Tecnologia de seguridad utilizada por el sector privado y su aplicacion en los sistemas de seguridad de las unidades militares

Jose Barrios Jimenez

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

2001

TECNOLOGIA DE SEGURIDAD UTILIZADA POR EL SECTOR PRIVADO Y SU APLICACIÓN EN LOS SISTEMAS DE SEGURIDAD DE LAS UNIDADES MILITARES

EMIRO JOSE BARRIOS JIMENEZ
Mayor

Director
OSCAR SANCHEZ VELEZ
Coronel

ESCUELA SUPERIOR DE GUERRA

CURSO DE COMANDO Y ESTADO MAYOR

BOGOTA D.C.

2001

CONTENIDO **Pag.**

INTRODUCCIÒN

Cumpliendo el requisito exigido por la Escuela Superior de Guerra, con el propósito de obtener el Diplomado en Estado Mayor, el alumno EMIRO JOSE BARRIOS JIMÈNEZ, con la supervisión directa del señor Coronel OSCAR SANCHEZ VELEZ, quien actúa como director, presenta el trabajo de grado titulado "TECNOLOGÌA DE SEGURIDAD UTILIZADA POR EL SECTOR PRIVADO Y SU APLICACIÒN EN LOS SISTEMAS DE SEGURIDAD DE LAS UNIDADES MILITARES"

La presentación de este trabajo fue posible gracias al apoyo y orientación del Señor Director, quien es especialista en Gerencia de Seguridad, al esfuerzo investigativo desarrollado, consultado y analizado, y a la cooperación de los Gerentes de las Empresas líderes en la aplicación sistemática de tecnología y su aplicación en los esquemas de seguridad, así como los Comandantes de las Unidades Militares visitadas. Sin la colaboración ofrecida por todos ellos, quienes hicieron valiosos aportes al trabajo, no se hubiesen logrado los resultados obtenidos.

La justificación y pertinencia del trabajo realizado, están basados en que la acción sistemática terrorista de los grupos al margen de la ley sobre instalaciones

militares y el riesgo por los daños que puedan suceder, obligan a una implementación de medios que generen un ambiente protegido, sólido y seguro. La inquietud surge por la inminente necesidad de neutralizar lo más pronto posible estas acciones, acudiendo a la tecnología utilizada por la empresa privada con excelentes resultados y así anticiparnos a nuevas y más complejas modalidades del terrorismo y la delincuencia común organizada. La urbanización desmesurada de las grandes y medianas ciudades, ha rodeado unidades militares que hace algunos años, en la periferia. Esto ha hecho que cualquier individuo o familia o personas, puedan vivir a pocos metros de las unidades militares generando un gran riesgo. Los sistemas de seguridad moderna precisamente se han especializado en diseñar equipos que puedan ser adoptados por las empresas privadas o instituciones públicas en las grandes ciudades, para neutralizar cualquier amenaza. Las unidades militares que tienen sus sedes en áreas urbanizadas, están bajo los mismos riesgos que otras empresas, por lo cual es imperante conocer sus sistemas de seguridad y adaptarlos a los nuestros, en la medida de su efectiva aplicación. Dada la condición de nuestras funciones futuras como comandantes de unidades y/o miembros de Estado Mayor de unidades operativas mayores y menores, es imperativo recomendar la integración de medios tecnológicos a los sistemas de seguridad de las unidades militares, para cubrir los vacíos que actualmente poseen.

Todo lo relacionado a los sistemas de seguridad de las unidades militares debe ser de cubrimiento e interés nacional e internacional dada la dinámica del

conflicto, que ha llevado a la amenaza a acudir a todas las formas de guerra para el logro de sus objetivos primarios. Las Fuerzas Militares han tenido que generar un sinnúmero de acciones para bloquear la iniciativa que en materia ofensiva ha desarrollado los enemigos potenciales de la República. Si bien es cierto, la iniciativa y el talento militar han estado de presente en el diseño de los planes de protección, ante posibles atentados y sabotajes terroristas, también es muy cierto que no se ha considerado en su verdadera dimensión, los alcances de la tecnología que nos brinda el mundo entero, en la implementación de las medidas tendientes a preservar la integridad de los hombres y las instalaciones militares. No así ha sucedido con las empresas del sector privado, quienes han acudido a la más alta tecnología en procura de atender las amenazas impuestas por las organizaciones armadas al margen de la ley, las cuales han condicionado la utilización de los medios de seguridad más oportunos, flexibles y veloces para anticiparse a complejas formas de delincuencia y terrorismo, propuestas por el enemigo.

El propósito fundamental del trabajo investigativo, es determinar qué tecnología incorporada a los planes de seguridad del sector privado, puede ser implementada en los sistemas de seguridad de las Unidades Militares. Los sistemas modernos de seguridad, presentan una gama amplia de posibilidades para adaptarse a las peculiaridades de los diferentes establecimientos, como es el caso de las instalaciones militares, que tiene áreas abiertas y áreas cerradas comunes, lo que implica desarrollar sistemas complementarios, dinámicos y flexibles de seguridad.

Las grandes compañías fabricantes de productos de seguridad, nos ofrecen alarmas de intrusión e incendio, dispositivos de comunicación y transmisión digital, sistemas de seguridad híbrido inalámbrico, detectores infrarrojos para salidas, sistemas integrados de seguridad y control de acceso, detectores de movimiento, alarmas y detectores fotoeléctricos, sistemas automáticos de transmisión de fotogramas, sistemas de vigilancia electrónica y grabación, sistemas de vigilancia remota vía telefónica y muchos otros. Todos ellos representan el referente para ser adaptados a las necesidades de los planes de seguridad existentes en las unidades militares.

Considero que el presente trabajo es de gran importancia, ya que dados los riesgos generados por la vulnerabilidad de las unidades militares, el reducir las posibilidades de error, necesariamente beneficia la imagen de las Fuerzas Militares, protege la integridad de los hombres y asegura las instalaciones contra los sabotajes. Reducir hasta lo más mínimo el accionar subversivo, permite disminuir los gastos millonarios, que debe asumir el Estado en vidas y materiales, para resarcir los daños cuantiosos producidos por los actos terroristas de los grupos armados al margen de la ley. Por lo anterior es de vital importancia para la implementación de los sistemas de seguridad de las Fuerzas Militares, realizar una investigación que favorezca las operaciones militares en todo sentido y disminuya los fracasos operacionales que minan la moral y la capacidad ofensiva de las Fuerzas.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

El objetivo que me he trazado en el presente trabajo de investigación es determinar y recomendar al mando superior, la implementación de sistemas de seguridad basados en tecnología de punta, utilizados actualmente por las empresas del sector privado, para complementar la aplicación de medidas pasivas, en los estudios y planes de seguridad de las unidades militares, en las diferentes fuerzas.

1.2 OBJETIVOS ESPECÍFICOS

- Identificar los sistemas de seguridad que utiliza tecnología de punta, empleados por las empresas de seguridad privada, sus resultados y experiencia.

- Determinar las fortalezas y debilidades de los sistemas de vigilancia electrónica, para ser incorporados en los planes de seguridad de las unidades militares en las Fuerzas.

- Identificar el sistema diseñado por la Seguridad Física Empresarial, para obtener su utilidad como marco de referencia para la implementación de acciones que conduzcan al mejoramiento de los niveles de seguridad de la institución militar.

- Recomendar los sistemas de seguridad basados en tecnologías de punta, que pueden adaptarse de mejor manera a cada una de las dependencias, almacenes, alojamientos, oficinas y áreas abiertas, que conforman las unidades militares y son peculiares dentro del panorama de organizaciones.

2. METODO Y TRABAJO DE CAMPO

2.1 METODO

Se utilizó el método de investigación activa, centrándome en el entorno y en dirección de la seguridad electrónica utilizada por el sector privado, contando para ello con análisis interpretativos, sobre situaciones reales en empresas privadas y en unidades tácticas. Se encausó el esfuerzo investigativo a determinar que medios o equipos de tecnología de punta están siendo utilizados por empresas y compañías industriales, para lo cual se realizaron importantes y variadas vistitas a los asesores y gerentes de la seguridad, que en su mayoría son oficiales retirados del Ejército Nacional y tienen la doble perspectiva de la seguridad militar y la seguridad privada, favoreciendo enormemente la objetividad en el trabajo.

2.2 TRABAJO DE CAMPO

Se desarrolló mediante visitas efectuadas a las sedes administrativas a dos de las multinacionales del petróleo más sólidas en Colombia, como lo es la BRITISH PETROLEUM CORPORATION y OCENSA. De igual manera se visitaron las unidades tácticas de la guarnición de Bogotá, donde a través de los oficiales de inteligencia y de operaciones se pudo establecer, la realidad de los sistemas de

seguridad, sus potencialidades y debilidades. Del análisis e interpretación de los documentos existentes en los cuales se ampara la seguridad de las unidades militares visitadas, se pudo establecer una omisión generalizada de complementar las medidas activas de seguridad, con medidas pasivas, acudiendo a equipos y sistemas electrónicos, que pueden reemplazar el desgastado capital humano, que se constituye en la base fundamental de la seguridad en las respectivas unidades. Los cuerpos de tropa han confiado de alguna manera, la seguridad a través del impacto disuasivo que imprimen los hombres, las armas y el cerramiento de del perímetro. Se hizo énfasis en este trabajo de campo, en las medidas pasivas internas de las unidades militares, las cuales se consideran las más débiles. En este micro-contexto se dedicó gran parte del esfuerzo, a verificar las medidas para asegurar la gran cantidad información y documentos clasificados, que no están lo suficientemente protegidos.

Se realizaron encuestas ha comandantes de unidades y gerentes de seguridad, quienes fueron las personas claves para obtener la información requerida.

Así mismo se visitaron las empresas y compañías dedicadas a importar y comercializar los equipos más sofisticados que en materia de seguridad están siendo adquiridos por el sector privado. En estos lugares se obtuvo información de todo el material que puede ser comprado e implementado por las Fuerzas Militares a presupuestos razonables.

3. CONCEPTOS BASICOS

3.1 SEGURIDAD

La necesidad de seguridad parte de las experiencias de cada persona, lo que hace de esto un concepto subjetivo inherente a cada ser humano y corresponda a una SENSACIÓN DE TRANQUILIDAD que difiere de cada persona según sea su condición, experiencia, entorno, actividad, careo, posición, riqueza, función, etc.
La seguridad en su esencia busca dar solución a tres problemas fundamentales:

3.1.1 Riesgo. Es la probabilidad de sufrir daño. Este es inherente a la actividad, la época y el entorno. Mientras exista alguna de estas tres variables, el riesgo nunca desaparece. La seguridad busca entonces disminuirlo hasta hacerlo razonablemente manejable.

