminal o mediante conexión al computador
- Maneja cualquier combinación de cinco de puertas, señales audibles, alarmas y otros dispositivos.
- Alarmas para "apertura forzada de puerta" "puerta abierta" e "intentos de impostor". Dispara alarmas audibles, luminosas, cámaras y otros dispositivos.
- Puede usarse conjuntamente con tarjetas magnéticas, "SMART CARD", tarjetas de proximidad o lectores de código de barras.

En los Estados Unidos se cuenta actualmente con un sistema automático de identificación de Huellas Digitales (AFIS) con más de 4.8 millones de huellas de sospechosos, convictos, fugitivos, etc., inclusive este nuevo sistema permite "leer" las huellas digitales de una persona, un documento de identificación, de una licencia de conducción, de un pasaporte, escaneado electrónicamente y transferido en segundos a este banco de datos, comparado, verificado, detectado y devuelve la identificación del individuo, por la misma vía (celular, CDPD, radio o telefax movil). Lo están usando los policías de tráfico de carreteras, aeropuertos.

Es un aparato simple y rápido en su uso, el costo de cada aparato es más barato que otros sistemas biométricos de identificación, es resistente al vandalismo, utiliza la glometría del dedo no la impresión de la huella, no requiere limpieza ni programación de mantenimiento preventivo. Incluye el desgaste por el uso constante ni contaminación por largos períodos de uso. La interfase es a través del RS 232/ o 422/ o 485 de puerto serial, puede ser conectado en serie con otros 125 aparatos del mismo tipo y clase, capacidad para 8000 datos, tiempo de lectura menos de 30 segundos y tiempo de verificación menos de 2 segundos

ANEXO C

UNIDAD 4. SUBSISTEMA DE TRANSMISION

En la actualidad los sistemas de transmisión tienen más aplicaciones que la tradicional transmisión de conversaciones, por ejemplo, por medio de los modems los datos y señales de alarmas de los bancos, fábricas, bodegas, etc. son transmitidos por el mismo equipo telefónico. Además de la red pública de transmisiones y telecomunicaciones existen sistemas privados dentro de los diferentes sectores bancarios, comerciales, industriales, militares, policiales, etc.

En nuestra red pública mezclamos la transmisión con las telecomunicaciones con instalaciones de señalización, intercomunicación con conexiones para computadores y su equipo periférico, etc. La información es distribuida por la red y recuperada en los extremos, usando terminales o impresoras.

Una gran ventaja de la transmisión de datos es la ofrecida por el sistema DATEX en el cual un equipo de computación comunica los datos a través de su propia red en forma automática.

La evolución continua de la tecnología permite que cada equipo nuevo sea producido con mejores técnicas y se apegue a los más estrictos requisitos de transmisión. En este campo el desarrollo esta en progreso continuo, el ejemplo más obvio hoy en día es el cable de fibra óptica.

4.1 Sistema de Transmisión

Un solo cable puede ser usado para diferentes tipos de información, y la transmisión de estos se realizan utilizando varios sistemas, por ejemplo, se puede diferenciar entre un sistema de transmisión de canal sencillo y un multicanal.

4.2. Sistema de Canal Sencillo

Originalmente los sistemas de transmisión eran únicamente del tipo de canal sencillo o sea que solo podría transmitir una conversación telefónica o un mensaje telegráfico a la vez en la misma conexión física. Así, se tendrán mayores requerimientos de transmisión, el número de conexiones deberá ser aumentado correspondiente.

Este sistema es el más común para transmisión a distancia cortas, tales como redes telefónicas, públicas, locales.

4.3. Sistema Multicanal.

En redes de transmisión para largas distancias, por razones financieras, se decidió utilizar las conexiones que brindarán un óptimo rendimiento, inicialmente fue la FANTONIZACION el cual balanceando cuidadosamente un cuádrete (cuatro conductores aislados individualmente y torcidos) podrían transmitir una conversación adicional, dando un total de tres conversaciones.

Los sistemas de frecuencia portadora son considerablemente más poderosos. Están basados en una mezcla de señales telefónicas originadas moduladas con varías frecuencia portadoras, de tal manera que puedan ser acomodadas una sobre la otra en términos de frecuencia. Como estos sistemas utilizan la división de frecuencia, se les denomina sistemas FMD (multiplexación por división de frecuencia).

En los últimos años la técnica digital ha hecho su aparición dentro de la tecnología de transmisión en la forma de sistemas PCM (modulación codificadora de pulsos). Estos sistemas cortan cada transmisión un gran número de periodos los cuales pueden ser detectados electrónicamente y codificados por medio de pulsos digitales; estos son condensados junto con los pulsos de otras transmisiones y transmitidos a una gran velocidad a través de cables multipares o coaxiales. Ya que estos sistemas son de división de tiempo, son llamados sistemas TMD (multiplexación por división del tiempo).

Tipos de cables: Se pueden clasificar de acuerdo a la forma o estructura del conductor.

Cables Multipares: Un cable par como lo indica su nombre, se caracteriza por tener dos conductores que forman un enlace entre transmisor y receptor.

Cables Coaxiales: Es diferente al multipar en su estructura, y esta constituido por uno o más tubos coaxiales, los cuales a su vez están formados por dos conductores, uno tubular y otro filiforme, colocados en el mismo eje, y están aislados uno del otro por polietileno, o por una combinación de aire con polietileno.

Su aplicación es para la transmisión de banda ancha de frecuencia y es utilizado en varios sistemas múltiplex, ya sea F D M o T D M.

Cables Para Conexión: Son los indicados para instalaciones de alarmas, tienen una cubierta de plástico. De varios tipos. Para ciertas instalaciones se requieren cables blindados y de coaxiales flexibles, para mejor protección contra las interferencias, además son fáciles de manejar.

Cables de Señalización: Llamados también de instrumentación y de control. El factor común es que las señales enviadas entre dos puntos deben llegar sin ser distorsionadas o deformadas. Si por ejemplo en un proceso de monitoreo, la distorsión o interferencia puede causar que el monitor electrónico registre otro valor, y no solo el enviado, ocasionando que el sistema efectúe la acción equivocada.

Cables Opticos: Uno de los avances tecnológicos de esta era, es el desarrollo de las técnicas de transmisión por cable ópticos. Este utiliza fibras ópticas del grosor de un cabello para transmitir señales en forma de pequeños pulsos de luz. Es completamente insensible a las interferencias electromagnéticas y pueden ser construidos para que no conduzca corrientes a tierra.

Existen tres tipos de fibras:

Fibras de índice escalonado, fibras de índice gradual (ambas son fibras multimodo) y fibras monomodo. Son apropiadas para muchas aplicaciones, en especial larga distancia, en troncales (líneas principales) en redes de televisión por cable sistemas de control remoto y principalmente para transmisión de banda ancha.

Instalaciones de Alarma Contra Robo

La instalación de los cables constituyen una parte muy importante en la función de la alarma, por esta razón, los cables deberán ser guardados dentro del área protegida por

la alarma. En caso contrario deberán colocarse en tubería (ductos) protectora.

En cuanto a las instalaciones de alarma existe una marcada preferencia en favor de las instalaciones computarizadas de vigilancia. La selección de los cables realiza con las mismas bases como para cualquier otro equipo de computación. En los grandes centros de alarmas hay además un gran número de instalaciones CCTV para vigilancia, cuyas señales deberán ser transmitidas desde las cámaras de T.V. controladas a distancia.

Las centrales de recepción, los circuitos cerrados de T.V. y el control remoto, son aplicaciones en que la señal de vídeo es transmitida entre diferentes instalaciones. Varios tipos de cable coaxial son generalmente usados para este tipo de equipos.

UNIDAD 5. SUBSISTEMAS DE ALARMAS

En las unidades anteriores hemos visto:

1. Sistemas de intrusión
2. Subsistemas de CCTV
3. Subsistema de control de acceso
4. Subsistema de transmisión

En cada uno de ellos se ha mencionado y concluido que los sistemas complementarios y más confiables de todos son los subsistemas de alarmas centralizados en un centro de alarmas y monitoreo con servicio 24 horas, desde donde puede prevenir, detectar, identificar, localizar el sitio exacto y tomar las medidas de reacción, vías necesarias contra cualquier evento o situación anormal dentro de la empresa.

