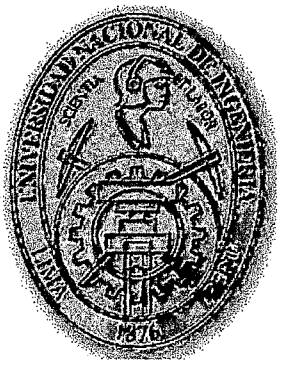
UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS



SISTEMA INTEGRAL INTELIGENTE DE SEGURIDAD EN EDIFICIOS DE USO TELEFÓNICO

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO INDUSTRIAL

FREDY MARSOLINY BECERRA CAPILLO

LUIS ALBERTO GARCÍA VARGAS

LIMA - PERÚ

2000

DEDICATORIA

Para mis adorados padres por su infinito amor a quienes les debo todo lo que tengo y soy; y a mis dos hermanos por todo su apoyo y comprensión.

Fredy Becerra Capillo

A mi madre por sus consejos y por su gran amor; a mi padre a quien admiro por su dedicación al trabajo; y a mis queridos hermanos.

Luis García Vargas

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

DESCRIPTORES TEMÁTICOS

01. Red Telefónica
02. Telecomunicaciones
03. Gestión de Riesgos
04. Medidas de Seguridad Electrónica
05. Medidas de Seguridad Física
06. Medidas de Seguridad Humana
07. Medidas de Seguridad Económicas
08. Sistema Integral Inteligente de Seguridad
09. Diseño de Sistemas de Seguridad
10. Análisis Costo Beneficio de Sistemas de Seguridad

SUMARIO

El presente trabajo de tesis busca medir las ventajas técnicas y económicas de la implantación de un Sistema Integral e Inteligente de Seguridad en empresas de telecomunicaciones para proteger sus activos, sus empleados y sus clientes en lugar de usar un sistema de seguridad basado únicamente en agentes vigilantes.

Específicamente nuestro estudio se centrará en la protección de Instalaciones Remotas de Uso Telefónico. Se propone para ello una metodología que comprende los siguientes procesos : Identificación del bien, Identificación de riesgos, Análisis de riesgos, Evaluación de riesgos, Políticas ante los riesgos y diseño de las Medidas de seguridad.

La metodología aplicada es el proceso para lograr la implementación de un sistema de seguridad de acuerdo a una visión moderna.

Como producto de la elaboración de esta tesis hemos podido concluir que se puede elevar la calidad del sistema de seguridad y reducir los costos de éste a través de la implantación de un Sistema Integral Inteligente de Seguridad en lugar de usar los servicios de agentes de vigilancia únicamente. Además recomendamos el uso de la tecnología y conocimientos económicos en el diseño de sistemas de seguridad por su impacto económico y de eficiencia.

INTRODUCCIÓN

Como es cada vez más público y notorio, la seguridad es un concepto muy utilizado, e incluso manipulado en nuestros días, no obstante, es un concepto tan antiguo como el propio hombre. En cualquier caso, no es preciso entrar en detalle de cómo ha evolucionado este concepto, su significado e importancia, principalmente en las últimas décadas en torno a los cambios que se han ido produciendo a nivel social, político y económico.

Pero tampoco debemos olvidar la creciente preocupación por la seguridad que, durante años nos ha hecho tomar conciencia de la situación real, es decir, la necesidad de la protección, concepto antiguo y ligado igualmente al hombre, a su existencia y a su desarrollo económico y social.

Por otro lado, no son nuevos la mayoría de los riesgos y amenazas con los que convivimos diariamente, tan sólo cabria decir que van cambiando en su valoración e incluso en sus parámetros de estudio y tratamiento (tipo y nivel de riesgo, entorno social, agresividad de ambiente, causas desencadenantes imprevistas, etc.).

Todo ello, sin olvidar que la seguridad es un estado de animo, una cualidad intangible. Aunque tampoco finaliza aquí, puesto que esta situación puede derivar en situaciones y, sobre, todo, en consecuencias de carácter físico o material.

La seguridad, en su definición y aplicación más básica, es un objetivo, es un fin y no un medio que el hombre anhela constantemente como una necesidad primaria. Pero en la últimas décadas, la búsqueda de algunas seguridades de marcado carácter social se ha desarrollado de manera muy especial. Este espectacular desarrollo ha generado, en general, un cierto confusionismo que, unas veces derivado de la falta de preparación y análisis de los distintos grupos humanos o profesionales, y otras veces porque los intereses legítimos que se encuentran en juego, ha conseguido mediatizar en su adecuada evolución.

El hombre tiene conciencia empírica, es decir, tiene una acumulación de experiencias propias y ajenas, de los riesgos, de los peligros y amenazas, potenciales y reales con los que convive en su entorno habitual (ambiente natural y social). Obviamente, como consecuencia directa de esta afirmación, las personas siempre se han sentido y se sentirán inseguras e, incluso, angustiadas y por tanto surge la necesidad de la seguridad que despeje sus miedos, que liberen sus angustias con el objetivo primario de su tranquilidad vital o lo que es lo mismo, la consecución de una seguridad intima, primaria y psicológica.

La seguridad en el hombre es un aspecto primario y psicológico, tan necesaria y tan importante como la autoestima, la posesión, etc., y esta necesidad de seguridad surge consciente e inconscientemente de manera permanente.

La seguridad es ante todo liberación y estas liberaciones que nos dará la seguridad pueden ser definidas en su conjunto como una relación de situaciones de carácter cotidiano que se pueden materializar en el desarrollo de nuestra vida. Por ejemplo la ley es muy clara en el artículo 2 inciso 9 respecto a la seguridad de las instalaciones de propiedad privada, en donde se interpreta que: La inviolabilidad del domicilio es el derecho del ocupante

legítimo de utilizar exclusivamente el lugar donde vive o trabaja, de manera que solo él o la persona a quien autorice pueda ingresar.