3.1.2 Vulnerabilidad. Es el nivel de peligro que existe. A través de éste se producen los siniestros y se franquean los riesgos. Esta puede eliminarse al ser identificada y calificada en los estudios de seguridad. Mediante su eliminación se disminuyen los riesgos.

3.1.3 Incertidumbre. Significa el no saber cuando va a ocurrir un siniestro. Al igual

que el riesgo, la incertidumbre no desaparece. Para reducir la magnitud de daños que la incertidumbre puede causar, sobretodo de tipo psicológico, se trabaja a nivel de prevención.

3.2 RIESGO

Cuando se habla en el campo de la seguridad sobre el tema del riesgo se necesita diferenciar entre amparar el riesgo o disminuirlo.

Se necesita inicialmente determinar el nivel de riesgo.

Se establece mediante elaboración de un panorama general de riesgos. Para lo anterior se requiere de un estudio de seguridad orientado a las características de la dependencia, empresa o unidad militar.

3.2.1 Amparar el riesgo implica: recuperar la pérdida que se ha tenido de un bien sea éste tangible e intangible. Esta función la realizan compañías de seguros con las que se contrata mediante una póliza que busca recuperar lo perdido. El objetivo de tales compañías es devolverle a personas o empresas el bien perdido.

3.2.2 Disminuir el riesgo. Implica tomar medidas que prevengan pérdidas o daños sean estos permanentes o temporales. Esto significa hacer lo necesario para disminuir los riesgos que se han detectado dependiendo de las necesidades

y capacidades de una empresa, dependencia o para nuestro caso unidad militar.

3.3 ELEMENTOS BÁSICOS PARA LA ADMINISTRACIÓN DE RIESGOS

Es imperativo conocer quien o que es lo que puede causar la sensación de intranquilidad y entonces determinar como disminuir su impacto.

Para esto debemos identificar y calificar este agente. Lo identificamos como EL ADVERSARIO. Este puede ser externo o interno y debemos anticipar sus acciones conociendo el modus operandi que demuestra en sus acciones.

Las intenciones hostiles del adversario se anticipan mediante la implementación de medidas que en nuestro negocio llamamos dispositivos de seguridad.

3.3.1 Objetivos.

Un dispositivo de seguridad busca tres objetivos:

Disuadir. Es tratar de desanimar que se realicen intentos hostiles hacia las instalaciones que protegemos.

Neutralizar. Es buscar anular las intenciones de causar daño en caso que las medidas no disuadan.

Retardar. Es procurar demorar al máximo el logro de siniestro a las instalaciones si por alguna razón no se puede neutralizar.

3.3.2 Dispositivos

Los dispositivos modernos están conformados por tres componentes:

Medidas administrativas. Son las normas o consignas que se aplican en un servicio de vigilancia y protección. Como son las reglas de juego por las que se presta el servicio es importante que sean claras para ambas partes.

Seguridad activa. Están conformados por el factor humano. Operadores de una central de monitoreo, los supervisores y vigilantes.

Seguridad pasiva. Están conformados por los sistemas y medios tecnológicos que se utilizan para detectar, anunciar, controlar, vigilar, supervisar y transmitir los eventos al centro de control. En estos medios que son en su gran mayoría de conformación electrónica, he orientado el esfuerzo investigativo. La seguridad activa de las Fuerzas Militares de Colombia, es la mejor que existe a nivel de instituciones dedicadas a la seguridad, sin embargo en las medidas pasivas, es donde se encuentra una gran debilidad.

3.4 CLASIFICACIÓN DE LAS INSTALACIONES SEGÚN EL RIESGO.

Encontramos cinco niveles para clasificar las instituciones según el riesgo:

3.4.1 Residencial. Conjuntos cerrados. Edificios de apartamentos y casas particulares

3.4.2 Comercial. Pequeños negocios, pequeñas industrias, fincas de recreo y edificios de oficinas.

3.4.3 Industrial. Centros comerciales, industrias medidas e industrias livianas.

3.4.4 Comercial/Industrial. Negocios de cadena, industrias pesadas (excepto minería), sector financiero, universidades, laboratorios y proyectos agroindustriales.

3.4.5 Militar/Gubernamental. Bases militares, industrias militares, represas, aeropuertos, comunicaciones, transporte de energía, edificios administrativos, vías, puentes, puertos, acueductos, proyectos mineros y centros de acopio de alimentos.

3.5 OBJETIVOS DEL RIESGO

3.5.1 Contra las personas (individualmente)

- Atentado: Es una acción violenta para causar muerte o daño físico. Generalmente se ejecuta contra ejecutivos y jefes de personal.

- 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 (generalmente un ejecutivo) para causar angustia, stress, miedo y aún desesperación con miras a minar la fortaleza moral del individuo.

3.5.2 Contra las personas como 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 empresa para causarle daño desde adentro. La infiltración acompañada de otra acción que causa el daño como atentado, el secuestro, el sabotaje y el robo de material o documentos clasificados.

- Adoctrinamiento subversivo: Es el que procura ganar para la causa política subversiva a los trabajadores (especialmente si están sindicalizadas) y luego, con apoyo de los trabajadores así conquistados minar las capacidades de la empresa mediante exigencias exageradas en los contratos colectivos u otros documentos y con amenaza o ejecución de huelgas generalmente ilegales, buscando no la reivindicación de los trabajadores, sino la destrucción de la empresa.

- Hostigamiento: Igual que el individual, pero ahora contra grupos de empleados o trabajadores leales a la empresa. Se hace a base de 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 empresa. Se coloca entre los riesgos para personal, aunque lo es también del patrimonio. Es actualmente el terrorismo una de las formas más complejas de violencia utilizada por los grupos al margen de la ley. Por su gran capacidad de destrucción, los efectos sicológicos en la población y el comprometimiento de un mínimo de recurso humano si se quiere para su aplicación, se ha constituido en una desafío para las compañías de seguridad

3.5.3 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 (operaciones tortuga). O Huelgas para disminuir o parar la producción. 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 la fuerza. (hurto calificado).

- Ataques desde el exterior: Que pueden generar no solamente destrucción patrimonial, sino también pérdidas de vidas de integridad personal y moral en los trabajadores o visitantes o la 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 la empresa u obtener ventajas de mercadeo y producción.

3.6 LA SEGURIDAD ELECTRÓNICA

La seguridad electrónica como parte de la seguridad pasiva debe cumplir con

varios objetivos:

- Planificación
- Sencillez
- Discreción
- Inmunidad

3.6.1 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.

3.6.2 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.

3.6.3 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. Es por eso que cuando se decide implantar un sistema de estos debe hacerse en días de poca actividad en la empresa y preferiblemente debe hacer durante la construcción de inmueble para que su instalación no presente sospecha.

3.6.4 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.

4. SISTEMA INTEGRAL DE SEGURIDAD

Habiendo superado la intención del capitulo anterior, de ambientarnos con la temática de la seguridad, haciendo alusión a algunos conceptos generales, nos corresponde ahora avanzar en un contenido más específico. Dentro del gran campo de la seguridad electrónica, interactúan diferentes subsistemas de seguridad, que hacen parte de un gran sistema integral. La base primaria de estos subsistemas, en cuanto a material y equipo se refiere, es la electrónica. La más avanzada tecnología está al servicio de la seguridad y esta no puede ser ignorada. A continuación se enuncian los subsistemas que serán objeto de este trabajo investigativo.

- Sistemas de seguridad perimetral, externa e interna
- Sistema de detección e intrusión
- Sistema de control de acceso
- Sistema de Circuito Cerrado de Televisión
- Sistema de monitoreo de alarmas
- Sistemas de transmisión

Todos los aparatos y equipos que componen los subsistemas anteriores se deben integrar, basados en el principio de la interrelación y la centralización. Recordemos

que este material de tecnología de punta, cumple con los siguientes propósitos de seguridad:

1. Disuadir. Discriminar al adversario
2. Neutralizar. Anular las intenciones de causar daño ya sea físico o material.
3. Retardar. Demorar al máximo el logro del siniestro.

5. SISTEMA DE DETECCION DE INTRUSION

La seguridad no es un producto en serie, no hay dos organizaciones que se vean afectadas por los mismos riesgos, por ello es indispensable conocer cuáles son sus puntos o actividades vulnerables para decidir cuál debe ser su sistema y prioridad de seguridad.

El entorno es un factor cambiante. Sus sistemas y procedimientos de seguridad deben evolucionar y estar totalmente adecuados a los riesgos que día a día surgen para su actividad.

El conocimiento y la experiencia del Administrador de Seguridad en el sector privado, Jefe de Inteligencia o Jefe de Operaciones para unidades militares le permite estar alerta para planificar su seguridad y estar prevenido para reducir y evitar riesgos que puedan causar enormes pérdidas. Es el que diseña la estrategia para el manejo de los agentes de riesgos, de tal manera que le permita prever, detectar, retardar, detener, escapar o responder una agresión contra su Entidad o Dependencia.

5.1 FILOSOFIA DEL DISEÑO

La seguridad debe ser siempre su primera previsión. El robo, el espionaje

industrial las fugas de información, el robo continuado o extemporáneo, por los empleados, los asaltos, el secuestro, la extorsión, el chantaje, el saboteo y el terrorismo, son solo algunos de los riesgos inherentes al desarrollo de cualquier actividad empresarial.

Diseñar un sistema de seguridad permite a su organización contar con una respuesta adecuada a las medidas de sus necesidades de seguridad y de su cultura organizacional. El diseño integral los recursos humanos, la tecnología, los procedimientos, entrenamientos, supresión, los recursos del ambiente y cualquier otro medio, de tal manera que la seguridad contribuya a aumentar la productividad y no a obstaculizarla. Un sistema de seguridad, puede ahorrarle cuantiosas pérdidas.

El administrador de seguridad o el jefe de inteligencia y operaciones militares, debe asesorar a sus superiores para que su organización integre sus propias soluciones de seguridad en áreas urbanas y rurales, y pueda contar con:

- Capacidad de disuadir la amenaza.
- Controles eficientes de vulnerabilidad.
- Capacidad de supervisión.
- Sistemas de respuestas de emergencias.
- Sistemas de respuestas externas
- Sistemas de respuestas internas

- Capacidad operativa.
- Procedimientos y controles
- Coordinación con las autoridades.
- Análisis y evaluación de lo actuado.