Los centros de alarmas cumplen funciones de detección, alarma y reacción:

1. Por acercamientos o amenazas de ingreso desde perímetros exteriores.
2. Ingresos a través de los puertos de control por la fuerza o por la falsificación de las tarjetas o elementos de control.
3. Ingresos a áreas prohibidas por personal ajeno y sin autorizaciones.
4. Intentos de robo, substracción o sabotaje en áreas de bodegas, línea de producción y almacenes. Con armas o engaños.
5. Inicio de fuego en oficina, áreas de producción, almacenes de materias primas o productos terminados.

6. Intentos de robo y fuga del perímetro interior. Escape.

Todos los sucesos anteriores pueden y deben ser detectados y anulados, gracias a los diferentes aparatos electrónicos que oportunamente, gracias a estudios, diseño e implementación fueron instalados para tal fin, de acuerdo a sus funciones:

1. Actúan los sensores de superficie que a través de cables enterrados transmiten dichas señales. Igualmente los avisadores de alambrados que día y noche cumplen su función y transmiten el intento de penetración mediante corte o ruptura de la valla exterior. Su comunicación se hace por cable enterrado y ductiado.
2. Los controles de acceso detectan y detienen a quienes no porten las tarjetas de identificación, activen los códigos en los teclados o que con tarjetas de otras personas tratan de violar las garitas y personal o sistemas electrónicos de vigilancia. Así mismo en caso de atracos por la fuerza y que con armas traten de ingresar a la empresa.

3. Los dispositivos de seguridad. Tales como sensores infrarrojos pasivos, sensores de movimiento, sensores de volumen, cámaras de CCTV camuflados o visibles que con detectores de movimiento incorporados activan su funcionamiento produciendo señales de un centro de recepción de audio y vídeo, graban el evento y pueden imprimir las fotografías correspondientes.

4. Los sensores infrarrojos pasivos, los sensores de movimiento, los sensores de microondas, los sensores de superficie, producen la señal de alarma que es llevada en forma alámbrica e inalámbrica al centro de recepción de señales. La alarma puede ser recibida y detectada con sistema acústico o visual para que el responsable del centro de recepción de señales de alarma o CENTRO DE MONITOREO, tome inmediatamente las medidas para las cuales ha sido entrenado previamente, ya sea avisando a las patrullas de vigilancia de la propia empresa, activando sirenas o medios acústicos o de bloqueo a las actividades de los ladrones. Avisa a la autoridad para el apoyo y medidas policiales que pueden efectuar.

5. El fuego puede ser detectado por sensores de partículas pesadas, sensores de humo, detectores de ionización detallada y transmitidos vía alámbrica o inalámbrica a su centro de recepción de señales o centro de monitoreo, traduciendo señales acústicas y visuales a aparatos de control, indicadores de

ubicación detallada para cada situación y los equipos.

Ellos son situaciones manuales que sobrepasan a la sección del mecanismo de tiempo y activan los sistemas de alarmas.

Generalmente se instalan sistemas inteligentes que tienen la particularidad al poseer memoria de cada uno de los elementos a instalar, su posición e identificación de los componentes del sistema y zona en la cual se genera la señal. Lo anterior se resume en: tablero de control inteligente, detectores de humo, iónicos fotoeléctricos, estaciones manuales, luces rotatorias o intermitentes (de destello).

6. Actúan los sistemas de esclusas, puertas automáticas electrónicas (de cierre o apertura) barricadas o cilindros, cerraduras electromagnéticas, puertas blindadas, barreras de parqueadero (dispositivo de piso).

En resumen, todas las señales llegan al centro de monitoreo donde a través de sistemas de alarma acústicos y visuales, indican la zona del evento, y el operador responsable del centro, ve, oye y sabe el sitio exacto de la alarma, para tomar inmediatamente las medidas de reacción, con el personal asignado para tal fin como de vigilancia o con el personal de la misma empresa que previamente se ha designado para tal fin como de vigilancia o con el personal de la misma empresa que previamente se ha designado y entrenado para proceder a neutralizar el motivo de la alarma.

Como vemos anteriormente, el centro de monitoreo o recepción de alarmas es el centro neurálgico de la seguridad de la empresa y es por ello que su diseño, selección, evaluación, montaje y operación de equipos, así como las medidas de reacción, son la prueba de fuego para el administrador de seguridad responsable del manejo y eficiencia del sistema general de alarmas.

ELEMENTOS BÁSICOS NECESARIOS PARA INSTALACIONES

- Juego de guías para cables
- Guía Telescópica (para halar cable)
- Cables de cobre 4 conductores cal. 22
  de cobre 2 hilos (2x22)

de cobre 4 hilos (4x22)
Multiplexado de 8 hilos

- Brocas de ¼" ∅ x 12"
  3/8" ∅ x 12"
  ½ " ∅ x 12"
  3/8" ∅ x 54"
  3/8" ∅ x 12"
- Protector de voltaje. Control electrónico de Relay – salida sinosoidal – voltaje de salida sin distorsión (Protección Vs- Corto circuitos y sobrecarga salida de voltaje 117 ± 5% VCA
- Transformadores de pared telefónico 12 a 24 VA (par sencillo – 2 pares – 6 pares

Central de Monitoreo y Alarmas

Es el lugar físico donde se concentran las terminales y equipos de recepción de alarmas. Básicamente esta constituido por: supervisor responsable o digitadores de turno.

1 computador
1 equipo de recepción y de codificación de señales
1 impresora
1 sirenas (cornetas) para alarmas de robo o fuego.
1 sistemas de comando y controles remotos para activación de conexión y comunicación a las patrullas de vigilancia propios, de la policía o bomberos, de acuerdo a la alarma y su verificación.

- Sensores infrarrojos pasivos, de movimientos volumétricos
- Switches magnéticos para puertas liviana o pesadas
- Botones de asalto tipo bancario o pánico.
- Botones (alámbricos o inalámbricos) para supervisores de seguridad.
- Transmisores digitales alfanuméricos para identificación de personal autorizado de apertura o desactivación o cierre de puertas y activación de alarmas.
- Líneas telefónicas con marcadores automáticos (diales).
- Botones electrónicos para control de rondas de vigilancia.
- Radioteléfono o central de radio / celulares
- Sistemas duales de energía (electricidad AC o baterías DC) con transformadores

- U.P.S. y estabilizadores de voltaje.

Manejo de Señales de Alarma y Procedimientos Correspondientes

Al recibirse una señal de uno de los abonados a la Central de Alarmas, aparece una señal en el monitor del computador de la Estación Central de Monitoreo, esta señal en diferentes colores, de acuerdo al orden de prioridades y se procesará según los parámetros determinados previamente para cada evento.

En la pantalla aparece una descripción completa del usuario o cliente donde esta ocurriendo el evento: nombre, número y estado de cuenta, dirección, actividad, teléfonos del local de instalación y de los empleados de contacto, tipo de alarma instalada, contactos para casos de emergencia, además descripción del evento: alarma (tipo), activación, desactivación, problema, tamper (tratar de romper una cerradura), etc.

SISTEMAS DE ALARMAS

Han sido diseñadas para detectar ladrones, no para detener su acceso a la propiedad.

SISTEMAS DE SEGURIDAD

Para combatir las siguientes consecuencias: Problema Psicológico

- Ruido: Tensión y estrés – problemas psicosomáticos – delirio de persecución – insomnio – descontrol en su entorno social – costos de primas – seguridad

SISTEMA BASICO DE ALARMA

Teclado Contados (puertos)
Perímetro Sirena
Detector movimiento (PIR)Batería (Transformador)
Detector de incendio

PARTES DE UNA ALARMA

Teclado
Detectores — Movimiento, Ruptura cristal, Incendio
Contador

El mejor sistema de alarma combina protección de perímetro con interior de su propiedad.

MANEJO DE SEÑALES DE ALARMA

MANEJO DE SEÑALES DE ALARMA Y PROCEDIMIENTOS CORRESPONDIENTES

Al recibirse una señal, de uno de los abonados a la central de alarmas, aparece una señal en el monitor del computador de la estación central de monitoreo. Aparece esta señal en diferentes colores de acuerdo al orden de prioridades y se procesará según los parámetros determinados previamente para cada evento.

En la pantalla aparece una descripción completa del usuario o cliente donde está ocurriendo el evento: nombre, número de cuenta, dirección, actividad, teléfonos del local de instalación y de los empleados de contacto, tipo de alarma instalada, estado de cuenta, contactos para casos de emergencia, además descripción del evento: alarma (tipo) activación, desactivación, problema, tamper (tratar de romper una cerradura), etc.