Las Empresas de Telecomunicaciones por el servicio que prestan a la sociedad o por las consecuencias negativas asociadas a su eliminación total o parcial, son objetivos apetecidos por delincuentes que por razones diversas buscan hacer daño a la empresa. Tales acciones tienen normalmente su origen en:

- El llamado terrorismo en sus aspectos más variados.
- Las crisis laborales o sociales en la que intervienen elementos incontrolados.
- Las revueltas callejeras que pueden terminar en actos vandálicos producidos también por cierta clase de individuos.

Ante estas amenazas es necesario que las instalaciones de telecomunicaciones se defiendan en forma activa y pasiva mediante la aplicación de medidas de seguridad que si bien no erradican el mal (misión y decisión que pertenece al campo político, judicial, policial o cultural), sí disminuyen o anulan las consecuencias nefastas de los actos delictivos, evitando males a la integridad de los trabajadores, clientes y bienes de dichas instalaciones. Estas medidas de seguridad se deducen de los estudios de seguridad y su viabilidad son función de: la amenaza a enfrentar y el grado de protección que se quieran conseguir.

Tradicionalmente se han utilizado medidas para brindar seguridad en las instalaciones basados única y específicamente en el hombre, los cuales han quedado insuficientes principalmente por las limitaciones de la naturaleza humana, debido a la complejidad de las instalaciones. Factor importante que ha llevado a la búsqueda de nuevas medidas de seguridad más eficaces, que disminuyan los riesgos y/o sus efectos., tales como

medidas físicas, electrónicas y económicas.

La seguridad debe ser considerada como una de las actividades de mayor importancia dentro de la empresa y debe abarcar :

- **Protección contra incendios**, la incertidumbre de que podemos quedar involucrados en situaciones de siniestros, fuera de nuestro control, demanda la necesidad de establecer medidas para disminuir al mínimo sus efectos.

- **Protección contra hurtos y sustracciones**, considerando que las debilidades humanas pueden permitir emplear al hombre en la realización de actos de hurto, vandalismo, espionajes, fraude, etc., con fines ocultos, es que nos demanda la necesidad de establecer medidas adecuadas que permitan proteger la propiedad.

- **Protección contra actos externos**, ciertas manifestaciones individuales o grupales de descontento, de rebeldía, de ideología, de desesperación o desorden social se han sumado a los campos de seguridad de las instalaciones; para lo cual se establecerán medidas de seguridad a fin de prevenir estas manifestaciones expresadas en atracos, asaltos, terrorismo, secuestro y otras modalidades.

El paso lógico es el establecimiento de un sistema de seguridad que combine las medidas humanas, físicas, electrónicas y económicas de acuerdo a las amenazas a enfrentar con aplicaciones de ingeniería.

CAPÍTULO I

ASPECTOS GENERALES

1.1 LAS TELECOMUNICACIONES

Se da el nombre de telecomunicaciones a aquellos sistemas eléctricos que permiten que las personas entre sí, o con las máquinas, intercambien a distancia mensajes audibles, escritos o visuales. Ejemplo de ello son los servicios de telefonía, telegrafía, teleproceso, transmisión de datos y televisión.

Además de brindar estos servicios, las telecomunicaciones están en capacidad de ofrecer otros variados servicios como recepción y transmisión de mensajes, telefonía móvil, radiolocalización y vídeo teléfono.

Cabe agregar que los últimos avances de la tecnología en el campo de los medios ópticos de transmisión, de las centrales de conmutación controladas por programa almacenado y de transmisión global vía satélite van rápidamente diversificando los servicios que las telecomunicaciones ponen a disposición de los usuarios, haciendo que actualmente las telecomunicaciones sean la herramienta más importante para cualquier tipo de organización: una empresa, una universidad, una municipalidad, un club, etc.

1.1.1 IMPORTANCIA

Las agencias de noticias y las empresas periodísticas se valen de las telecomunicaciones para enviar sus boletines noticiosos o recepcionar el material informativo; las empresas industriales, bancarias y los agentes de bolsa, se valen de las telecomunicaciones para enterarse de los índices financieros que servirán de base a sus transacciones; las empresas públicas o privadas, oficinas administrativas del gobierno central y local se valen de las telecomunicaciones para su gestión administrativa. No sería posible que las modernas aeronaves se aproximaran a los grandes aeropuertos sin las telecomunicaciones.

Las telecomunicaciones por sí solas se han convertido en vía principal del desarrollo, acelerando el intercambio comercial, cultural y tecnológico, permitiendo la conjugación de esfuerzos a través del acercamiento de las gentes, aumentando el nivel de vida de la población al permitirle trabajos más productivos, en una palabra fomentando el desarrollo.

En un país en vías de desarrollo como el Perú, el mejoramiento de las telecomunicaciones constituye a la vez un apoyo, un acicate para el progreso. Sin buenas comunicaciones no podremos aspirar a mantener el ritmo de progreso que se requiere en nuestra época para lograr una posición competitiva y destacada dentro del consenso mundial. Cabe destacar otro aspecto sumamente importante, el cual es la integración a la vida económica del país de un gran número de localidades que se encuentran actualmente marginados, vale decir que las telecomunicaciones cumplen además una función social que ha de redundar en forma indirecta sobre el crecimiento de la actividad económica.

En las últimas décadas se han desarrollado los sistemas de computación electrónica de datos que multiplican algunos aspectos de

capacidad mental del hombre y se han convertido en herramienta indispensable para la toma decisiones.

Las telecomunicaciones a través del teleprocesamiento de datos amplían enormemente el uso de las computadoras tanto en su radio físico de acción como en el uso oportuno de grandes cantidades de información y divulgación de los resultados donde y cuando son útiles, permitiendo además la interconexión directa de diversos sistemas de procesamiento especializado en la solución de problemas de diversa índole.