5.1.1 Detección de intrusión externa o perimetral.

La vulnerabilidad de instalaciones técnicas sofisticadas o de alto valor económico, requieren el empleo de medidas de seguridad, las cuales ocasionan en primera medida un aumento de personal de vigilancia. Pero las experiencias en los últimos años han demostrado que los autores potenciales de atentados, en la mayoría de los casos son políticamente motivados y también apoyados desde adentro o por medios técnicos, por lo tanto no es posible oponerse con eficiencia mediante el solo aumento del recurso humano.

Es por ello que muchas empresas internacionales y nacionales desarrollan desde hace muchos años instalaciones automáticas y electrónicas para la vigilancia de áreas de grandes instalaciones tales como:

- Centrales eléctricas, acueductos y de comunicación
- Instalaciones Militares, de Policía y de Seguridad.
- Depósito de municiones o sustancias nocivas.

- Aeropuertos, puertos marítimos y aduanas.
- Fábricas o plantas de ensamblaje.
- Bodegas o depósitos industriales.
- Centros comerciales y bancarios
- Refinerías, oleoductos y gasoductos, etc.
- Centros de detención y penitenciarios
- Agencias, oficinas y plantas de gobierno, residencias y conjuntos residenciales, parqueaderos

Para la realización de las más diversas finalidades de vigilancia numerosas empresas han desarrollado tecnologías, fabricación y comercialización de equipos e instrumentos a disposición del requeriente, quien deberá evaluar y seleccionar dichos aparatos de mando y compatibilidad con los existentes, así como de sensores que permitan adaptar cada sistema de vigilancia a las particularidades propias de cada espacio abierto, y por supuesto a las condiciones del medio ambiente y el factor costo eficiencia.

5.1.2 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.

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

- Sensores de detección, para reducir el riesgo de robos, intrusión, fugas de cárceles y riesgos donde no es viable un guardián o vigilante.

- Circuitos cerrados de televisión, donde las cámaras (interiores, exteriores u ocultas) son elementos importantes en la seguridad exterior.

- Sensores de barrera;
- Sensores de volumen
- Sensores orientados a las cercas
- Sensores de movimiento incorporados a caminos
- Sensores infrarrojos de corto y largo alcance
- 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.

5.3 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.

5.3.1 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.

5.3.2 Plantas y Torres de Energía.

Tratamiento de aguas, procesos químicos, fábricas.

5.3.3 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.

5.3.4 Aduanas y Fronteras

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

5.3.5 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).

5.3.6 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 activa, pasiva, cobertura, volumétricos y sensores en línea, para proteger eficientemente las comunicaciones nacionales, internacionales y los sitios de transmisión.

5.3.7 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:

- Sistemas de detección de intrusos en perímetros.

- 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)

- 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.

- 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.

- Sensores de vibración, volumétricos (perimetrales) de intrusión (cables blindados y enterrados) Crean un campo electromagnético que detecta intrusos.

- Sistemas de protección por 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.

- 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 al ingreso o egreso seleccionables (desde 22 metros hasta 78 metros.

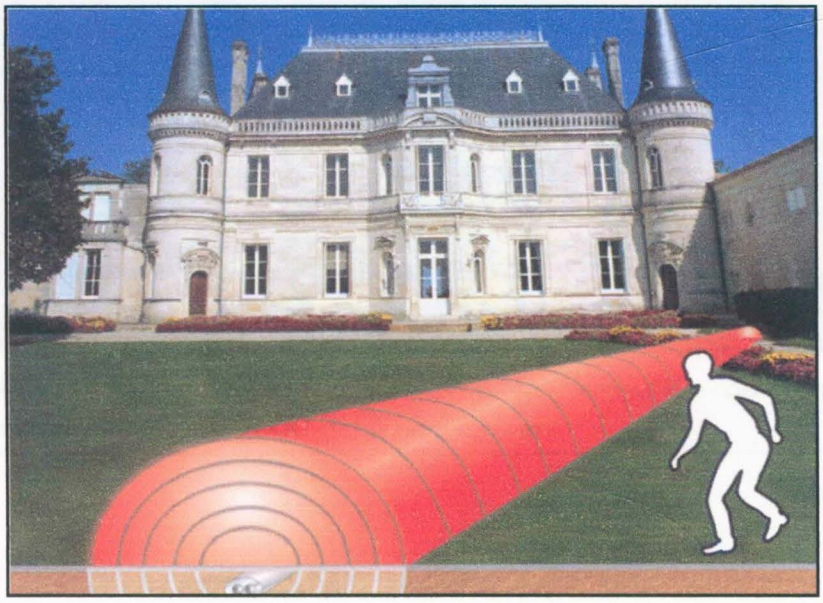
5.4 SEGURIDAD PERIMETRAL

Como sensores de intrusión externos y que desencadenan una señal de alarma existen a disposición los siguientes tipos, que por su función genérica, pueden ser incorporados a los esquemas de seguridad de las unidades militares. Toda la gama de sensores, representa un capital importante en seguridad, especialmente para dependencias de manejo crítico dentro de las unidades militares, que están al acecho de la audacia del enemigo, para sustraer armas, municiones y explosivos entre otros. Dependencias, como los depósitos de armas y municiones, depósitos de almacenaje de toda clase de explosivos, conocidos como los "polvorines", depósitos de material de comunicaciones y las secciones de operaciones e inteligencias, deben a lo mínimo tener un sistema de sensores, complementado electrónicamente con un sistema de alarma y/o monitoreo, para garantizar la custodia y la protección de todo este material físico y de información, que están permanentemente, en la mira de los grupos armados al margen de la ley.

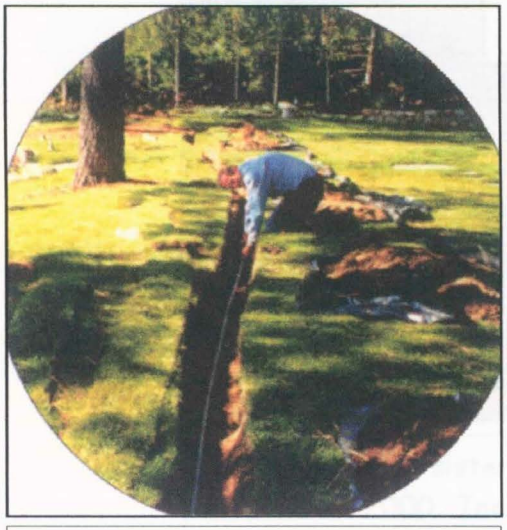
5.4.1 Sensores de Superficie:

Todos los sensores de superficie fueron diseñados para complementar el control y protección que normalmente ejerce el recurso humano de día o de noche. Esta herramienta permite cubrir las posibles debilidades de un sistema basado en el recurso humano, que es vulnerable, al sueño, al cansancio y a la oportunidad.

5.4.1.1 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.



Sensor Coaxial Inteligente de cuarta generación para detectar el acercamiento de intrusos. Referencia PERIMITRAX ofrecido por Magal Group.



Instalación del Sensor Coaxial Inteligente PERIMITRAX

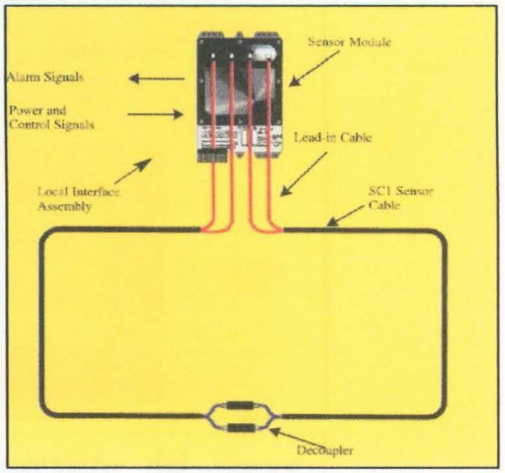


Diagrama de la configuración del sistema sensor PERIMETRAX con su respectivo módulo de señales.

Instalación de un cable sensor para la detección de intrusos. Referencia PANTHER 2000 del Magal Group

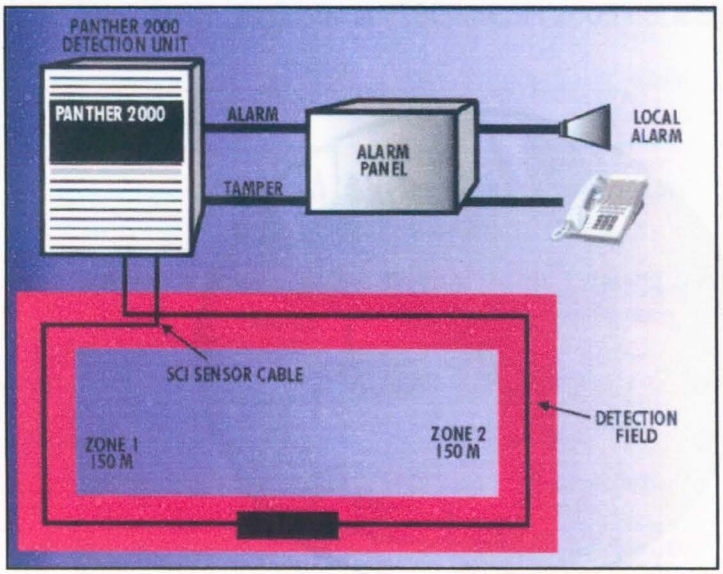
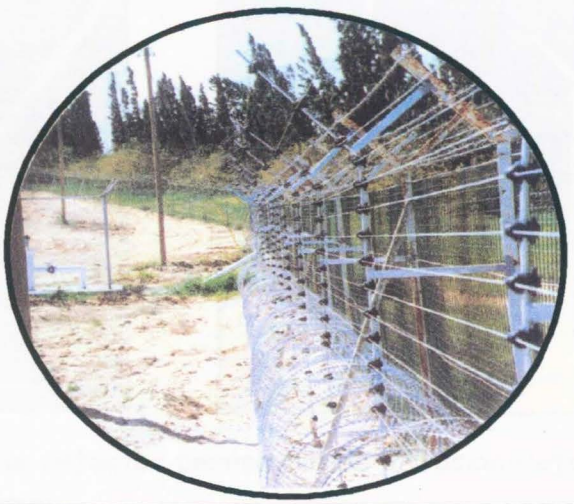