TIPO DE SEÑALES

1. Señales de Supervisión.

1.1 Apertura (actividad evento) y procedimiento
1.2 Cierre (activación por parte del usuario) y procedimiento
1.3 Test (prueba automática sistema) y procedimiento

2. Señales de Excepción.

2.1. Cierre Invalido (cuando el sistema no ha sido activado en el horario establecido), procedimiento (llamar, pedir santo y seña, al verificarlo se procede a una nueva hora de cierre). Su respuesta se temporiza por 30 minutos, para avisarle al usuario de la no activación. Enviar motorizado a verificar en el sitio.

2.2. Apertura Invalido. Cuando se recibe esta señal el sistema no ha sido desactivado dentro del horario establecido. Indica que no hay nadie en el local o que no se ha recibido la señal de apertura. Procedimiento se llama y sí responde, luego del santo y seña se procede a generar un mantenimiento por pérdida de señal. Si no hay respuesta se asume que no hay nadie en el local, luego no se ha desactivado el sistema.

2.3. Test. Indica que ha recibido el test automático de prueba. Procedimiento. en horas hábiles: verificar a que hora y cual fue el último evento. Se contacta con el local y se le pide active señal de pánico. Si no recibimos la señal se da una orden de mantenimiento. En horas no hábiles: lo mismo que el anterior, pero al no poder tomar contacto se envía inmediatamente al motorizado para hacer pruebas desde allí con la Central. Solicitar permiso en el local para entrar y revisar.

3. Señales de alarma y emergencia:

Se reciben estando el sistema activado o desactivado durante 24 horas.

3.1. INCENDIO. Es generado por detectores de humo, calor o estaciones manuales de incendio. Procedimiento. Si el local esta abierto, se llama a constatar la causa de la señal. Si la persona que contesta reporta incendio, se avisa inmediatamente a los bomberos y al motorizado. Si fue falsa alarma se restaura la cuenta.

3.2. PÁNICO, ATRACO Y CÓDIGO DE AMENAZAS. Señales generadas por pulsadores de emergencia alámbrica o inalámbrica, temporizado para cajas fuertes y apertura o cierre bajo amenaza. Procedimiento. Informar inmediatamente a la policía y al motorizado. Se comunica con el local, si es afirmativa, se continua con el procedimiento. Si es falsa alarma se dan las contraordenes necesarias.

3.3. INTRUSION. Señales emitidas por detectores de movimiento, rompimiento, sísmicos, tampers, contactos magnéticos, discriminadores de audio. Procedimiento: se envía inmediatamente el motorizado. Si la señal continua se da aviso a la policía y se solicita su apoyo, si es afirmativa se avisa al usuario para que se presente en el sitio.

4. Señales de Problemas.

Fallas de AC Batería son reportadas por el sistema al detectar fallos de sus componentes o cuando ocurren fallas en la energía. Procedimiento. En horas hábiles se toma contacto telefónico para establecer si el corte es en local o en el sector o si es solo del sistema, en este último se da una orden de mantenimiento

urgente. Si persiste la situación se pide autorización al usuario para que permita reemplazo de baterías. En horas no hábiles, al no haber nadie en el local, la Central de Monitoreo, esta atenta a cualquier cambio de situación. Si el fluido eléctrico no se restaura después de cierto tiempo, se le informa al usuario en los teléfonos que suministro para que se desplace hasta el sitio para cambiar baterías.

Prevención de Incendios

El administrador de seguridad coordina con Seguridad Industrial, la prevención de incendios especialmente en el campo de acción, prioridades y líneas jerárquica.

I. Diagnósticos
II. Implementación y entrenamiento
III. Asesoría

I. Diagnostico.

1. Clasificación de riesgos en procesos productivos, edificaciones e instalaciones en general.
2. Clasificación de incendios según las características de los edificios. Evaluación de las instalaciones de protección contra incendios, específicamente de equipos, alarmas (señales y recepción) y extinción.
3. Codificación de equipos para protección, alarmas y extinción.
4. Desarrollo y colaboración con los programas de mantenimiento, conservación y operación de equipo de detección, alarmas y extinción.

II Implementación y Entrenamiento

Implementación de las recomendaciones. Adiestramiento de personal a formar brigadas de prevención y combate de incendios, simulación y evacuación.

III Asesorías

Estudios y proyectos relacionados con las medidas contra incendio en edificación en general. Instalaciones eléctricas y mecánicas. Manejo de materiales inflamables. Programas de seguridad par las industrias y empresas. Control.

UNIDAD 6. SUBSISTEMA DE RONDAS DE VIGILANCIA

Como complemento a los sistemas de seguridad, son necesarios los sistemas de rondas de vigilancia, las cuales deben ser efectuadas por personal entrenado previamente para tal fin.

Dicha función se cumple en:

Exteriores: observando, detectando, investigando y comunicando a sus superiores inmediatos cualquier anomalía a los aspectos generales de vigilancia y seguridad. Las manifestaciones o eventos a tener en cuenta son: personales o grupos de merodeadores con permanencias prolongadas en tales áreas. Vehículo que circulan en forma sospechosa en cuanto a velocidad, número de personas en su interior, frecuencia de su presencia en la zona (registrados por CCTV.) Conversaciones con el personal de la empresa al inicio o término de sus horarios de trabajo. Vehículos estacionados o de aspecto de abandono en las cercanías a la empresa o rutas de ingreso, ya sea de personal como vehículos propios o de carga de la empresa. Hoy en día debido a lo frecuente de los atentados, es necesario verificar e informar al superior responsable, de trabajos de trazado y construcción de zanjas para cableado o tubería, reparación o cambio de cables eléctricos y postes, merodeadores en los armarios telefónicos donde están conectados los teléfonos de la empresa. Las mudanzas y acarreos de muebles y enseres en las vecindades.

De ser posible conocer y hacer contados personales con los dueños o administradores de tiendas, cafeterías, panaderías, talleres, almacenes, etc. del área. Cualquier variación o alteración a las situaciones de rutina normales, deben ser tenidos en cuenta, reportados e investigados por el personal de seguridad de la empresa.

Interiores: Se hacen de acuerdo a instrucciones y programas establecidos por los administradores de seguridad. Se fijan rutas, tiempos, puntos (relojes o sensores) de chequeo y comunicación, aparatos o equipos específicos a observación y cuidados, transmitir cualquier novedad anormal a sus superiores o supervisores. Dejan constancia escrita de ello en el libro correspondiente a rondas de vigilancia.

Evitar la intimidad con personal de la propia empresa ajeno a la actividad de vigilancia. El elemento femenino es en la mayoría de los casos, motivo de distracción para eliminar la funciones de los vigilantes en sus rondas y funciones.

Hoy gracias a los diferentes tipos de control, relojes o sensores, se pueden seguir las rondas de los vigilantes desde los centros de monitoreo, y en caso de no efectuarse en

las horas previstas, producen alarmas visuales y acústicas, que deben ser tenidas en cuenta por el supervisor, quien deberá comunicarse vía radio, teléfonos o con el personal de patrullas de vigilancia, con el vigilante que no ha transmitido la señal de chequeo determinada.

Para las alarmas de eventos especiales los vigilantes pueden contar con: medios radiotelefónicos, electrónicos, inalámbricos (pulsadores) estaciones manuales, botones de asalto o pánico con activación directa con la mano, o con el pie o por presión. Ninguna señal de alarma efectuado por las rondas de vigilancia, sea externa o interna, deberá ser descartada, todos tendrán que ser considerados por los supervisores de vigilancia o por los operadores de centro de monitoreo. Cada sitio deberá estar identificado con rutas de acceso, distancias y aparatos o equipos aledaños al lugar del evento.

En el caso de falsas alarmas, estas pueden ser efectuadas por:

- Malas instalaciones
- Cables deteriorados o pelados por el uso o ubicación
- Cargas electromagnéticas que por falta de aislamientos, produzcan efectos de activación
- Por mal uso de tarjetas o códigos
- Por falta de entrenamiento o nerviosismo del personal de vigilancia
- Variaciones eléctricas en las redes.
- Falta de coordinación en las medidas y manejo de elementos de seguridad. Horas extras de trabajo o despachos y recepciones.