Podemos sintetizar el rol de las telecomunicaciones como un apoyo imprescindible al desarrollado de las actividades de todos los sectores del país. Sin embargo, es necesario señalar que el desarrollo de los servicios de telecomunicaciones impone grandes inversiones y la movilización masiva de recursos humanos y materiales.

1.1.2 SERVICIOS BRINDADOS POR LAS EMPRESAS DE TELECOMUNICACIONES

El grado de desarrollo de las actuales redes de telecomunicación permite ofrecer al usuario una atractiva gama de servicios de telecomunicaciones orientados tanto al usuario de tipo residencial como al de tipo profesional o comercial.

Los servicios actuales mas generalizados a nivel mundial son los siguientes:

1.1.2.1 SERVICIOS TELEFÓNICOS

Los servicios telefónicos se pueden dividir en :

- Servicios normales telefónicos
- Servicios especiales telefónicos
- Servicios de funciones inteligentes

1.1.2.2 SERVICIOS TELEMÁTICOS

Son servicios de comunicación de datos usuario a usuario. Los tipos de información son : escrita, gráfica y cualquier dato en general.

- Teletex
- Facsímil
- Vídeotex
- Transferencia electrónica de fondos (cajeros automáticos, terminales punto de venta).
- Modo mixto (Faxtex)

1.1.2.3 SERVICIOS DE VALOR AÑADIDO

Proporcionan funciones adicionales a la simple comunicación entre terminales de usuario, como las de almacenamiento, proceso y distribución o difusión de información, tales como:

- Mensajería telemática
- Mensajería de voz
- Interfuncionamiento de servicios telemáticos
- Servicios de base de datos

1.1.2.4 SERVICIOS DE TELECONFERENCIA

Los servicios de teleconferencia se pueden dividir en:

- Audioconferencia
- Videoconferencia

1.1.2.5 SERVICIOS DE TELEACCION

Permiten la supervisión o actuación en tiempo real sobre un determinado conjunto de elementos, susceptibles de ser controlados a distancia, a través de redes de telecomunicación, tales como:

- Telealarmas
- Telecontrol
- Telemedida

1.1.2.6 SERVICIOS MÓVILES

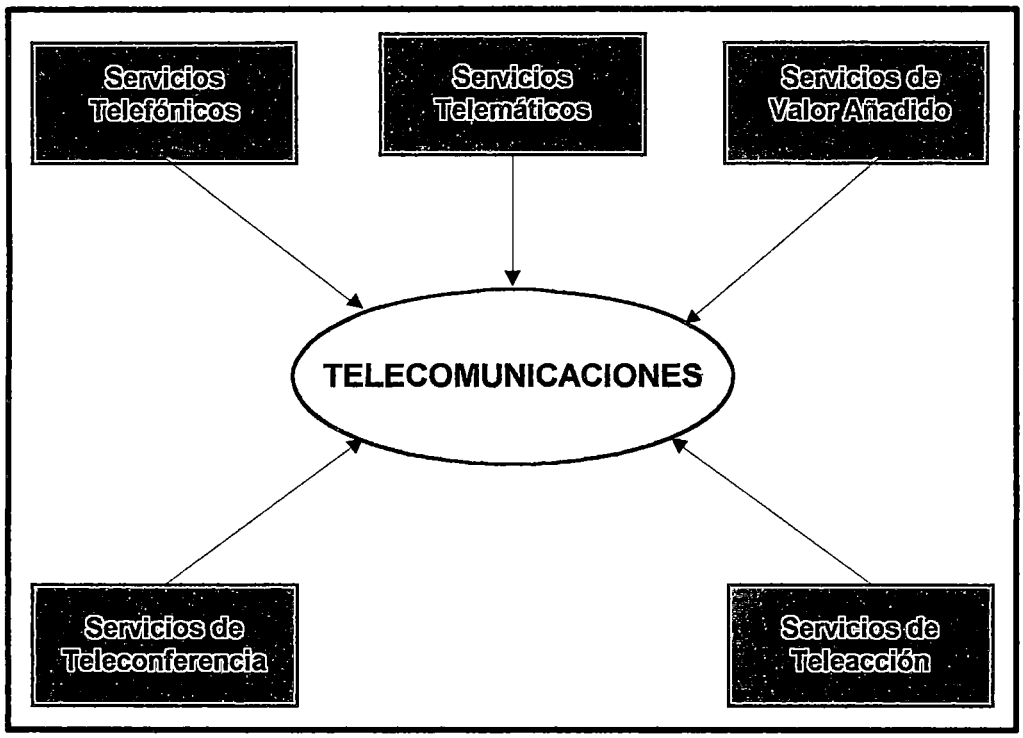
Estos servicios se clasifican como:

- Servicios móviles terrestres
  - * Telefonía móvil automática
  - * Radiobúsqueda
  - * Mensafonía
  - * Radiotelefonía privada

- Servicios móviles marítimos
  - * Telefonía
  - * Telex
  - * Telegrafía

- Servicios móviles aéreos

Gráfico 1.1: Servicios de Telecomunicaciones



Fuente : Elaboración Propia

1.1.2.7 SERVICIOS DE DISTRIBUCIÓN

Suministran información a sus abonados de una forma unidireccional desde estaciones o puntos centralizados de las reales que los soportan. Los tipos de información suministrados consisten fundamentalmente en programas musicales y programas de TV, tales como:

- Audiodistribución
- Videodistribución

1.1.2.8 SERVICIOS DE TELEX

- Servicio de telex básico
- Servicios especiales telex

1.1.3 RECURSOS DE LAS EMPRESAS DE TELECOMUNICACIONES

Según la UITT la distribución promedio de la inversiones, de acuerdo con un estudio realizado para 16 países es la siguiente:

Tabla 1.1 : Distribución de la Inversión en las Empresas de Telecomunicaciones

PLANTA	DESCRIPCIÓN	% DE INVERSIÓN
EXTERNA	Instalaciones de abonados	13%
	Redes locales de líneas de abonado	27%
INTERNA	Centrales	27%
	Circuitos de larga distancia	23%
	Edificios y terrenos	10%

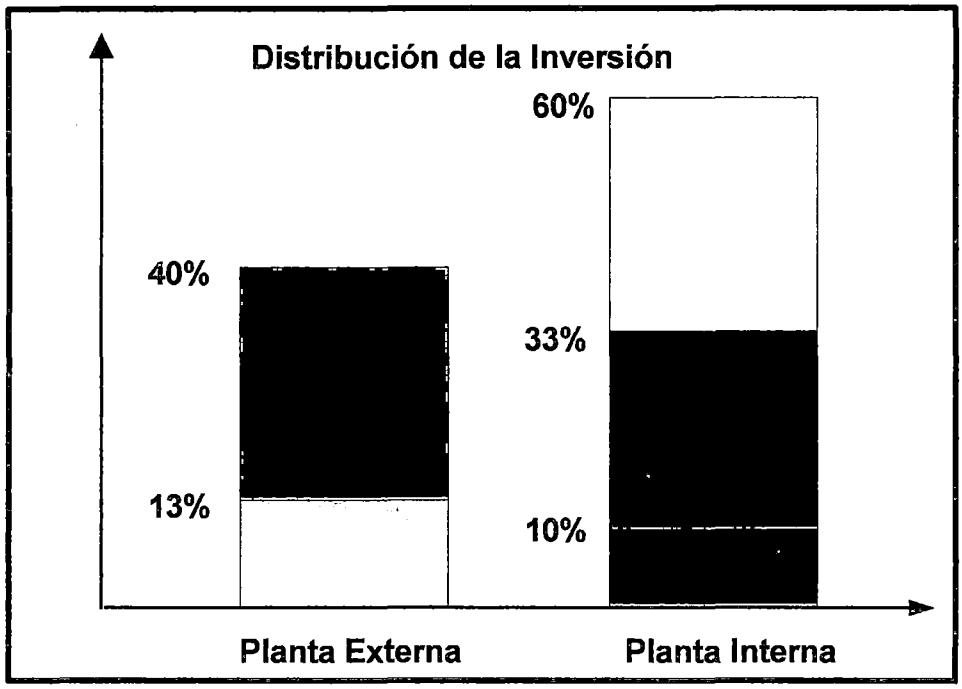
Fuente : UITT

De la tabla anterior se deduce que la Planta Externa necesita una inversión igual al 40% (suma de los dos primeros ítems de la tabla: instalaciones y redes locales), y la Planta Interna necesita la inversión más alta igual al 60%, dividida en: Conmutación que tiene una inversión igual al 37% (suma del tercer y quinto ítem de la tabla: centrales y edificios y terrenos) y Transmisión, que necesita un inversión igual al 23%, basado en el valor de los circuitos de larga distancia. Las Centrales Telefónicas están constituidas principalmente por cuatro grandes recursos:

- Conmutación
- Transmisiones
- Energía
- Cable Submarino.

A continuación se muestra la gráfica de esta distribución:

Gráfico 1.2: Distribución de la Inversión en Sector de las Telecomunicaciones



Fuente: Elaboración Propia

1.1.3.1 Conmutación

Esta comprendido por todas aquellas centrales digitales o analógicas que permiten la interconexión entre dos abonados.

1.1.3.2 Transmisiones

Comprende cualquier tipo de medio que permita la comunicación entre dos centrales como puede ser: Ondas de radio, fibra óptica, satélite. Se clasifica en tres grandes rubros:

- **Sistema de transmisiones**, que abarca todos aquellos sistemas que enlazan físicamente como puede ser un cable de fibra óptica, a diferentes velocidades los rangos de velocidades es de 2, 8, 34, 140, 155, 565,622 mbps hasta 2.5 gbps.

- **Sistemas de radio**, que abarca todos los equipos de radio analógico - digitales tanto de baja capacidad que comprende equipos de UHF, VHF, y equipos de radio de una velocidad de transmisión de 2 y 8 mbps; los equipos de mediana y alta capacidad son equipos cuyas velocidades de transmisión son de: 17, 34, 140 y 155 mbps.
- **Sistemas MAR**, comprende todos aquellos equipos de radio de baja capacidad que forman parte de la Red de Multiacceso Radial.

1.1.3.3 Energía

Estos equipos dentro de la planta de telefónica están agrupados en cuatro grandes grupos:

- **Aire Acondicionado**, son los equipos que permiten mantener los equipos de una central a una temperatura estable para su conservación y explotación.
- **Grupos Electrógenos**, son los equipos que permiten suplir la energía comercial permitiendo el normal funcionamiento de la central.
- **Rectificadores**, son los equipos que permiten convertir la energía comercial que viene como corriente alterna a corriente continua para que pueda entrar a la central.
- **Baterías**, son los equipos que se utiliza en las centrales cuando la energía comercial se corta.

1.1.3.4 Cable Submarino

Es un cable de Fibra óptica de 7,310 kilómetros de longitud el cual esta interconectada a la Red Mundial de Cables Submarinos.

1.2 ASPECTOS GENERALES DE LAS EMPRESAS DE TELECOMUNICACIONES EN EL PERÚ

1.2.1 ANTECEDENTES

A inicios de los noventa, en el Perú ocurrió un cambio conceptual sobre el papel del Estado en una economía de libre mercado. Se transfirió entonces al sector privado, la responsabilidad de desarrollar las actividades productivas y los servicios, mientras que el Estado se reservó para sí la función de promotor y regulador de la inversión privada, y también mantuvo la potestad de establecer mecanismos para evitar las prácticas de competencia desleal.