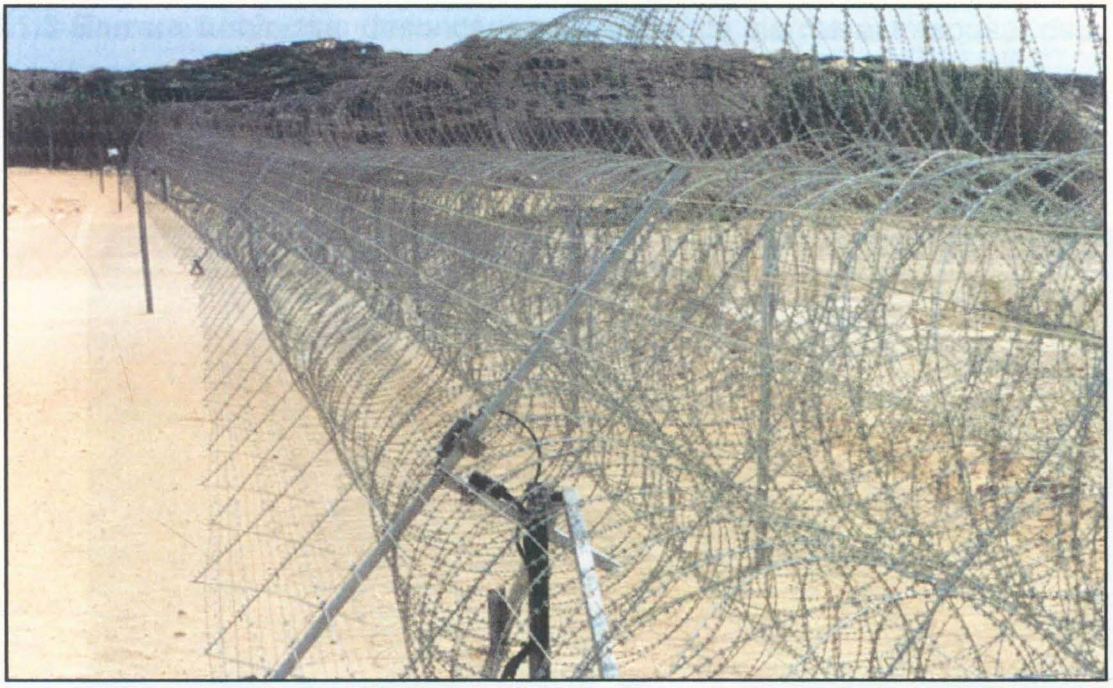
Diagrama del sistema completo del sensor PANTHER 2000. Incluye unidad de detección, panel de alarma y terminal de alarma.

5.4.1.2 Avisador de alambradas: o sensores de barreras. Desencadena la señal de alarma cuando se sobrepasa o se intenta destruir una cerca o alambrada metálica.

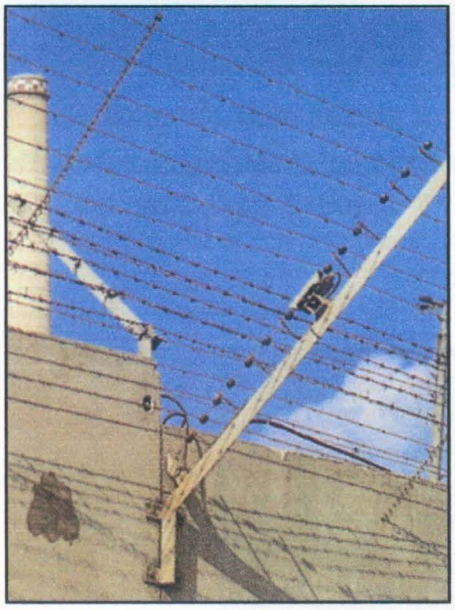
Sistema detector de intrusión de alambradas, mediante utilización de fibra óptica. Referencia FIBERMESH 2005 del Magal Group.

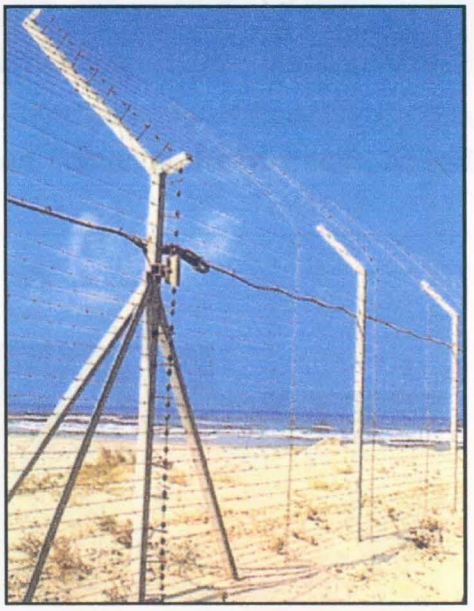


Sistema detector de intrusión de mallas y alambradas, mediante utilización de corriente eléctrica. Referencia ELECTRO-FENCE del Magal Group.



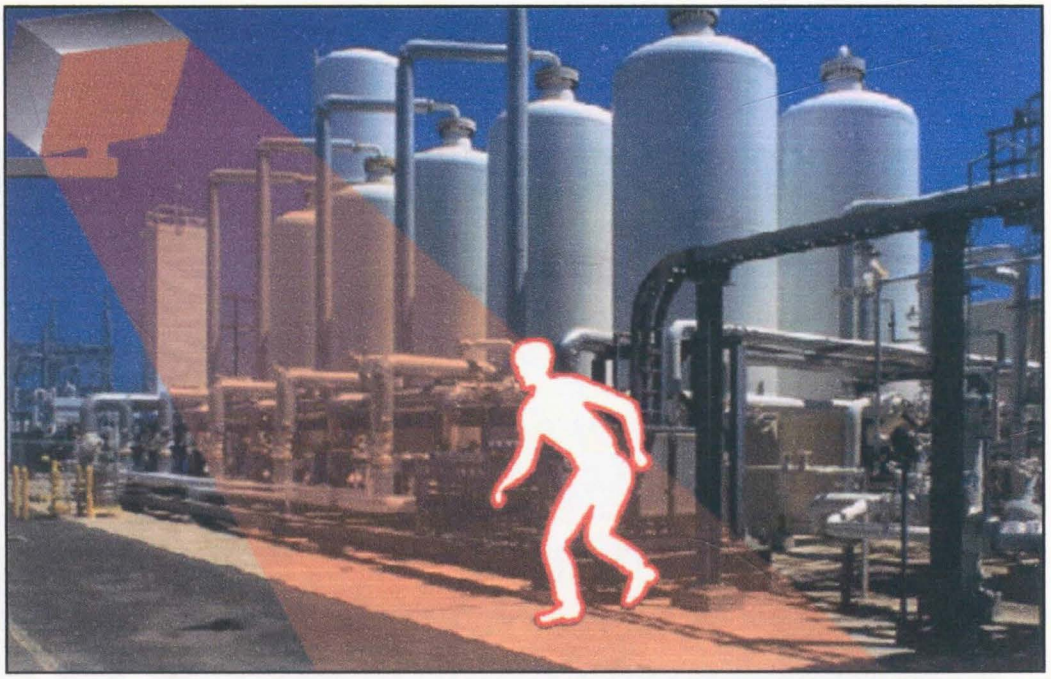
Sistema de cable tenso detector perimetral de intrusión para concertinas. Referencia YAEL-18 del Magal Group.



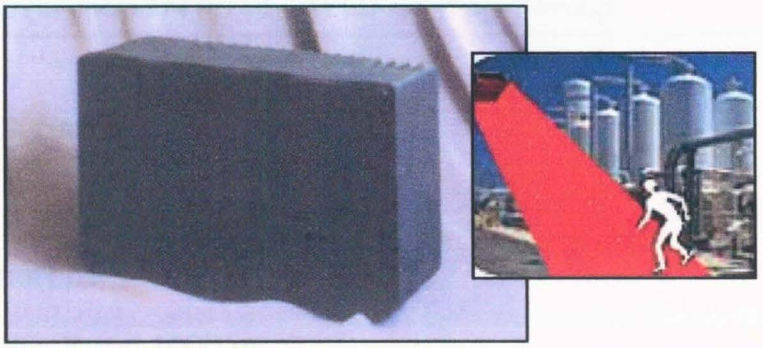


Sistema de cable tenso detector perimetral de intrusión Referencia YAEL-15 del Magal Group.

5.4.1.3 Barrera luminosa: desencadena la señal de alarma al traspasar esta, por ejemplo cercas de protección perimétrica o portones de entrada.

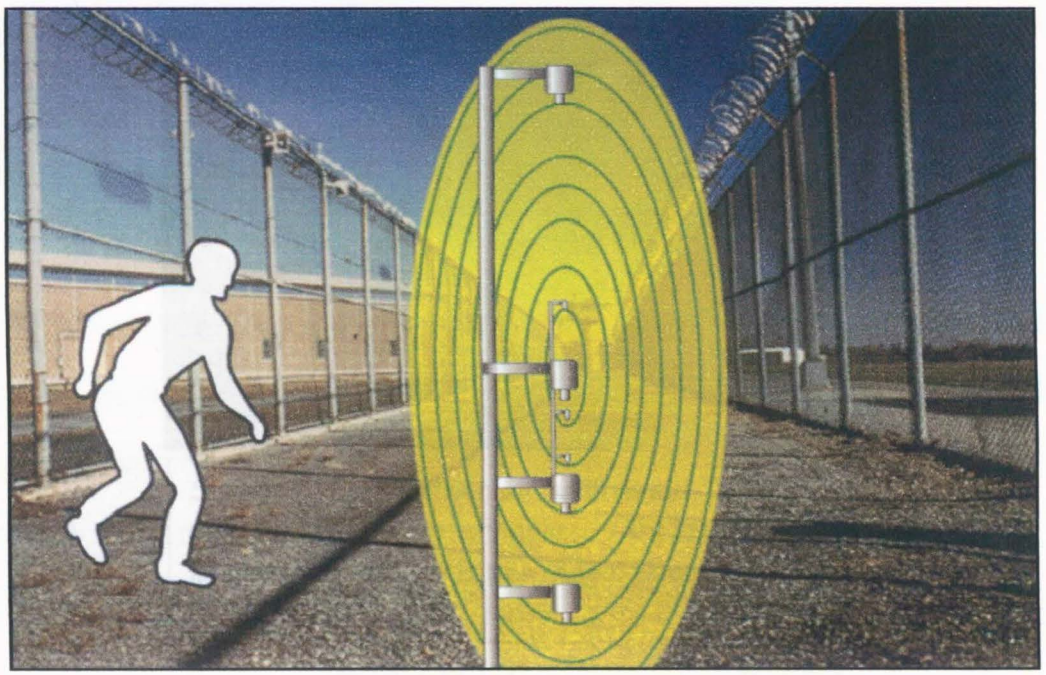


Sistema de iluminación externo, mediante la utilización de una luz invisible infrarroja, para uso con cámaras. Referencia STARLED 200 del Magal Group.