SUBSISTEMAS

DETECCION DE INCENDIOS

¿Qué es fuego?

Es una reacción química que produce calor, luz y compuestos químicos. Una combinación química de materiales combustibles con oxigeno.

¿Cómo combatir el fuego?

La mejor forma es la prevención, usando sistema de prevención de incendios, podemos detectarlos, evitando el desarrollo y su propagación. Actualmente

existen en el mercado una gran variedad de sensores o detectores de fuego, que en conjunto con iniciadores manuales, paneles de control de alarmas y otros accesorios, forman en si un sistema de prevención de incendios.

El sistema debe tener comunicación directa con una estación central de monitereo y al mismo tiempo con la estación de bomberos, más cercana, para evitar cualquier tipo de propagación del fuego.

Detectores de Incendio

Existen 3 tipos básicos:

1. **Térmicos:** Funcionan bajo el principio de detección de calor generalmente ajustados de 135 a 200 F, generalmente son mecánicos, usando laminillas metálicas que se expanden con el calor y se contraen cuando la temperatura disminuye. Dentro de estos hay tipo resorte que funcionan una vez aplicación donde la temperatura tiene una variación de 15 grados minuto, en lugares como almacenes, lavanderias, lencerías en general donde tengan rápida propagación del fuego. Su cubrimiento máximo es de 16.5 X 16.5 mts. o 33 metros cuadrados, la altura máxima de instalación es de 5.20 metros, hay varios modelos:

   Fijo / variable 135F
   Fijo / variable 194F
   Fijo 135F * Fijo reemplazable
   * Variable se restablece al bajar la temperatura

2. **Ionicos:** Funcionan bajo el efecto de ionización del aire, dentro de una cámara radioactiva, la cual contiene partículas alfa de radiactividad, produciendo iones y cationes (moléculas positivas y negativas). Al entrar partículas de humo a la cámara estas son atraídas por las moléculas creando una resistencia a la conductividad del aire y por ende una reducción en el flujo de corriente. Este flujo es medido electrónicamente y al bajar de su nivel requerido, envía una señal de alarma al panel de control y de allí a la central de alarmas.

   Uso: En áreas donde los materiales combustibles al reaccionar al fuego crean una propagación de humo rápidamente formando partículas de humo al nivel de 0.3 micrometros, especialmente en bodegas, papelerías, etc. Una de sus desventajas es que su tiempo de respuesta es muy lento, se recomienda en centros o cuartos de computación y de telecomunicaciones.

Hay varios modelos de acuerdo a las velocidades del viento de 0 a 1.5 metros por segundo o mayores.

3. **Fotoeléctricos:** Funcionan bajo el principio de dispersión de la luz. Este principio se representa dentro del detector usando un bloque opto – electrónico, dentro del bloque existe un oidor emisor de cierta intensidad a cierto ángulo de inclinación y dentro de una cámara, al extremo opuesto, existe un opto – rele que recibe la señal enviada, al entrar partículas de humo dentro de la cámara, estos funcionan como reflejos incrementando la intensidad de la luz recibida, lo que activa el opto – rele y se dispara creando una alarma. Es el más confiable por su velocidad de respuesta y funcionan muy bien en los fuegos lentos, tales como polimeros, materiales textiles, etc. Se aplican en plantas textiles, polimeros, oficinas, centros comerciales, residencias, hoteles, cuartos y centros de controles eléctricos, etc.

   Hay varios modelos sencillos o con combinaciones de detectores térmicos, para usar con voltajes AC o DC, de 2 o 4 hilos para tipo stylus, detectores de ductos, de 120 VAC 9VDC los de circuitos A / B y D. Hay alámbricos e inalámbricos para residencia.

4. **Detectores de ductos:** Su función principal es controlar el paso del humo de un área a otra. Enviar señales al panel de control, pero no reemplazar a los detectores de humo en el área a proteger. Simplemente controlan el movimiento del aire dentro de los ductos de aire acondicionado.

   Sus ventajas es que contienen (E.S.L) medidores de flujo incorporado, no requieren extensión de tubería, monitoreo constante del cableado, LED de memoria, configuración en 2 o 4 hilos voltajes de 9VCD, 12VCD, 24VCD, 120VAC, establecimiento local de energía, supervisión de líneas, contactos auxiliares, cubierta trasparente (no necesitan abrir el detector), terminales para cableado desde 12AWG hasta 18AWG, alarma a control remoto, fácil instalación, aplicaciones es a nivel de ductos (aire acondicionado) para uno o varios pisos. Hay 15 modelos diferentes.

5. **Detectores de humo con rayos lineales:** Funcionan bajo principios fotovoltaicos, pero a diferencia de los detectores fotoeléctricos (funcionan bajo dispersión de luz) estos funcionan bajo el principio de emisión de un rayo de luz, el cual es recibido por un receptor a cierta distancia, y que contiene un fotosensor que mide la densidad de

la luz emitida (recibida) cuando partículas de humo reducen la densidad de luz emitida, el fotosensor envía una señal de alarma, aplicaciones en áreas abiertas y en techos muy altos, donde la velocidad del aire tiene corrientes de más de 15 metros por segundo.

6. **Otros tipos de detectores.** Hay una gran variedad de detectores que por su uso y aplicaciones, además del costo son poco usados, entre los más importantes:

   - Detectores incipientes
   - Detectores de dos líneas (2 hilos)
   - Detectores de llamas ultravioletas
   - Detectores de llamas infrarrojos
   - Detectores combinados ultravioleta/infrarrojo.

Componentes auxiliares

Existen una gran variedad de componentes, cuya función es enviar una función de alarma, advertir a los residentes o notificar a las autoridades, sobre un posible conato de incendio. En su mayoría son manuales o trabajan por funciones mecánicas creando un contacto eléctrico al ser accionadas, enviando así una señal de alarma o de avería según sea la condición, al panel de control de fuego, quien a su vez se comunicará con la estación central de monitoreo vía telefónica o radial usando su comunicador analógico o digital.

Entre los principales componentes auxiliares están los siguientes:

- Interruptores de seguridad para flujo de agua.
- Interruptores de seguridad para válvulas.
- Estaciones manuales.
- Campanas de alarmas.
- Sirenas o cornetas
- Parlantes anunciadores
- Lámparas de emergencia
- Luces de alta densidad (STROBES)
- Retenedores electromagnéticos de puertas.

OBSERVACION: Leer bien los boletines y características técnicas de cada componente

para verificar su función, especificaciones y características.

Panel de Control de fuego

Es el aparato más importante del sistema de control de fuego. Es el encargado de recibir, controlar y trasmitir las señales de alarmas, averías etc. Cada panel cuenta con los siguientes elementos:

- Fuente de poder primaria.
- Fuente de poder secundaria.
- Batería de respaldo (60 horas).
- Tarjeta de control.
- Tarjeta iniciadora de alarmas
- Luces indicadoras de zonas.
- Luces indicadoras de averías.
- Cargador de baterías.
- Supervisión de zonas.
- Supervisión de potencia.
- Potencia limitada.
- Capacidad de expansión.
- Salidas de campanas, sirenas y cornetas.
- Comunicador analógico / digital
- Prueba a control remoto.

APLICACIONES. Cada instalación y construcción es diferente, el uso de aplicación de cada panel de control debe ser de acuerdo a las necesidades del área a proteger. Por lo general se recomienda una zona por cada 600 metros cuadrados (25 x 24) de construcción, claro esta que sigan las normas de la NFPA, CEN y de las autoridades de cada país o municipios encargados de la supervisión de la obra antes de dar el permiso de habitar el edificio.

La ubicación del panel debe ser en el cuarto de control de cada edificio y debe estar protegido siguiendo las reglas especificas anteriores.

ANEXO D

UNIDAD 7. SISTEMA INTEGRADO

7.1. Fundamentos de la Centralización

Parte Primera

1. Necesidades

La centralización se define como el nexo integrados de todos los subsistemas que componen un sistema de seguridad, posibilitando unas relaciones óptimas entre éstos, el entorno y los operadores o usuarios del sistema, garantizando el funcionamiento dentro de los límites establecidos en el diseño.