El sector de telecomunicaciones no fue ajeno a estas transformaciones. Su modernización empezó con la promulgación de la Ley de Telecomunicaciones (Decreto Legislativo 702, Noviembre de 1991), en virtud de la cual se creó legalmente OPSITEL en sustitución de la Comisión Reguladora de Tarifas de Telecomunicaciones. En 1993 OPSITEL inició sus actividades y también se publicó el Texto Unico Ordenado de la Ley de Telecomunicaciones.

A OPSITEL se le asignó las funciones de promover una competencia efectiva y leal; resolver controversias por la vía administrativa entre prestadores de servicios portadores, finales, de difusión y de valor añadido; asesorar al Ministerio de Transportes, Vivienda y Construcción en el otorgamiento de autorizaciones, permisos y licencias; fijar las tarifas de los servicios públicos de telecomunicaciones y administrar el Fondo de Inversión en Telecomunicación (FITEL).

En enero de 1994, la Ley 26285 dispuso la desmonopolización progresiva de la telefonía local y de los servicios portadores de larga

distancia nacional e internacional. Un mes más tarde, se aprobó el Reglamento de la Ley de Telecomunicaciones.

En Febrero de ese mismo año, se vendió un paquete de acciones del Estado en la Compañía Peruana de Teléfonos S.A. (CPT) y ENTEL Perú S.A., monopolios estatales de los servicios de telecomunicaciones en Lima y provincias, respectivamente. La subasta fue ganada por Telefónica Internacional de España (TELEFÓNICA), cuya oferta ascendió a 2,002 millones de dólares, cifra muy superior al precio base de 546 millones de dólares y a las ofertas de sus competidores. El Estado recaudó por este concepto 1,392 millones de dólares, y los 610 millones restantes fueron destinados a aumentar el capital de la antigua CPT en 23.3%.

El 16 de Mayo de este mismo año, Telefónica hizo efectivo el pago del monto ofrecido y se firmaron los contratos de concesión por un plazo de veinte años contados a partir del 27 de Junio de 1994

En los contratos de concesión se fijaron una serie de compromisos para la empresa concesionaria. Entre otros puntos, se contempló la expansión del servicio fijo local, el crecimiento de líneas instaladas y teléfonos públicos, la mejora en la calidad de los servicios, la sustitución de las centrales manuales por digitales y un programa de rebalanceo tarifario.

En las condiciones de la subasta se estableció que el futuro operador podía fusionar ambas empresas, luego de cumplir con los trámites definidos en la Ley General de Sociedades. La fusión debía realizarse durante el primer año y medio del período de rebalanceo, y en una proporción de valor de 55% para CPTSA y 45% para ENTEL Perú. En Diciembre de 1994 se concretó la fusión: ENTEL Perú fue absorbida por CPT. Un año después, por acuerdo de la Junta General Extraordinaria de Accionistas, cambio su denominación a Telefónica del Perú S.A.

Con los contratos, el Estado otorgó a Telefónica del Perú la concesión para prestar el servicio telefónico en el ámbito nacional y para operar los servicios de larga distancia nacional e internacional.

Asimismo, se estableció un período de concurrencia limitada, o de exclusividad en los servicios mencionados, que debía concluir en Junio de 1999, pero como veremos su vigencia concluyo un año antes de lo previsto gracias al cumplimiento adelantado de los términos pactados con el Estado.

Desde que Telefónica inició sus actividades se han realizado grandes avances en el sector de las telecomunicaciones, dando acceso a modernos productos y servicios a todos los niveles socioeconómicos del país. En Lima se han sustituido 168,324 líneas de centrales manuales por automáticas, con lo que se ha superado la meta contractual de 135,000 líneas en un 34%. En provincias igualmente se superó en un 82% sobre la meta impuesta, al haberse sustituido 136,539 líneas. En cuanto a la instalación de teléfonos públicos, Telefónica ha sobrepasado en 175% la meta impuesta en Lima, mientras que superó en un 60% la meta señalada para las provincias. En estos momentos se supera los 50,000 teléfono públicos, a nivel nacional.

En Julio de 1996, se produce una gran evolución en los servicios de transmisión de datos en el Perú, Telefónica lanzó los servicios Inter Lan, Uni Red e Info Vía. Los dos últimos hacen posible el desarrollo de los servicios Internet en el país, al poner la información e intercomunicación mundial al alcance de todos los peruanos en forma económica, sencilla y universal. Actualmente Info Vía/ Internet tiene alrededor de 120,000 usuarios en el Perú.

Además, Telefónica ha incorporado otros servicios en el mercado nacional, tales como la Red Inteligente (0800 - cobro revertido, 0808 - audio

servicios de valor añadido), la Red Digital de Servicios Integrados (RDSI) y los servicios satelitales. Esto permite que el Perú se encuentre en la actualidad entre los países más desarrollados en telecomunicaciones de América del Sur.

Como se mencionó anteriormente el progreso alcanzado por las telecomunicaciones determinó que un año antes de lo previsto se abriera el mercado a la competencia. Al respecto, en Agosto de 1998, se promulgaron los Decretos Supremos 020-98-MTC y 021-98-MTC que regulan esta apertura, la que se debió sobre todo a que Telefónica, adelantándose al plazo fijado de cinco años, cumplió en forma satisfactoria y superó todas las metas fijadas en los Contratos de Concesión.

Esta apertura total del mercado ha significado poner en vigencia un nuevo sistema de tarifas, que se encuentran debajo del promedio de la región, además de poner al servicio de los clientes un conjunto de nuevos productos que los beneficiará directamente. Por otra parte, se ha puesto en funcionamiento la tarifa intra departamental que hace posible que la llamada cueste igual que una llamada local dentro de una misma área departamental.