Mostrario del Sistema de barrera infrarroja STARLED 200.

5.4.1.4 Campo eléctrico: lámparas por sensor infrarrojo; prende automáticamente al detectar calor 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.



Sistema de sensor electroestático para campos inteligentes, a través del cual se puede detectar cualquier intrusión, dando alarmas visuales y acústicas. Referencia INTELLI-FIELD del Magal Group.

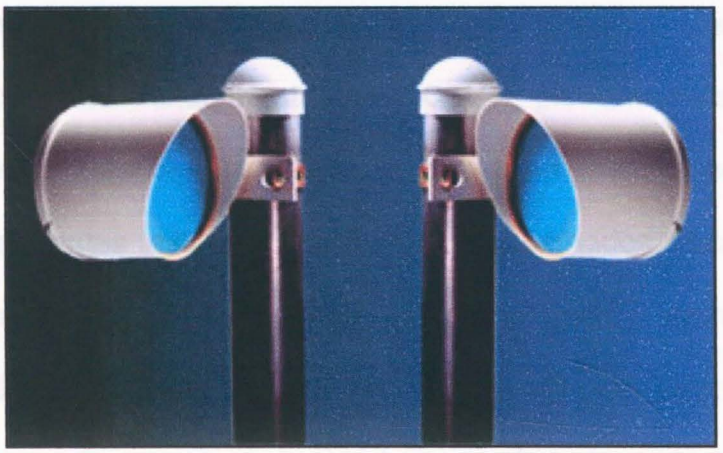
5.4.2. Sensores de Subsuelo

- Sísmicos magnéticos
- Cable microfónico lineal 1000 m.

5.4.3. Sensores de Volumen

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

- **Barreras de microondas (MW)**



Sistema de protección utilizando sensor de microondas. Referencia INTELLI-WAVE. Dispositivo, ofrecido por Magal Group.

Sistema de detección de intrusión por microondas. Referencia MODEL 14101 ofrecido por Magal Group.

6. SISTEMA DE CIRCUITO CERRADO DE TELEVISION. (C.C.T.V.)

El 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 un procesador electrónico, mayor 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.

Las nuevas microcámaras C.C.D. poseen las mismas características de las cámaras regulares, tienen un lente PINHOLE y 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 hacerse 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 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 ellos 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 de pantalla y secuenciador. La última tecnología de informática ha incorporado a los computadores las funciones de pan/tilt, zoom y 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.

6.1 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.

6.2 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. 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.

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 y combinarlos comparativamente.

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.

6.3 CÁMARAS, MONITORES Y VIDEO-GRABADORAS

- Cámaras

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.

Al diseñar un sistema de CCTV, se deberán tener en cuenta los siguientes ítems.

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, 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.

Igual como las cámaras, hay pantallas en blanco y negro, a color, desde 4 pulgadas hasta 54". 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 activadas y operadas manualmente o por secuenciador. Para casos especiales y de mucho control son recomendables 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.

- 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.

6.4 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. Es importante cuando se decide adquirir este material, tener muy en cuenta las especificaciones técnicas, ya que cada uno de estos lentes está adaptado para diferentes tomas deseadas, teniendo en cuenta la amenaza, el riesgo y los resultados que se persiguen dentro de un sistema integral de seguridad. No es igual el lente que se requiere para observar el acercamiento de vehículos a distancia lejana dentro de una ruta de aproximación, que el requerido para registrar el rostro de personas que ingresan a una instalación militar o una dependencia particular.

6.5 EQUIPOS AUXILIARES

6.5.1 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.

6.5.2 Divisor de pantalla (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 de ellos tienen zoom.

6.5.3 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.

6.5.4 Iluminadores Infrarrojos

Desde 6,3 vatios hasta 1000 vatios, para interiores o exteriores.

6.5.5. 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 lámparas o faroles o domos térmicos

6.5.6 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.

6.5.7 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.

6.5.8 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 cámara.

6.6 TRASMISIÓN DE AUDIO Y VIDEO A COMPUTADOR (DICAM)

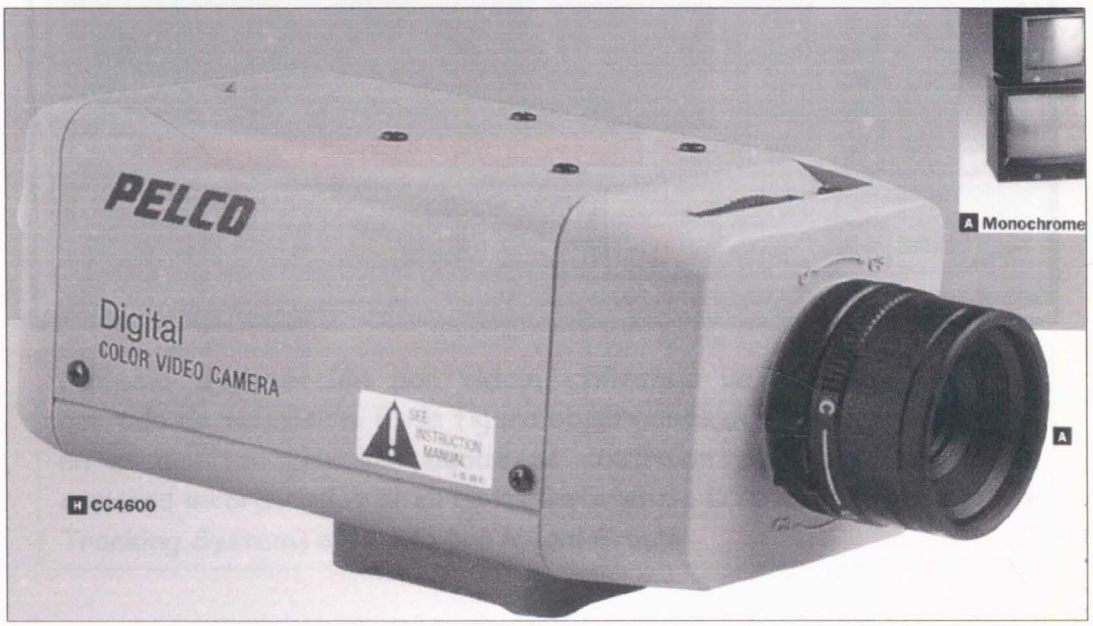
Gracias a las últimas investigaciones y desarrollos tecnológicos, se han diseñado y fabricado equipos de transmisión de las imágenes captadas por cámaras CCD a través de línea telefónica vía RF (radio VHF, UHF, HF) celular móvil o fijo a un equipo de CDPD recepción interconectado a un computador con 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.

6.7 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

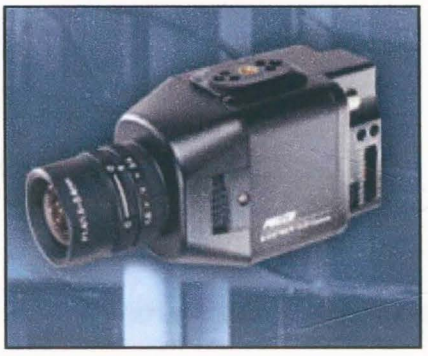
ofrece una excelente imagen aún en lugares oscuros, puede dar imagen en casi oscuridad total. El monitor portátil puede ser trasladado a oficinas, almacenes, bodegas o exteriores, ofreciendo rápida libertad de movimiento y audio y vídeo inmediato. Hay sistemas que ofrecen la posibilidad de conectarse a un televisor comercial para obtener una imagen en pantalla grande.

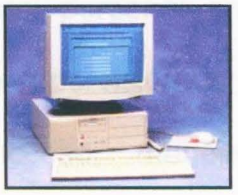


Cámara digital HC4600, para circuito cerrado de televisión. Industrias PELCO.

Sistema d detección por video, utilizando un completo circuito cerrado de televisión. En la figura observamos la imagen que aparece en el monitor principal donde se controlan y regulan todas las cámaras incorporadas al circuito. Referencia DTS1000 (Detection & Tracking System) ofrecido por Magal Group.

Apreciamos tomas diferentes de una misma cámara, haciendo el seguimiento a una persona mediante dispositivo sensor de movimiento. Referencia DTS1000 (Detection & Tracking System) ofrecido por Magal Group.





Diferentes dispositivos para la instalación de un CCTV. Industrias PELCO.

Sistema de CCTV para ambientes cerrados, referencia LEGACY, ofrecido por Industrias PELCO.

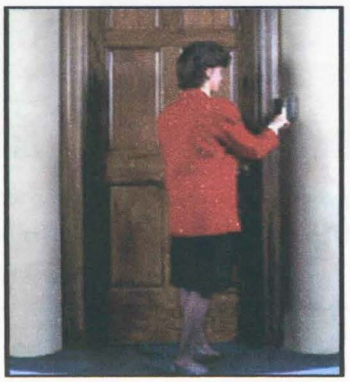
7. SISTEMA DE CONTROL DE ACCESO

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 indispensable 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 acceso controlados por códigos (Password).

7.1 COMPONENTES DE CONTROL DE ACCESO

7.1.1 Lectora sin teclado = PUERTA CAJEROS

Boca adicional



Acceso a interiores mediante dispositivo de control de acceso.