De esta consideración emana un primera necesidad que debe cumplir todo sistema de seguridad complejo, como es su modularización en sistemas más sencillos. El criterio de modularización debe atender a las diferentes funciones de seguridad requeridas, según la siguiente clasificación general:

- Control de acceso
- Control de rondas
- Vigilancia por circuito cerrado de televisión
- Detección de intrusión
- Detección y extinción de incendios

La función integradora de un sistema de centralización se dirige, fundamentalmente, hacia los siguientes objetivos.

- Información inmediata de los eventos producidos y presentación de la misma de una manera adecuada y simple.
- Modificabilidad de la base de datos general de sistema, manteniéndola viva en todo momento.
- Modificación, debidamente protegida, de los procesos automáticos.
- Back up constante de todos los datos y movimientos realizados por el sistema, tanto automáticos como en los que interviene algún operador.

En los que se refiere al funcionamiento del sistema de seguridad, la centralización debe

contemplar planteamientos y estrategias que aseguren tanto la alimentación ininterrumpida de todos los equipos electrónicos, como la redundancia de componentes, de manera que se impida la caída del sistema por fallo de la red de alimentación o avería de equipos críticos. Por último, un sistema de centralización de seguridad plantea , en sí mismo, una serie de necesidades. Dentro de ellas se pueden citar como más importantes las siguientes:

- Reducido tiempo de respuesta desde que se produce un evento hasta que es reconocido.
- Flexibilidad y adaptabilidad tanto a cambios como a ampliaciones.
- Simplicidad de operación y mantenimiento.
- Alta fiabilidad de equipos y componentes,
- Alta inmunidad frente a pérdidas de información
- Gran facilidad de manejo incluso para personas no especializadas.

2. Base Teórica. Sistemas de Control de Procesos.

La centralización es una parte indispensable en todo sistema que pretenda controlar un determinado proceso.

Desde el punto de vista histórico, éste ha sido un problema que ha suscitado múltiples estudios y soluciones en los sistemas de control de procesos industriales, y de manera muy especial en lo que se refiere a las comunicaciones entre los dispositivos sensores y los equipos controladores.

Un sistema de seguridad, es en definitiva, un sistema de control de procesos, en la teoría clásica de esta disciplina se defina la siguiente terminología.

- El Medio, que presenta una serie de estados diferenciables.
- Los dispositivos Sensores, que muestren periódicamente los estados del medio.
- Los equipos Controladores, que reciben las señales generadas por los sensores a través de un determinado sistema de transmisión, produciendo otras en función del estado del medio.
- Los Actuadores, que reciben las señales del controlador y generan una acción.

Como ejemplo ilustrativo se puede ver el funcionamiento de un sistema de aire acondicionado, en el que sus diferentes elementos se identifican con el modelo descrito de la siguiente manera:

- El medio es la temperatura ambiental y se intenta que permanezca en un valor fijo (temperatura deseada).
- Los sensores son transductores que convierten la temperatura medida en una señal eléctrica proporcional.
- El controlador es un circuito electrónico que compara las señales recibidas de los sensores con una señal patrón equivalente a la temperatura deseada. En función de la diferencia entre ambas, se generan las señales actuantes.
- Los actuadores son motores eléctricos y resistencias accionados a través de las señales actuantes del controlador.

Cada una de las funciones que puede realizar un sistema de seguridad (control de acceso, detección de intrusión, vigilancia por circuito cerrado de televisión, detección y extinción de incendio), se pueden englobar dentro de la estructura descrita anteriormente. De este modo, en un sistema de detección de intrusión se puede, por analogía, distinguir los siguientes elementos:

- el medio lo constituye el recinto a proteger. Su estado establece o deseado, sería sin intrusos.
- Los sensores, lógicamente, son los dispositivos de detección de intrusión, o aquellos destinados a reconocer objetos (contactos magnéticos, detectores volumétricos, vídeo sensores, lectoras de tarjetas, etc.)
- El controlador es la central de alarma, donde se reciben todas las señales procedentes de los detectores.
- Los actuadores pueden ser múltiples, desde sirenas, flashes, marcadores telefónicos o posicionadores de cámaras de televisión, hasta la propia intervención humana (personal de seguridad).

Los sistemas de control de procesos están basados en el principio de la realimentación, por el cual las actuaciones generadas son función de los estados del medio y no se realizan de una manera determinista.

De forma general, un sistema de seguridad cumple el principio de realimentación. No obstante, existen una serie de funciones que no dependen del estado del medio, sino del criterio del usuario o la configuración del sistema, como pueden ser la conexión - desconexión de zonas de alarma o el cambio de niveles de acceso dependiendo de la hora del día.

Esta analogía estructural entre los sistemas de seguridad y los sistemas de control de procesos, conduce, en lo que se refiere a centralización, a adaptar las soluciones ya existentes, fundamentalmente en las siguientes materias.

- Adquisición de señales: utilización de contactos tipo real, libres de tensión.
- Transporte de señales: utilización de bucles de comunicación y redes de área local.
- Tratamiento digital: utilización de memorias y microprocesadores.
- Recursos informáticos: utilización de ordenadores, para control, presentación y registro o almacenamiento de datos.

Por último, hay que considerar que la centralización se integra sobre un sistema de seguridad que hay que diseñar y en este sentido los planteamientos difieren notablemente de aquellos diseños orientados al control industrial, fundamentalmente por el manejo de variables estadísticas con un amplio margen de desviación, como puede ser:

- El comportamiento humano, tanto individual como social.
- Los factores meteorológicos.
- Influencias electromagnéticas.
- La evolución dinámica del propio recinto (cambio de objetos, nuevas construcciones, reformas, etc..)

El problema de la seguridad puede cerrarse estadísticamente y siempre asumiendo un cierto margen de riesgo.

El problema del control industrial puede cerrarse completamente, desde el momento en que se conocen los propios límites de los diseños artificiales (máquinas, motores, etc.).

3. Recursos Técnicos.

Para conseguir los objetivos señalados, en un sistema de centralización existen una serie de recursos técnicos de común aceptación, tanto por parte de los fabricantes como por los usuarios finales de estos sistemas.

Estos recursos son los siguientes:

- Distribución de la capacidad de proceso (manipulación de información en

distintos puntos del sistema).

- Distribución de la base de datos (reflejo total o parcial de la base de datos del sistema en punto estratégico de control).
- Especialización por sistemas (tratamiento especial para cada subsistema componente de la instalación de seguridad).
- Multifuncionalidad de las estaciones de operación (terminales de presentación de alarmas, terminales de control de acceso, etc.)
- Asignación de prioridades (ciertos eventos tienen un tratamiento preferente a los demás).
- Utilización de redes de área local para comunicación de datos en sistemas complejos.
- Multiplexación de señales, que permite la comunicación de varios canales lógicos sobre un mismo canal físico.
- Utilización de lenguajes de programación estándares (Pascal, lenguajes para programación de base de datos, etc.)
- Manejo de paquetes gráficos (software para presentación de información)

4. Tendencia Actual de los Sistemas de Centralización.

La evolución de los sistemas de centralización en seguridad trata de mejorar, fundamentalmente, tres aspectos.

- La capacidad de proceso.
- Las comunicaciones.
- Nivel de integración con otros sistemas de control.

A ello ha contribuido de manera decisiva el progresivo abaratamiento de los costes de microprocesadores y memorias, así como el amplio desarrollo y aceptación de las redes de área local.

A medida que aumenta la complejidad, se ponen de manifiesto las carencias de los sistemas clásicos de centralización, basados en una unidad central e interfases de recogida de señales y comunicación.

Entre los principales inconvenientes planteados se pueden citar:

- Aumento del coste en equipos.
- Aumento del coste en infraestructura de canalizaciones.

- Aumento del tiempo de respuesta.
- Complejidad de instalación y mantenimiento.
- Complejidad de configuración del sistema
- Complejidad de control de las comunicaciones.
- Limitación en la ampliación del sistema.

La evolución hacia sistemas distribuidos permite incluir, en puntos distintos a la unidad central, la inteligencia necesaria para el reconocimiento de eventos y la generación de las señales actuales correspondientes, así como la configuración dinámica de las zonas de alarma conectadas a dichos puntos. La unidad central pasa ahora a realizar las funciones de presentación de información y control de comunicaciones, además de permitir, de forma interactiva con el operador, la configuración de todo el sistema de seguridad.

No obstante, existe una limitación para estos sistemas en cuanto a los canales físicos de comunicaciones disponibles como puertas de entrada - salida en la unidad central. La utilización de redes de área local soluciona este problema, ya que requiere un único canal físico sobre el que se implementan todos los canales lógicos mediante técnicas especiales de transmisión.