Además, desde el año 2000, los clientes podrán elegir a los proveedores de servicios de larga distancia nacional e internacional de su preferencia.

En la actualidad, el Gobierno ha otorgado concesión a 17 nuevas empresas para prestar servicios portadores nacionales y a 16 para prestar servicios portadores internacionales. La libre competencia propiciará asimismo, la prestación de variados servicios con tecnología de punta, tales como voz, videoconferencia, multimedia y transmisión de datos en banda ancha, a través de redes IP, "Frame Relay" y/o ATM, incluyendo la red mundial Internet y las redes inalámbricas vía satélite.

Actualmente los clientes demandan una mayor calidad y diversidad de servicios, lo que implica un reto cada vez mayor para las operadoras. Es por ello que la puesta en funcionamiento, el 19 de Febrero de 1999, del Cable Submarino Panamericano de Fibra Óptica, cuya administración está a cargo de Telefónica, como principal promotora e inversor de este proyecto, constituye un avance sin precedentes en el país. Gracias a la puesta en marcha de esta obra, la red peruana se encuentra interconectada mediante fibra óptica con otros países de Latinoamérica, Estados Unidos, Europa y el resto del mundo. Esto permite brindar una insuperable calidad en las comunicaciones internacionales a una velocidad impresionante de 2,5 Gigabips y transmitir en forma simultánea más de 30,000 conversaciones.

1.2.2 MERCADO DE LAS TELECOMUNICACIONES EN EL PERÚ

Actualmente el mercado de las telecomunicaciones está conformado por los siguientes servicios:

1.2.2.1 LARGA DISTANCIA NACIONAL E INTERNACIONAL

Actualmente existen dos empresas en telecomunicaciones : Telefónica que ya viene operando en este mercado y Tele2000 a la cual recientemente se la ha dado la licencia para operar por espacio de 20 años.

1.2.2.2 PORTADOR EN LIMA Y PROVINCIAS

Proporciona la capacidad de transporte de señales e interconexión de redes y servicios dentro de una misma área urbana. En Lima existen tres empresas, Telefónica que opera en Lima y Provincias, Tele2000 que ya entró a operar en base a su red de fibra óptica con 20 nodos de tecnología digital

y con el 100% de su red radial, así como Resetel que ya empezó a operar con su red de fibra óptica.

En Telefonía móvil Lima y Provincia existen dos competidores actualmente, Telefónica y Tele2000.

1.2.2.3 SERVICIO TRONCALIZADO O DE CANALES MÚLTIPLES DE SELECCIÓN AUTOMÁTICA

Consiste en la transmisión de comunicación privada vía radio, por medio de una central y diversos canales de frecuencias, desde un punto cualquiera a distintos puntos, sean estos fijos o móviles. Este sistema brinda facilidad de comunicación y nitidez a bajo costo para los usuarios. Sus mayores usuarios son los servicios de seguridad, las actividades comerciales y en gran medida en los servicios de taxis.

A pesar de que su presencia es reciente en el Perú, se tiene cerca de 11 compañías, a la fecha se han entregado en concesión 319 canales y existen otros 200 disponibles en Lima, sin embrago la demanda excede al oferta habiéndose solicitado más de 1200 canales, provenientes de 23 empresas. Por este motivo y considerando que es necesario administrar eficientemente el espectro radioeléctrico, el Estado peruano resolvió que la concesión de servicios troncalizados en Lima, se otorguen por concurso público de ofertas.

1.2.2.4 BUSCAPERSONAS

Lejos de verse afectado por la competencia de los teléfonos celulares, como ha sucedido, se ha mantenido en un segundo segmento de mercado, para quienes el servicio de celular es muy costoso. La exigencia del mercado ha estimulado que las empresas incorporen nuevos servicios a los beepers,

una de esas es la firma del convenio entre Mastercall y la Red Científica Peruana, con el fin de interconectar el servicio de buscapersonas con mensajería electrónica vía Internet.

Existen 75 mil usuarios, quienes realizan el 90% de sus comunicaciones dentro de su localidad, y el 10% restantes en forma interprovincial. Esperándose un crecimiento para el presente año del 35%.

Existen actualmente 26 empresas autorizadas a operar el servicio buscapersonas. Las mayores empresas del rubro son: Martercall, cuya participación estimada asciende al 30% del mercado; Skytel (Tele2000) que cubre el 25% del mismo; Natar 20% y Mensatel (Telefónica) con el 10%.

1.2.2.5 TELEVISIÓN POR CABLE

En el caso de Telefónica del Perú, a pesar de que los ingresos obtenidos por la televisión por cable sólo representan el 4% del total, este rubro fue el de mayor crecimiento en 1996. Para ampliar su cobertura, obtuvo la concesión para operar el servicio en provincias. El número de clientes de cable mágico aumento en mas de cinco veces llegando a 100 mil usuarios, habiendo extendido sus servicios a 21 distritos adicionales, ampliando también su programación llegando a 101 canales.

La segunda operadora de televisión por cable es Tele2000, a través de su servicio de Telecable, ofreciendo 90 canales y llegando a 70 mil usuarios.

1.2.2.6 SERVICIOS DE VALOR AÑADIDO

Se define a trece tipos que son: Facsímil, videotex, teletex, teletexto, teleacción, telemando, telealarma, almacenamiento y retransmisión de datos,

teleproceso y procesamiento de datos, mensajería interpersonal, mensajería de voz, servicio de consulta y servicio de conmutación de datos, las empresas que operan este servicio no están sujetas a concesión, únicamente deben de cumplir con inscribirse en los registros.