7.1.2 Lectoras con teclado = EXPENDEDOR DE DINERO

Banda infrarroja / Magnética / Aproximación

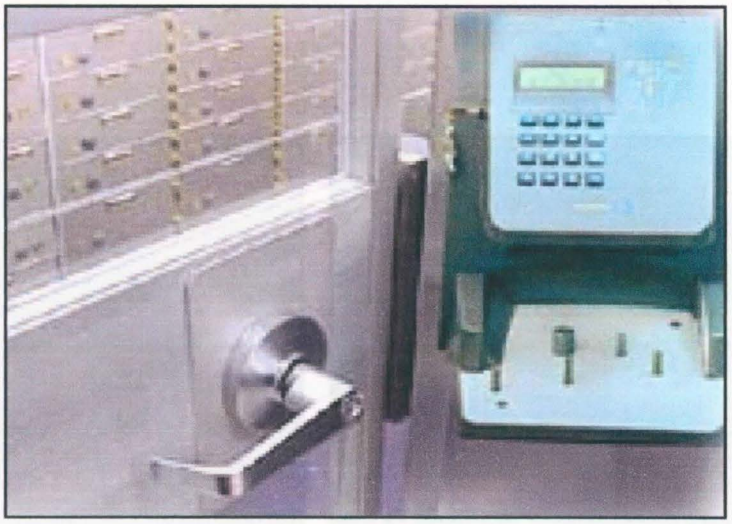
7.1.3 Tarjeta estándar

Banda infrarroja

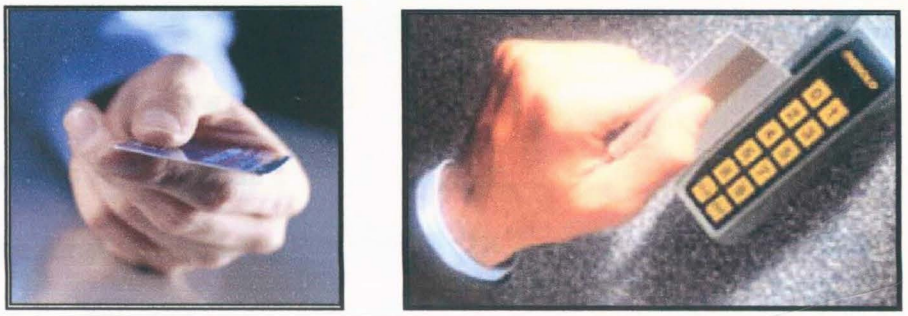
Banda invisible

Banda magnética

Banda por aproximación



Unidad Lectora de sistema de control de acceso mediante tarjeta electrónica. Dispositivo ofrecido por DIEBOLD COLOMBIA S.A.



Acceso mediante tarjeta electrónica y tarjeta chip.

7.2 SEGURIDAD FISICA

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

Sistema de Control de Acceso, mediante dispositivo de esclusas. Corporación DIEBOLD COLOMBIA S.A.

- Concertinas
- Vallados Metálicos
- Cámaras Acorazadas
- Cerraduras, Candados
- Cristales Blindados
- Puertas Blindadas / Automáticas
- Vídeo - Porteros

7.3 DETECCION Y REGISTRO

- Detectores de Metales (Manuales guantes)
- Detectores de Explosivos
- Detectores de Rayos X
- Detectores de Antihurto
- Detectores Carta Bomba
- Sillas detectoras partes íntimas (Boss)

7.4 CONTROLADORES ELECTRÓNICOS

- Lectores de Tarjeta de Código de Barras, Infrarrojo (ir) de Alta Seguridad (invisible)

- Tarjeta de Barras Magnéticas (PTA. CAJEROS)

- Controles de Teclado Para Digitar Claves Personales en Áreas de Alta Seguridad.

- Sistemas de aproximación

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

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

7.5 SISTEMAS DE ACCESO BIOMÉTRICO

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

- Exploración dactilar
- Escaneo de iris/retina
- Volumétrico
- Análisis de voz
- Geometría de la mano (ergonométricos)

- Firma
- Reconocimiento facial
- Otros sistemas biométricos exóticos: exploración del cuerpo humano, patrones

de venas de la mano, reconocimiento oreja y olor corporal

7.6 IDENTIFICACIÓN POR EL IRIS

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.

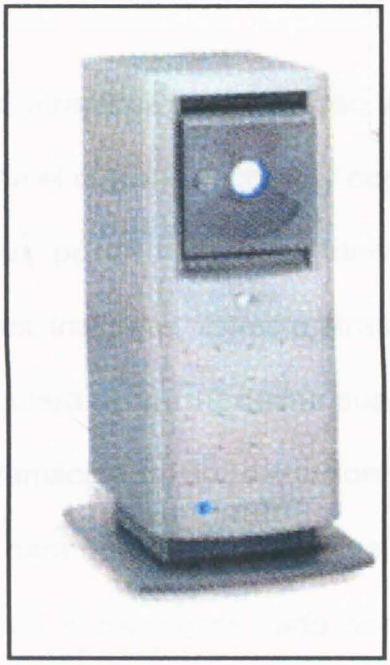
Dichas fórmulas le permiten a una cámara de video localizar el iris en la imagen de un ojo y luego escudriñan la estructura textural de dicho iris, codificando sus rasgos distintivos en una pequeña "forma" electrónica que es almacenada en un archivo de computador para su futura referencia.

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. 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.

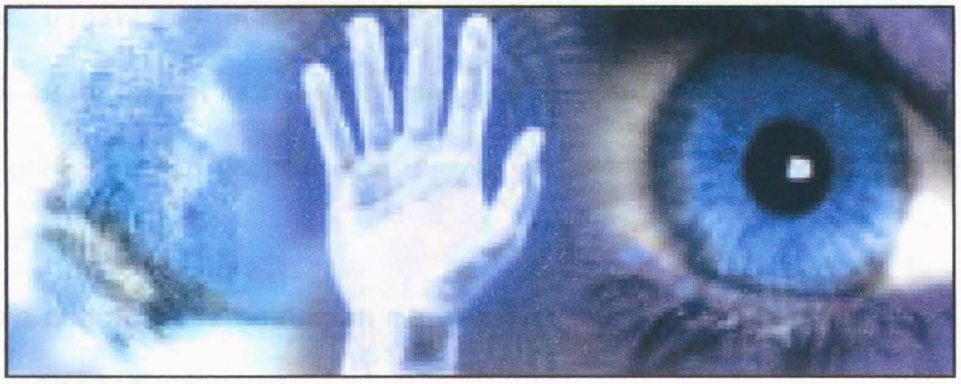
7.7 IDENTIFICACIÓN DE HUELLA DIGITAL

El sistema utiliza verificación biométrica (cada firma tiene su patente) para proveer identificación de personal irrefutable, solo personal autorizado tiene acceso

permitido a áreas restringidas o el registro de entradas o salidas.



Sistema IRISACCES®, consistente en un archivo codificado el cual contiene un resumen digital del iris. Ofrecido por DIEBOLD COLOMBIA S.A. Casa representante IRIDIAN TECHNOLOGIES.



La biometría se ha constituido en ciencia de vanguardia para la seguridad, facilitando el reconocimiento y autenticación en procesos de accesibilidad.

7.8 VENTAJAS Y CARACTERÍSTICAS

- Asegura rapidez y fácil acceso al personal autorizado
- Elimina el registro hecho por 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 móvil). Lo están usando los policías de tráfico de carreteras y 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. 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

8. SISTEMAS DE ALARMAS

En las unidades anteriores hemos visto:

- Sistemas de intrusión
- Subsistemas de CCTV
- Subsistema de control de acceso
- 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 una institución y dependencia.

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

- Por acercamientos o amenazas de ingreso desde perímetros exteriores.
- Ingresos a través de los puertos de control por la fuerza o por la falsificación de las tarjetas o elementos de control.

- Ingresos a áreas prohibidas por personal ajeno y sin autorizaciones.
- Intentos de robo, substracción o sabotaje en áreas de bodegas, línea de producción y almacenes. Con armas o engaños.
- Inicio de fuego en oficina, áreas de producción, almacenes de materias primas o productos terminados.
- 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:

- 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.

- Los controles de acceso detectan y detienen a quienes no porten las tarjetas de identificación, activen los códigos en los teclados o tratan de violar las garitas con tarjetas de otras personas. Así mismo en caso de atracos por la fuerza y que con armas traten de ingresar a la empresa.

- 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.

- 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 Institución, activando sirenas o medios acústicos o de bloqueo a las actividades de los ladrones.

- 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.

8.1 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 y un material que relacionamos después de la figura.

Centro de monitoreo de un CCTV.

- 1 computador
- 1 equipo de recepción y de codificación de señales

- 1 impresora
- 1 sirenas (cornetas) para alarmas de robo o fuego.
- 1 sistema de comando y control remoto para activación de conexión y comunicación a las patrullas de vigilancia propios.
- Sensores infrarrojos pasivos, de movimientos volumétricos
- Switches magnéticos para puertas livianas 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.

8.2 MANEJO DE SEÑALES DE ALARMA Y PROCEDIMIENTOS

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.

9. SISTEMA 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 contínua 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.

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.

9.1 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.

9.2 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 cuadrete (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).

9.3 TIPOS DE CABLE

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

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

9.3.2 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.

9.3.3 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.

9.3.4 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.

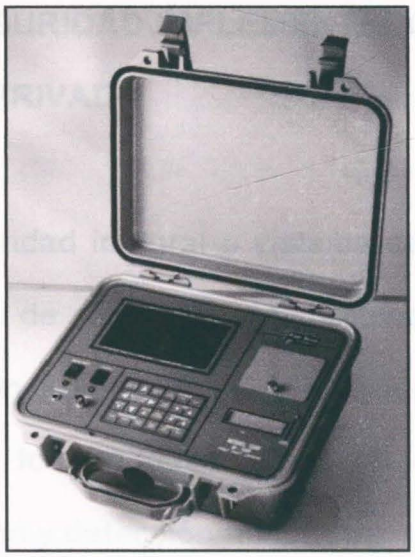
9.3.5 Cables Opticos: Uno de los avances tecnológicos de esta era, es el desarrollo de las técnicas de transmisión por cable óptico. Este utiliza fibras ópticas del grosor de un cabello para transmitir señales en forma de pequeños pulsos de luz. Es completamente insensible a las interferencias electromagnéticas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

9.4 INSTALACIONES DE ALARMA CONTRA ROBO

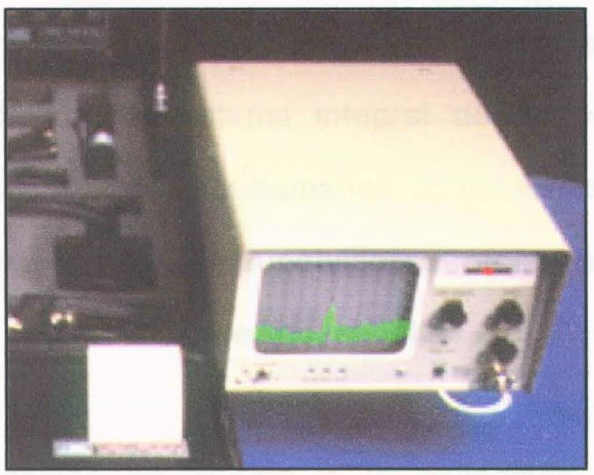
La instalación de los cables constituyen una parte muy importante en la función de la alarma, por esta razón, los cables deberán ser guardados dentro del área protegida por la alarma. En caso contrario deberán colocarse en tubería protectora (ductos). En cuanto a las instalaciones de alarma existe una marcada preferencia en favor de las instalaciones computarizadas de vigilancia.