En una red local todos los elementos conectados se consideran como terminales, existiendo un elemento, el controlador de red, encargado de mantener de forma coherente las comunicaciones. Esto hace que el sistema sea especialmente versátil a la hora de atender futuras ampliaciones.

Existe un inconveniente para la aplicación masiva de este tipo de comunicaciones, puesto que las redes de área local están pensadas para la comunicación de datos en complejos sistemas informáticos y disponen de velocidades de transmisión notablemente superiores a las necesarias en un sistema de seguridad.

No obstante, se están realizando esfuerzos para conseguir estándares de red con unas prestaciones que se adapten de una manera más lógica a los requerimientos en el campo de la seguridad.

Una de las tendencias más novedosas es la integración de los sistemas de seguridad a otros de control en grandes edificios, como pueden ser la iluminación, climatización, etc. Dado el actual desarrollo del campo de la telemática y las redes de ordenadores, que se reflejan en la consecución de estándares de comunicación (modelo de referencia □ISO

de 7 niveles, para la transmisión de datos entre ordenadores), es posible la integración de cualquier ordenador a cualquier telemático, si se dispone del software necesario y la tarjeta hardware adaptada el ordenador a una determinada red de transmisión, pudiendo ser ésta de dos tipos:

- **Red de área local (ya referenciada anteriormente):** el medio de transmisión es un cable dedicado (cable de pares, coaxial o fibra óptica). El entorno es un edificio, un conjunto de edificios o un complejo industrial, es decir, distancias pequeñas o medianas.

- **Red de área distribuida:** normalmente se utiliza el conjunto de medios que aporta la red telefónica. En otras ocasiones se utilizan líneas específicas para transmisión de datos. Se puede tener cualquier entorno de comunicación (provincial, regional, nacional e internacional).

Parte Segunda

1. El Modelo Jerárquico.

El modelo jerárquico describe, desde un punto de vista formal, una estructura de bloques para un sistema de seguridad, que permite abordar su centralización según los siguientes criterios.

- **Modularidad:** Se puede pensar que el sistema está constituido por bloques, hardware y software, que combinan de diferentes maneras dando lugar a distintas configuraciones.

- **Redundancia:** Todos los bloques fundamentales pueden ser duplicados, de tal manera que se asegure el funcionamiento en caso de fallo o avería.

- **Compatibilidad:** La ampliación de las prestaciones del sistema es siempre compatible con la situación precedente.

La estructura base del modelo jerárquico comprende tres niveles fundamentales.

- **Nivel 0:** Está relacionado con lo que, en términos de control de

procesos, se definió como sensores. Comprende las medidas técnicas de seguridad, es decir, contactos, detectores, actuadores y lectoras de tarjetas.

- **Nivel 1:** Está relacionado con el sistema de transmisión, en el que se integran los concentrados y las interfases de comunicación, además del propio soporte de las comunicaciones.

  Este nivel debe asegurar el transporte y la correcta interpretación de los datos procedentes del nivel 0.

- **Nivel 2:** Está relacionado con la gestión global del sistema de seguridad. En este nivel se incluyen tanto la interfase de usuario, como la base de datos del sistema. Normalmente se implementa un software, en el que existe una parte cuya función es el diálogo con el operador y otra parte cuyo funcionamiento vienen regulado por las señales recibida desde el nivel 1.

A continuación, se realizará una clasificación en función del número de señales a centralizar, donde se podrá ver las características generales de cada tipo de sistema, así como la aplicación jerárquica a cada uno de ellos.

5. Sistemas Aislados.

Se pueden caracterizar de la siguiente manera:

- Reducido número de señales.
- No hay operador
- Existe una unidad central a la que se conectan directamente los detectores. No hay interfase de recogida de señales.
- La comunicación fuera del entorno local se realiza a través de línea telefónica.
- La topología de conexión es radial
- Según el modelo jerárquico, sólo existe nivel 0 (detectores) nivel 1 (Unidad central).

6. Sistemas Medios.

Pueden caracterizarse de la siguiente manera:

- Poseen una cantidad moderada de señales.
- Tratamiento sencillo de señales.
- Necesitan, al menos, un operador, por lo que incorporan una unidad de presentación de información (monitor, teclado e impresora)
- Utilizan una topología de tipos bus común o anillo.
- Disponen de una unidad central a la que se conectan los detectores a través de interfases.
- Necesitan un algoritmo de arbitraje de comunicaciones (prioridad estática, prioridad dinámica, pooling, FCFS).
- Respecto al modelo jerárquico, se puede distinguir el nivel 0 (detectores), estando el nivel 1 y el nivel 2 implementado conjuntamente en la unidad central.

7. Sistemas Complejos.

Entre las principales características de estos sistemas, se pueden destacar las siguientes:

- Gran cantidad de señales.
- Existen varios subsistemas (detección de intrusión, incendios, control de acceso, etc.)
- Necesitan más de un operador (multipuesto)
- La topología utilizada es de tipo irregular.
- Dentro del modelo jerárquico, se puede distinguir claramente cada uno de los tres niveles:

* Nivel 0, detectores.
* Nivel 1, interfases y concentradores.
- Nivel 2, ordenador de presentación y registro de información.

ANEXO E

LOCALIZACION AUTOMATICA DE VEHICULOS (AVL)

1. Descripción del Producto.

La Localización Automática de Vehículos (AVL), utiliza técnicas de GPS (Posicionamiento Global por Satélite) con el propósito de tener un control eficiente de la flotas de vehículo, en cualquier lugar en que se encuentre. Con está información las funciones básicas de despacho y el rastreo de vehículos en caso de hurto pueden ser realizadas con gran eficiencia.

El GPS está basado en una red de 24 satélites. U pequeño receptor de GPS en tierra (instalado en el móvil) procesa la información recibida. Con la información provista por cuatro satélites y utilizando técnicas de triangulación, se determina la posición de un objeto en términos de latitud, longitud y altura; la velocidad y el rumbo.

Los datos de los móviles son enviados al centro del control manteniendo actualizada la posición del móvil a intervalos programables de acuerdo con la actividad de la flota. Una vez la información se encuentra en el centro de control se monitorea en mapas digitados de la ciudad o región en una o varias terminales de computador.

2. Aplicaciones.

* **Localización:** El móvil o el conjunto de móviles que forman una flota son mostrados en mapas digitalizados.
* **Grabación de datos:** Todos los movimientos y actividades de cualquier vehículo pueden ser grabados para ser reprocesados en el sistema.

* **Reporte de operación:** Producción de diversos reportes de operación de los vehículos.

* **Definición de Rutas:** Definir rutas con el operario para evitar ciertas zonas.

* **Telemedición de Variables:** Se pueden medir variables físicas del vehículo.

* **Base de Datos.**

3. **Sectores de la Industria.**

* **Empresas de Transporte:** Supervisión permanente de los diferentes buses y camiones.

Suministrando beneficios como:

- Asegura cumplimiento de entregas
- Control permanente de itinerarios
- Permite redespachos inmediatos
- Permite asistencia inmediata en caso de varadas
- Mayor seguridad para la carga

* **Servicios de Emergencia:** Tales como ambulancias, policía y bomberos , ya que presenta las siguientes características:

- Controla la localización exacta de los miembros de la flota
- Verificar cumplimiento de ordenes
- Coordinar labores de persecución y localización

* **Servicios de Seguridad:** Es aplicable para el transporte de valores y seguridad empresarial.

LOCALIZACIÓN AUTOMATICA DE VEHICULOS

LO ULTIMO EN TECNOLOGÍA GPS A SU ALCANCE

Identifique la posición exacta de sus vehículos en forma automática. Por menos de la décima parte del precio del vehículo usted instala un sistema completo receptor de 8 satélites, el cual utilizando el radio de comunicaciones (de cualquier marca), informará a la estación central de su exacta localización en forma automática, las 24 horas del día.

Ponga a su flotilla de vehículos a la altura que se merece.

¿Cómo se integran a un sistema de radiocomunicación?
GPS es un "Sistema de Posicionamiento Global". Puesto en servicio por Estados Unidos para que un usuario conozca su ubicación exacta en cualquier parte del mundo. Fue utilizado completamente y con éxito en la Guerra del Golfo Pérsico y ahora, el sistema cuenta con un servicio para la población civil.