Existen actualmente 36 empresas registradas, las cuales ofrecen servicios de consulta a base de datos (incluyendo 16 empresas que ofrecen acceso a Internet), Correo Electrónico (24%) y Facsímil(8%).

1.2.3 LAS NUEVAS CONCESIONES

El Estado ha otorgado en 1999, las primeras ocho concesiones para prestar el servicio de larga distancia nacional e internacional, que antes estaba a cargó en exclusividad a Telefónica.

Las primeras concesiones fueron entregadas el 22 de Enero de 1999, a un grupo de empresas que demostraron la seriedad y solidez necesarias para atender esta necesidad tan importante.

Las Empresas : Tele2000, Firstcom, Global Village Telecom y Ormeño Comunicaciones Perú, fueron las cuatro primeras empresas concesionarias. Y el 19 de marzo de 1,999 , continuando con esta nueva decisión de apertura se otorgo otras concesiones adicionales a cuatro empresas especializadas: Compañía Telefónica Andina, Nexfax Technologies Insatel S.A.C., Nortek Comunicaciones S.A.C. y Telepuerto Internacional del Perú S.A.

Las prestaciones de servicios de estos nuevos operadores de larga distancia nacional e internacional abarcarán en principio, las ciudades de Lima, Piura, Tumbes, Chiclayo, Trujillo, Chimbote, Huancayo, Arequipa, Cajamarca, Ucayali e Ica. Ampliándose posteriormente a otras ciudades como Cusco, Puno y Tacna.

1.2.4 INVERSIONES A LARGO PLAZO

La Inversión proyectada de estas primeras ocho empresas concesionarias asciende en conjunto a 23 millones 506 mil 788 dólares, sólo para el primer año de las operaciones y a 83 millones 397 mil 410 dólares para los cinco primeros años de operación. Adicionalmente otras catorce solicitudes - al momento de finalizar este trabajo se encuentran en trámite para prestar servicio de larga distancia nacional e internacional, lo que indica el interés sostenido del empresariado por participar estas.

De otro lado, se ha dado la concesión a Tele2000 el día 20 de junio de 1999 para el sector de telefonía fija local.

1.2.5 PROYECCIONES DE INVERSIÓN EN EL PERÚ EN EL SECTOR DE LAS TELECOMUNICACIONES 1999 – 2000

Se ha proyectado para el período 1999-2000 la inversión en servicios públicos de telecomunicaciones bordeará los mil millones de dólares. A la fecha se tiene previsto para este período compromisos de inversión y proyectos por el orden de los 446 millones de dólares.

Hasta finalizar el año 2000 se debe de alcanzar la densidad de 14 líneas telefónicas por cada 100 habitantes, y de 20 líneas para el año 2002. También, completar íntegramente la digitalización de las redes y ampliar la cobertura en las prestaciones de servicios de telecomunicaciones a 1,600 nuevas localidades.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 ANTECEDENTES

Podríamos decir que la seguridad "Estado ideal, libre y exento de todo peligro, daño o riesgo" ha existido siempre como meta, utilizando la protección como medio para conseguirla, de ahí que desde los tiempos más remotos tanto las colectividades u organizaciones humanas, como los propios individuos, han buscado ese estado a través de la protección ante algo o contra algo; sin considerar o analizar los altos costos de la seguridad en base a vigilantes únicamente, los que muchas veces podrían superar los beneficios y además sin que lleguen a cubrir totalmente las amenazas.

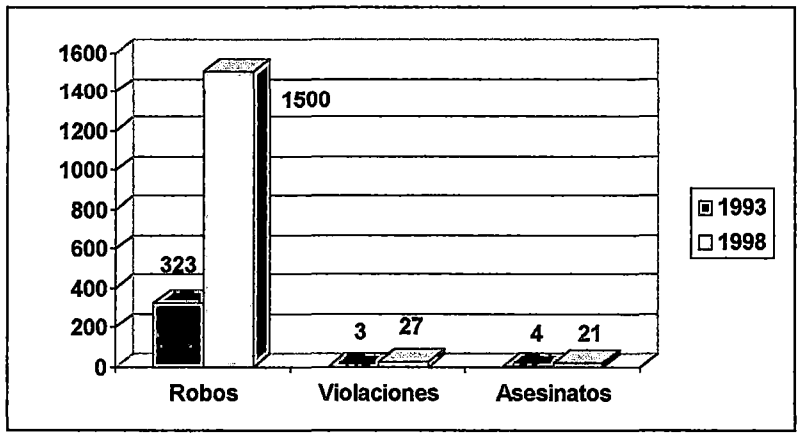
Los motivos por los cuales se debe invertir en un sistema de seguridad que reemplace al sistema tradicional y que sea eficiente en cubrir todos los riesgos y de menos costo, se fundamenta en lo siguiente:

2.1.1 ALTO ÍNDICE DE DELINCUENCIA EN EL PERÚ

Los peruanos de hoy, y específicamente los limeños, tienen miedo de un mal que fulmina, hiere, veja, aterroriza, despoja y destruye. Este estudio de la violencia, con cifras oficiales, revela que la criminalidad crece

aceleradamente, a un ritmo anual de 25% en promedio, aunque entre 1997 y 1998 el nivel fue de 47%, porcentaje según la INTERPOL. Durante 1993 en Lima se cometían 323 robos diarios, hoy sobrepasa de 1500. Se asesinaba a 4 personas, hoy a 21. Se violaba a 3, hoy a 27.