La selección de los cables se 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. Imaginémonos un centro de alarma en el Centro de Operaciones Tácticas, de brigada o División, donde permanece un personal alerta las 24 horas del día. Que dicho centro de alarma electrónica esté integrado a un CCTV y a un sistema de cableado para permitir la activación de sensores, en el depósito de armamento, depósito de comunicaciones, oficina de comando, tesorería, sección de inteligencia y operaciones entre otros, que son las áreas más críticas. Este sencillo sistema de vigilancia electrónica, facilitaría de manera efectiva, el control y por ende la protección de los recursos más importantes de una unidad militar. Dentro de este sistema de transmisiones se cuenta con unos equipos adecuados para ser instalados en los centros de operaciones de las unidades o salas de guerra o comandos de las unidades, ya que allí se maneja la información más importante

en una unidad. Estos equipos son rastreadores de posibles interceptaciones o interferencias. A continuación fotografías de dichos equipos.



Sistemas analizador computarizado de líneas telefónicas, para verificar que no estén intervenidas.



Sistema de monitoreo del espectro electromagnético (barrido electrónico). INFOSAFE.(Servicios de Seguridad de la Información) Bogotá-Colombia.

10. DIFERENTES SISTEMAS DE SEGURIDAD IMPLEMENTADOS EN EL SECTOR PRIVADO

Recordemos, que el concepto de seguridad integral o sistema de seguridad física, se deriva de la interacción de factores de protección física, representados en barreras de protección y elementos de detección de área o puntos específicos, que representan, lo que describimos en el área de seguridad como elementos de protección y detección temprana.

Estos sistemas deben estar compuestos por la integración de recursos humanos, animales, físicos y tecnológicos, lo cual permite que mediante su interacción se establezca un sistema integral de protección física. Se pueden identificar como recursos humanos a personas dedicadas a la vigilancia (Centinelas, vigilantes, supervisores etc); en el área de los animales, se pueden señalar a los perros, caballos etc.

Existen varias diferencias en cuanto a la aplicación del concepto de seguridad física entre las áreas privada y pública, aunque los conceptos básicos sean los mismos. Para este caso en particular, se identifica al sector público representado por las Fuerzas Militares y sus instalaciones, y para el caso del sector privado tomaremos el caso de una empresa particular.

Basados en la experiencia de una persona que ha tenido la oportunidad de trabajar directamente con las Fuerzas Militares y que actualmente se encuentra trabajando en el sector privado en el área de seguridad, se harán las respectivas comparaciones y posteriores evaluaciones en cuanto a las principales diferencias y similitudes de los sistemas. Las lecciones aprendidas en la seguridad privada, coadyuvaran al diseño de esquemas adecuados, para la protección de las instalaciones militares, basados en factores presupuestales, contextuales y funcionales.

A raíz de la delicada situación financiera y económica que actualmente vive el país, las instituciones militares se han visto afectadas directamente en sus presupuestos. Esto ha obligado a dichas instituciones a dirigir estos presupuestos en su gran mayoría para combatir los grupos al margen de la ley, lo cual les ha impedido destinar recursos suficientes tendientes a proteger y generar condiciones efectivas de seguridad físicas en sus instalaciones. Por esta razón es muy frecuente encontrar en unidades militares, que el recurso humano es el principal medio de protección física de sus instalaciones.

En el momento en que se tomen determinaciones de implementar tecnología, se incurriría en unos costos de inversión inicial, para la adquisición de los equipos, pero en el mediano plazo esta inversión tendría una amortización representada en la optimización del recurso humano, ya que se vería

disminuido considerablemente el numero de personas dedicadas a la protección perimetral y de esta forma se podrían dedicar a reforzar los núcleos de reacción y protección. Se presenta con cierta frecuencia que el único sistema de protección física, se basa en un turno de centinelas, unas mallas o muros, cuando no son reemplazados por un alambre de púas. Lógicamente este esquema de seguridad puede ser considerado como un sistema elemental de protección. Empero, será efectivo? Hasta que punto puede depender de la supervisión de una persona? Se puede lograr que el centinela cumpla eficientemente con su función?

Este esquema no puede ser considerado como un sistema integral de seguridad; situaciones como las presentadas en la base de las Delicias, el cerro Patascoy, los ataques a las Escuelas de Formación de la Fuerza Aérea y el Ejército, por nombrar algunos casos, muy posiblemente se hubiesen podido evitar si se contara con los elementos mínimos de prevención que hubiesen permitido detectar oportunamente la aproximación del enemigo y no haber sido objeto del factor sorpresa, decisivo en estos casos.

Ejemplo real de sistemas vulnerables de seguridad física, es la situación de protección de unidades militares como comandos de División y Brigada, instalaciones de la Escuela Militar de Cadetes e instalaciones del Ministerio de Defensa Nacional.

Hasta el momento nos hemos enfocado al tema de la seguridad física bajo el concepto de la protección de amenazas externas, pero no podemos dejar a un lado las amenazas que provienen desde el interior de esas unidades, como pueden ser las personas infiltradas que ocasionan las frecuentes perdidas de armamento, robos de activos, fuga de información entre otros.

El tema del manejo y custodia de la información, es un área que en muchas organizaciones es desconocida y no cobra la importancia que esto representa. A manera de ejemplo existen compañías que tienen perdidas anuales superiores a los 300 millones de dólares por concepto de perdidas de información; estas perdidas son realizadas utilizando diferentes modalidades y tecnología que van desde un simple micrófono hasta personas especializadas y dedicadas a esta actividad como son los "Hackers"

En el caso de las Fuerzas Militares, existen infinidad de documentos, conversaciones, reuniones etc, que son de carácter confidencial, y que no son manejadas o protegidas como tal. Existe en la actualidad una tecnología de punta dedicada a la protección de esta clase de actividades, que se representan en sistemas de detección de líneas telefónicas interceptadas, detección de micrófonos, protección del espectro o simplemente pruebas de vulnerabilidad de sistemas de redes, en donde se

puede almacenar información valiosa tales como nomina, traslados, informes secretos, ordenes de operaciones, planes de seguridad de unidades etc.

Para entrar en el tema del sector privado, de acuerdo con el incremento de las condiciones de inseguridad del país, de las amenazas propias a las que se ven sometidas las empresas privadas, y porque no, de la tendencia mundial de la globalización, las empresas se han visto en la obligación de hacer grandes inversiones en el tema de la seguridad física.

Hoy en día este tema a tomado tal madurez, que ya no es visto como un problema en los presupuestos de las empresas los cuales incrementaban considerablemente los costos operacionales de estas, sino que están comenzando a percibirse como inversiones que permitirán una mayor eficiencia en los resultados y desempeño de la empresa.

Pero esta situación no es exclusiva de países como Colombia, en donde las condiciones de seguridad son un tema imperante para las empresas, sino que en países desarrollados como USA, Europa y algunos países de Asia, el tema de la seguridad se constituye en un factor integral en sus actividades, convirtiéndose de esta manera en los pioneros en esta área.

Las Fuerzas Militares de los EE.UU. vienen aplicando estos sistemas desde la década de los 80's. No es extraño encontrar instalaciones militares sin

ninguna clase de custodia ya que esta se realiza a través de un sistema de monitoreo electrónico custodiado por una sola persona.

Las inversiones en sistemas de control de acceso, CCTV, barreras perimétricas, sistemas de seguridad de área se convierten en una constante en el sector privado. No es difícil encontrar empresas en donde el proceso ingreso es más complicado que hacerlo en Ministerio de Defensa.

Los sistemas de detección perimetral, son en estos momentos herramientas fundamentales para prevenir o en algunos casos evitar que actos se cometan en contra de los intereses o patrimonio de las empresas.

Uno de los temas más preocupantes y que en estos momentos cobra mayor relevancia en el sector privado, es el tema de la seguridad de la información; paradójicamente en el sector público, este tema no se constituye en uno de los recursos vitales o estratégicos para las actividades propias de la unidad.

Para algunas empresas la información es el activo más valioso, por tal razón implementan esquemas de protección que van más allá de los convencionales.

Es absolutamente relevante generar conciencia sobre la implementación de tecnología aplicada a la protección perimetral y prevención de incidentes, adaptándonos a los cambios constantes del contexto de seguridad global.

De esta forma, esta actualización, nos permitirá estar a la vanguardia en y no alejarnos de la realidad y de los avances que la tecnología dispone a nuestro alcance para la obtención de resultados concretos que permitan finalmente cumplir con los objetivos finales de toda organización publica o privada.

Estos objetivos los enmarcamos en la protección de los intereses del negocio que no es otro que el de velar por las condiciones de seguridad de sus personas, bienes e intereses de tal forma que las actividades propias de la organización se puedan realizar libres de incidentes de seguridad.

No se puede ser ajeno a la tendencia de la globalización y lo que este concepto representa. Es por eso que las unidades militares deben propender por diseñar estudios y planes de seguridad, incluyendo todos los recursos existentes, que han sido implementados con efectividad en los países más adelantados y en las empresas más prosperas.

Las siguientes ilustraciones nos permiten obtener un alcance cercano, de la manera como las empresas del sector privado han implementado tecnología de punta, en sus sistemas de seguridad.

Estas fotografías fueron obtenidas gracias a la colaboración de la Compañía de Petróleos B.P. tanto en las instalaciones administrativas, como en el campo abierto.

Sistema de control biométrico para áreas de alta seguridad. Entrada presidencia BP Exploration. Bogotá D.C.

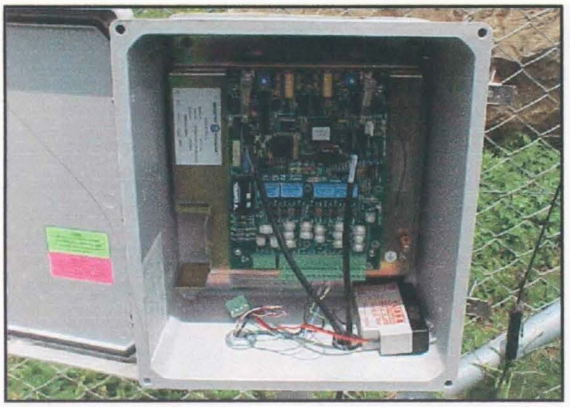
Malla de seguridad, con capacidad de absorber ondas explosivas, instaladas en los pozos de producción del un complejo petrolero en Casanare. BP. EXPLORATION.