LAV significa "Localización Automática de Vehículos". Es un sistema que se utiliza para conocer la ubicación de unidades móviles propiamente equipadas. Los receptores de GPS obtienen su ubicación en Latitud y Longitud (A).

La información de ubicación, que el receptor GPS deduce es enviada a la base por medio de una señal de radio que el MODEM controla (B).

Es primordial contar con una vía confiable de comunicación (C), los datos se pueden transmitir a través de:

- Sistema convencional VHF, UHF y 800MHz (Voz y Datos)
- Sistema Troncal (Voz y Datos)
- Sistema de Repetición Digital DIGIPEATER (Datos)

El LAV/GPS puede convivir con las comunicaciones normales, siempre que no esté muy congestionado el canal.

En la central es necesario tener un radio base. Aquí se instala otro MODEM, el cual recibe información del radio móvil. Es necesario también tener una computadora compatible con IBM (D).

El área en la que se puede rastrear un vehículo depende de la cobertura del sistema o de la red de repetidores.

EJERCICIO

EQUIPO A BORDO DEL VEHICULO	**EN LA BASE**
ACE-III Tarjeta receptora de GPS, no	RVD-97, Módulo para LTR y Convencional

incluye antena $323.00
RVD-97 Módulo para LTR y Convencional sin receptor GPS
Detalles $264.00
SYG-058 Gabinete (espacio para RVD97, ACEI y radio) $85.00 Dls
G-052 Gabinete (espacio para RVD97 y ACEI)

sin receptor GPS
Detalles $276.oo
SYG-058. Gabinete (espacio para RVD97, ACEI y radio) $85.00
G-052. Gabinete (espacio para RVD97 y ACEI) $13.00
CYBERNAV. Software hasta 20 vehículos $1.950.00
Software hasta 100 vehículos $3.250.00
Software hasta 500 vehículos $3.630.00

SISTEMAS DE COMUNICACION

FRECUENCIAS (Cuadro anexo)

DIAGRAMAS Radios portátiles
Radios fijos
Microondas Sencillo 30 canales
Sencillo 60 canales

ANEXO F

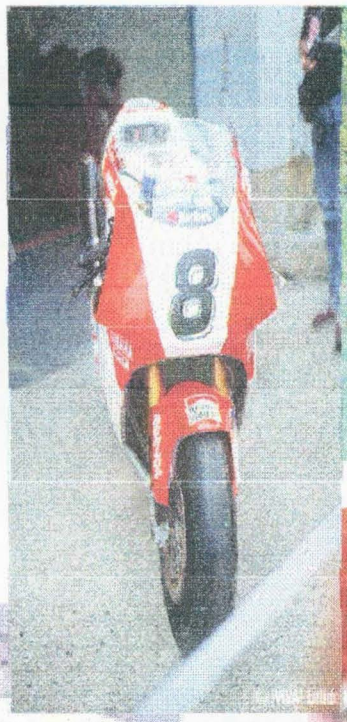
EQUIPOS DE SEGURIDAD ESPECIALIZADOS

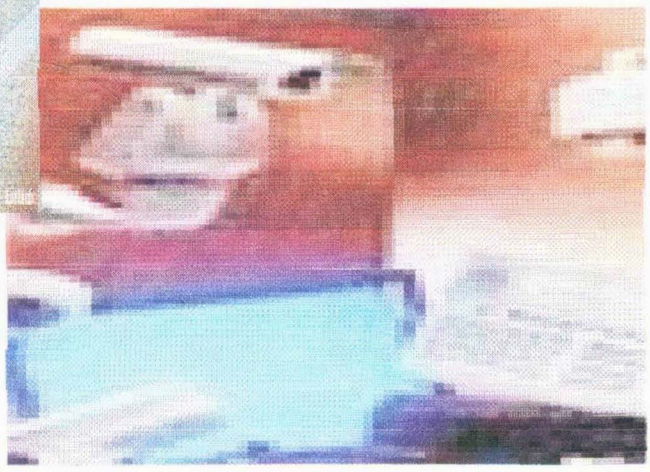
- Activador silencioso alarmas antisecuesto. 150 m
- Análisis de datos y sistema de monitoreo, intercepción, monitoreo y análisis de comunicación de datos entre objetivos múltiples
- Analizadores de voz, pruebas de la verdad y de engaño
- Autoadhesivos (stickers) temporizados
- Barricadas contra vehículos terroristas
- Blindaje niveles 1 – III – V Kerlar KEVLAR
- Cámaras ocultas infrarrojos para revisión vehículos
- Chalecos antibalas
- Chapas con llaves programables y memoria
- Computadora de grabación de audio de canales múltiples
- Desactivador de dispositivos de escucha de líneas de teléfono / fax
- Detectores de minas
- Equipo criptográfico (codificados – decodificados)
- Equipos de receptores y transmisores portátiles (accesorios) para sistemas de inteligencia multicanales
- Equipo de seguridad táctico
- Equipo de monitores de inteligencia de audio modular
- Equipos e instrumentos de penetración forzada
- Grabadora de número marcado, de líneas telefónicas (maletín)
- Grabadoras de largo tiempo y multigrabaciones
- Identificador de llamadas – grabador de números marcados
- Iluminación de emergencia
- Interceptor de líneas telefónicas, fax, datos
- Laboratorio de explosivos portátiles. Detector de partículas explosivas y vapor altamente sensitivo.
- Micrófonos miniaturas direccionales, de solapa, inalámbricos de cuarzo
- Micrófonos direccionales y de largo alcance
- Micrófonos parabólicos electrónicos
- Minas luminiscentes. Marcadores, minas térmicas personales para identificación nocturna
- Monitor pasivo de líneas telefónicas. Láser
- Monitoreo "infinidad". Láser digitalizado

- Monitoreo global remoto
- Nulificador de teléfonos celulares
- Palígrafo electrónico
- Protección N.B.Q. Civil
- Protección anti-agresión
- Repetidores (VHF/UHF) y transceptores
- Receptores portátiles miniatura, ocultos de bolsillo discretos de bolsillo
- Repetidoras VHF/UHF
- Sensores de transmisores y rastreo
- Sensores de transmisores de intervenciones
- Sensores sísmicos, acústicos
- Sistemas de rastreo direccional electrónico (remoto)
- Sistemas aéreos detección intrusos (microprocesador)
- Sistema de transmisión infrarroja de largo alcance
- Sistemas transmisor encriptado
- Sistema transmisores de corriente
- Sistema de monitoreo telefónico a control remoto
- Sistema de recopilación de información vía teléfono celular
- Sistema de intercepción beeper digital
- Sistema decodificado
- Sistema computarizado recopilados de fax
- Sistema de analización del protocolo de computadoras
- Sistema de recopilación digital
- Sistema regional para monitoreo teléfonos celulares. Centro de comando
- Sistema para monitores para teléfonos celulares, bloqueador de celulares
- Sistema móvil de intercepción telefónica
- Sistema de monitoreo celular con número seleccionado de interés
- Sistema analizador digital para pruebas de celulares
- Sistema de transmisión encriptado
- Sistema interceptor de 3 líneas para teléfono y fax
- Sistema de monitoreo de información vía redes telefónicas celulares a través del mundo
- Sistema localizador direccional. Antisecuestro
- Sistema de interferencia ECM, montado en vehículo
- Sistema CCTV cámaras ocultas
- Sistema interceptor GSM (Global system mobile comunication) 1, 2, 3
- Sistemas modulares de imágenes térmicas
- Sistemas de análisis y monitoreo de comunicaciones

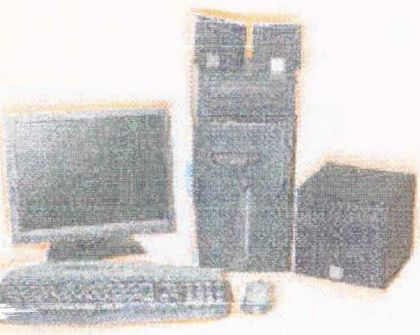
- Sistema ciberphone
- Sistema de detección de intrusión, sensores geofónicos
- Sistemas anti-espía
- Sondas para monitores de audio / video
- Stum-gum, bastones atendidos
- Teléfonos Acramblers (beepers, datos)
- Telímetros lasáricos – sensores láser activos – sistemas láser de detección
- Transmisores corporals (gomas, cigarrillo, sensores) accesorios (antenas, micrófonos, adaptadores y baterías)
- Transmisores telefónicos, detectores y localizadores
- Transmisores telefónicos paralelos
- Transmisores miniaturas, inteligente, encubiertos, activados por voz, estetoscópicos, decodificador.
- Transmisores con tono de rastreo, inalámbricos para rastreo, acústico, fantasma, larga duración, ocultos (beeper, mouse, pin, relojes, etc.)
- Transmisores de electricidad AC, modulares, incorporados de extensiones eléctricas, activados por control remoto.
- Transmisores telefónicos para línea telefónica, para línea de fax, intercambiables para teléfono.
- Transmisores corporal inalámbrico, bolígrafo.
- Vigilancia espectrometral y localizador de emisiones de precisión
- Visión nocturna y combate. Sistema observación
- Visores nocturnos

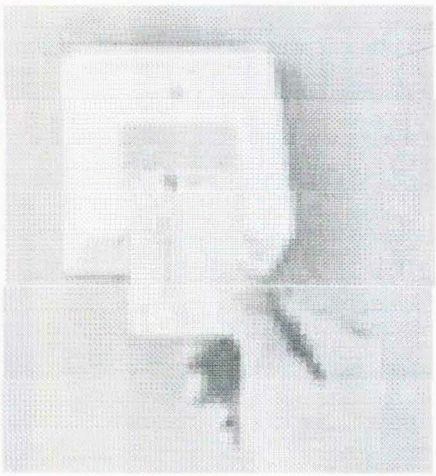
SISTEMA DE CONTROL PERIMETRAL

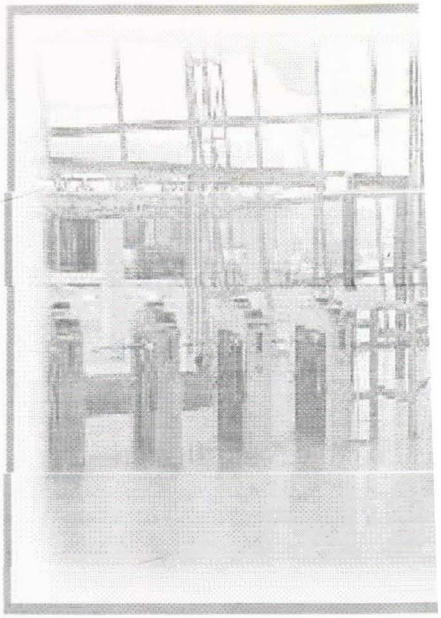


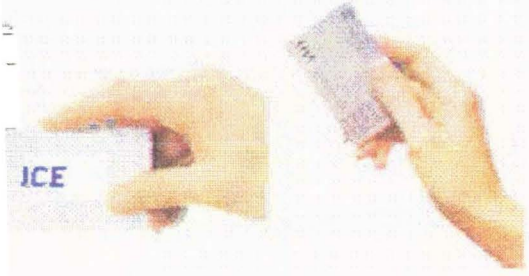


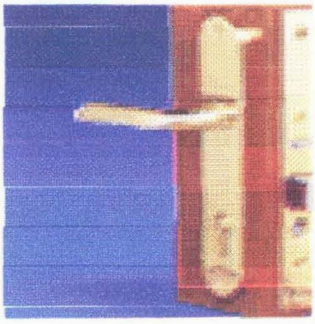
SISTEMA CONTROL DE ACCES



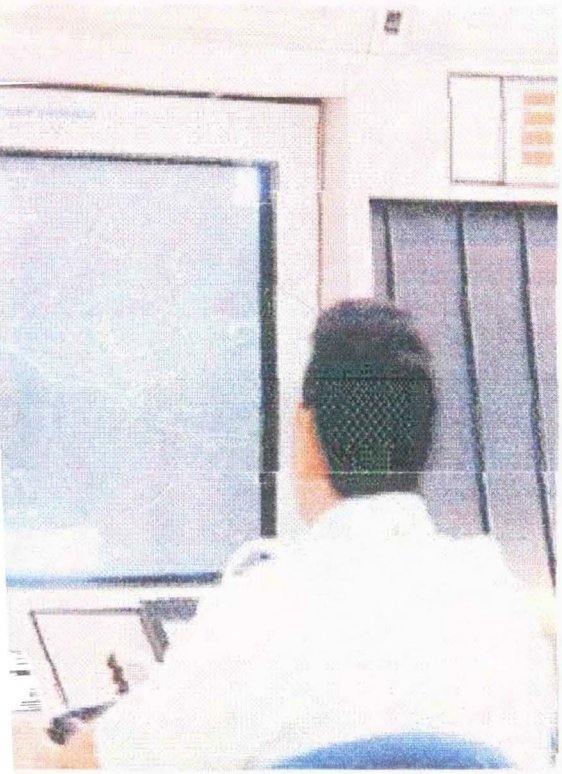




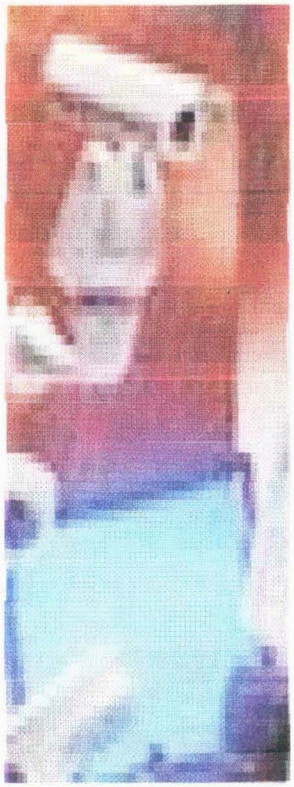


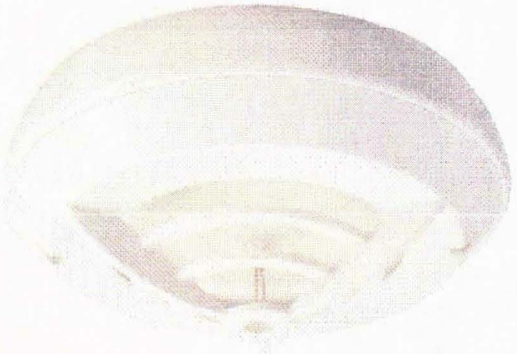


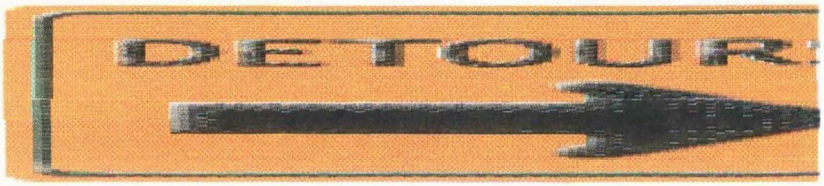
SALA DE CONTROL CENTRAL



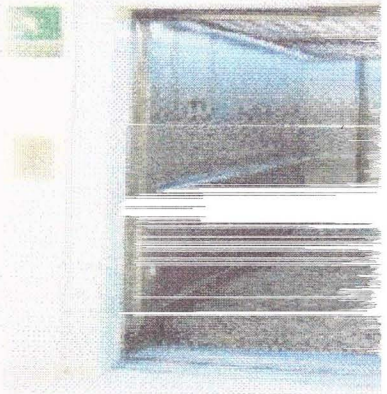
SISTEMA DE SEGURIDAD INTERNA







SISTEMA CONTROL DE ENERGIA Y MAQUINA



BIBLIOGRAFIA

- Directiva Permanente sobre Seguridad Integral del Complejo Militar CAN.
- Manual de Contrainteligencia FF.MM. 2-6 Reservado
- Manual de Seguridad Militar FF.MM. 2-7 Restringido
- Manual de Inteligencia de Combate (MIC) EJC-2-3 IV Edición
- Informe Revista de inspección CGFM-ING-893
- Informe Prueba de Vulnerabilidad DINTE-CECIM-DISEM-233
- Directiva Permanente Seguridad Integral del Complejo Militar CAN
- Estudio de Seguridad Perimetral.
- Manual de Funciones del Departamento de Seguridad.
- Constitución Política de Colombia 1.991.
- Guía para la nacionalización de tramites y procedimientos.
- Manual de seguridad técnica de (Dr. LUIS FERNANDO GOMEZ.)