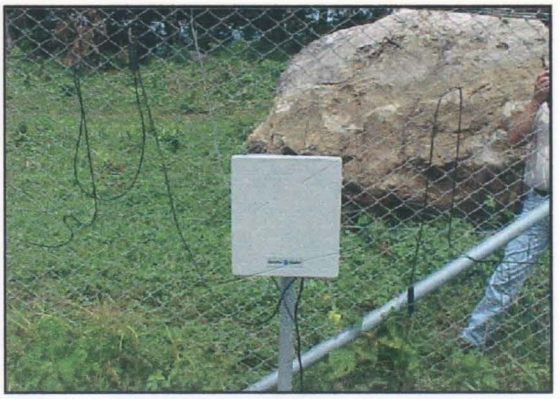
Vista panorámica de una malla de seguridad de absorción de onda explosiva. Pozo de producción complejo petrolero. BP

Sistema de detección de intrusión (Cable microfónico) Instalaciones Pozos de perforación complejo petrolero Casanare. BP EXPLORATION..

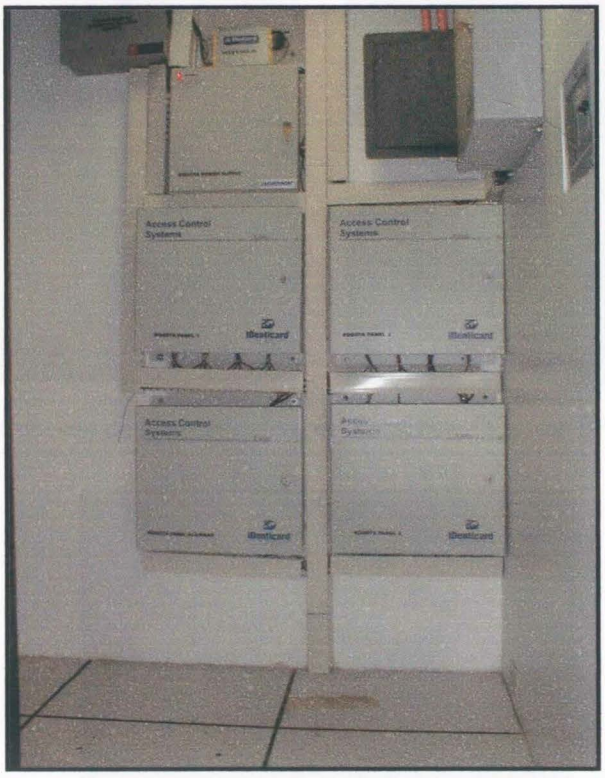
Doble malla de encerramiento de instalaciones. Complejo petrolero Cusiana Casanare. BP EXPLORATION.

Doble malla de encerramiento de instalaciones. Complejo petrolero Cupiagua Casanare. BP EXPLORATION.



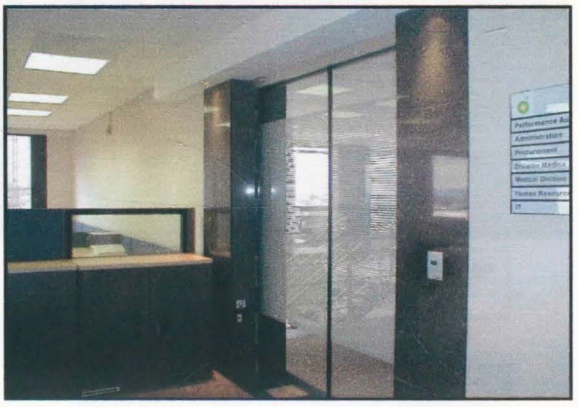


Unidad central de control sistema de detección de intrusión (Cable microfónico) Instalaciones Pozos de perforación. Complejo petrolero Casanare. BP EXPLORATION..

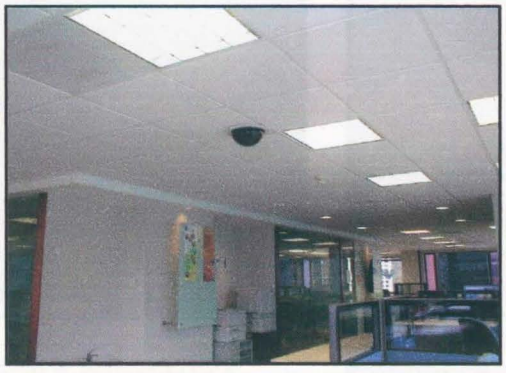


Unidades centrales de mando del sistema de control de acceso. Instalaciones OCENSA (Oleoducto Central).Bogotá D.C.

Sistema de control de acceso, mediante lector magnético. Oficinas OCENSA. Bogotá D.C.



Sistema de control de acceso de aproximación por sensores. Oficinas BP EXPLORATION.



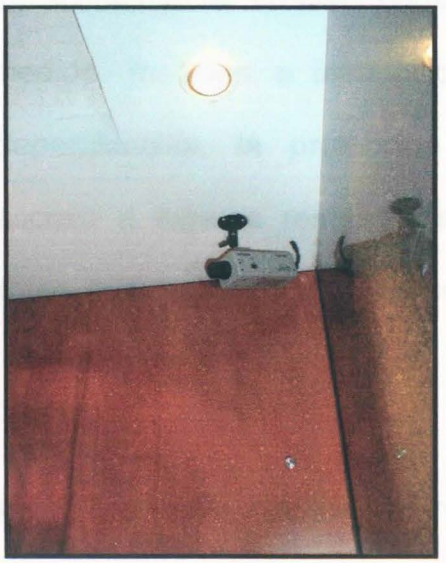
Domo de tecnología láser. Componente del sistema de CCTV. Oficinas BP EXPLORATION.

Sistema de detección electrónica oficinas BP EXPLORATION.

Sistema de detección de metales, oficinas BP EXPLORATION.

Sistema de control de acceso (torno) oficinas BP EXPLORATION

Sistema de CCTV oficinas BP EXPLORATION.



11. CONCLUSIONES

Los grupos armados al margen de la ley se han destacado como una amenaza con capacidad de llevar a cabo acciones terroristas, ocasionar graves daños a instalaciones militares, acceder a información clasificada y de pertinencia institucional, hurtar planes y documentación secreta, atentar contra los miembros de la institución militar y entre otras sabotear los sistemas de comunicaciones y de seguridad interna.

De manera consuetudinaria, las unidades militares han diseñado planes de seguridad interna, donde solo se han considerado la ubicación de puestos de vigilancia a través de una guardia de reacción, acudiendo al recurso humano, dejando de un lado la implementación de medios, medidas e instrucciones relacionadas con la protección física de dependencias, la protección de documentación e información, el control de acceso a lugares restringidos, la aproximación de personas y otra serie de factores que permiten establecer un sistema de seguridad integral.

Las empresas del sector privado en Colombia, han sido un ejemplo sobre la implementación integral de sistemas de seguridad, que les garantizan en un alto porcentaje, neutralizar los riesgos ocasionados por los agentes generadores de

violencia, los cuales son comunes para la empresa privada y las instituciones públicas. Los sistemas de control de acceso, el sistema de circuito cerrado de televisión, los sistemas sensóricos de vigilancia invisible, los sistemas de seguridad perimétrica y los sistemas de control de documentos e información digital, son medidas dignas de ser imitadas por las Unidades Militares, para reducir al máximo el riesgo a cualquier forma de agresión del enemigo.

Las grandes multinacionales del sector tecnológico han dedicado sus esfuerzos investigativos, a la búsqueda de nuevos y más efectivos sistemas electrónicos de aplicación multifuncional, para el servicio de la seguridad mundial. Dicha tecnología de punta se encuentra disponible en nuestro país para ser considerada e incorporada, en la medida de las necesidades y los recursos, a los planes de seguridad de las unidades militares en entornos rurales y urbanos, para obtener junto con el excelente capital humano orgánico de las Fuerzas Militares, sistemas de seguridad integrados, efectivos y verdaderamente funcionales.

12. RECOMENDACIONES

Una vez finalizado este proceso investigativo, me permito recomendar a los comandantes en todo los niveles de la organización militar, realizar con la participación directa de los oficiales de inteligencia y operaciones, estudios de seguridad integral, para implementar además de los puestos de centinelas que son la base de los planes de seguridad y reacción, medidas pasivas de seguridad, materializadas en toda una tecnología disponible para garantizar la protección de las personas, la información y las instalaciones, de las continuas formas de agresión de los grupos al margen de la ley. Además me permito recomendar, efectuar un análisis del material disponible en el mercado, en particular, controles de acceso, medios de seguridad perimetral, sistemas de circuito cerrado de televisión y sistemas de seguridad informática, para determinar cual de todos ellos, se ajusta a la misión, las necesidades, el presupuesto y el contexto, para ser incorporado al esquema de seguridad de todas las unidades de las Fuerzas Militares de Colombia.

BIBLIOGRAFIA

NOMBELA, Juan José. **Seguridad Informática**. Editorial Paraninfo, 1997.

EJERCITO NACIONAL. **Manuales de Seguridad y de Inteligencia Militar**. 1970 – 1998.

BURBANO Chavez, Oscar (Coronel). **Seguridad Física Empresarial**. Tipografía Dulcinea, 1996.

LA ROTTA, Luis Enrique (Coronel). **Impacto de la Seguridad en la Gestión Empresarial**. Conferencista. Revista Sicurex, 1994.

PEDRAZA C., Guillermo (Mayor) **Administración de la Seguridad**. Editores Bogotá, 1995.

VALLEJO Rosero, Silvio (Coronel) **Gerencia de Seguridad Preventiva**, 1995

ANEXO 1

EQUIPOS DE SEGURIDAD ESPECIALIZADOS

La siguiente es una relación de los equipos que actualmente están disponibles para la integración de los más novedosos, sofisticados y efectivos sistemas de seguridad.

- Activador silencioso alarmas antisecuestro. 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 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
- Polígrafo 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 análisis 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 laséricos – 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

ANEXO 2

DIRECCIONES DE PAGINA WEB DE LAS EMPRESAS QUE OFRECEN PRODUCTOS DE ALTA TECNOLOGIA AL SERVICIO DE LA SEGURIDAD.

- www.americansecurity.com.co
- www.info-safe-com
- www.diebold.com
- www.anti-terrorism.com
- www.tycoint.com.co
- www.Pelco.com
- www.magal-ssl.com