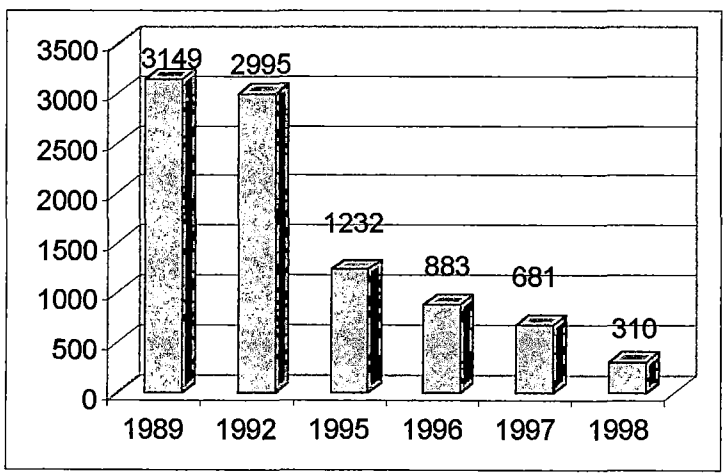
Gráfico 2. 1 Actos Delictivos Diarios 1,998 Vs. 1,993



Fuente : Ministerio Del Interior

Si el terror senderista hizo lo suyo en el pasado reciente, asesinando a más de 13 mil personas, hoy la violencia y el terror tienen otro rostro.

Gráfico 2.2 : Acciones Subversivas Registradas 1989-1998



Fuente: Ministerio Del Interior

El escenario que hasta hace 5 ó 6 años ocupaba el terrorismo hoy en día es ocupado por el fenómeno de la delincuencia común, creando en la ciudad de Lima un ambiente de inseguridad con un origen distinto y un desenlace diferente.

En Febrero de 1998, el INEI, aplicó la 1ra. Encuesta de Victimización en Lima Metropolitana, con el propósito de caracterizar el fenómeno de violencia colectiva y callejera que nos afecta diariamente. Uno de los resultados refleja un récord penoso para nuestra juventud: Haber desplazado al terrorismo en la ejecución de actos vandálicos, pues entre pandillas de jóvenes y las denominadas "barras bravas", llegan a 83% de autoría en la modalidad de violencia pública.

La inseguridad ciudadana es un fenómeno complejo que tiene su origen en la convergencia de determinadas situaciones sociales, económicas, psicológicas y culturales:

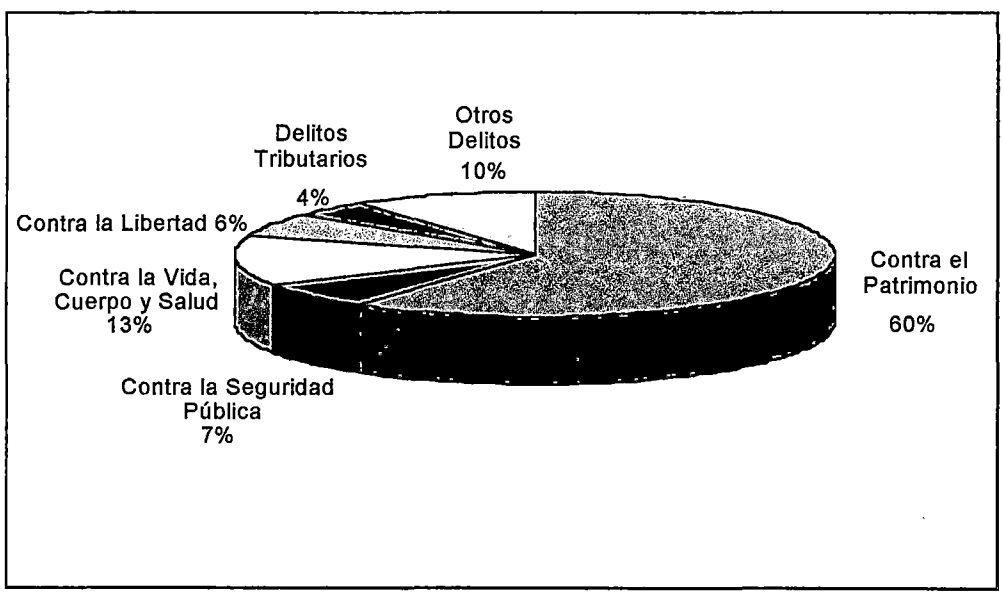
- Desde el punto de vista socioeconómico, la pobreza, la miseria. Pero hay otro problema central en el trasfondo: la galopante desocupación y el clima cada vez más depresivo de la población económicamente activa, cuyos ingresos han decaído a extremos peligrosos.
- En el ámbito policial tenemos una situación donde ciertos oficiales no ayudan a resolver el problema; lamentablemente contribuyen a él.
- En el anquilosado sistema judicial penal, se suman venalidades como el pago a actuarios para que redacten cartas falsas que sirvan para borrar las órdenes de aprehensión que están en el computador de la policía de investigaciones o se ha llegado a pagar por tramitar órdenes falsas de libertad provisional.
- En el aspecto cultural, la inseguridad urbana se origina en una nueva cultura de violencia, herencia directa de los 12 años de terrorismo vividos

por nuestro país. Esta cultura de violencia ha derivado en un incremento en el número de pandillas callejeras, las denominadas "barras bravas", "pirañitas" y delincuentes comunes en todas sus modalidades, pero sobre todo en un surgimiento de la delincuencia organizada como son los secuestradores al paso.

- Según cifras oficiales, la capital cuenta con unas 60 bandas de criminales adultos y alrededor de 100 bandas de pandilleros juveniles, a los que hay que agregar grupos de "pirañitas" y de delincuentes drogadictos dispersos en Lima y Callao. A estos grupos organizados hay que agregar unos 50 mil delincuentes que operan individualmente o en parejas.

En el siguiente cuadro se muestra el porcentaje por tipo de delitos cometidos en Lima. Como podemos observar existe una alto porcentaje de delitos contra el patrimonio o bienes (60%).

Gráfico 2. 3 : Intervenciones en Delitos Registrados por la Policía Nacional, Según el Tipo de Delito: 1998



Fuente : Policía Nacional del Perú

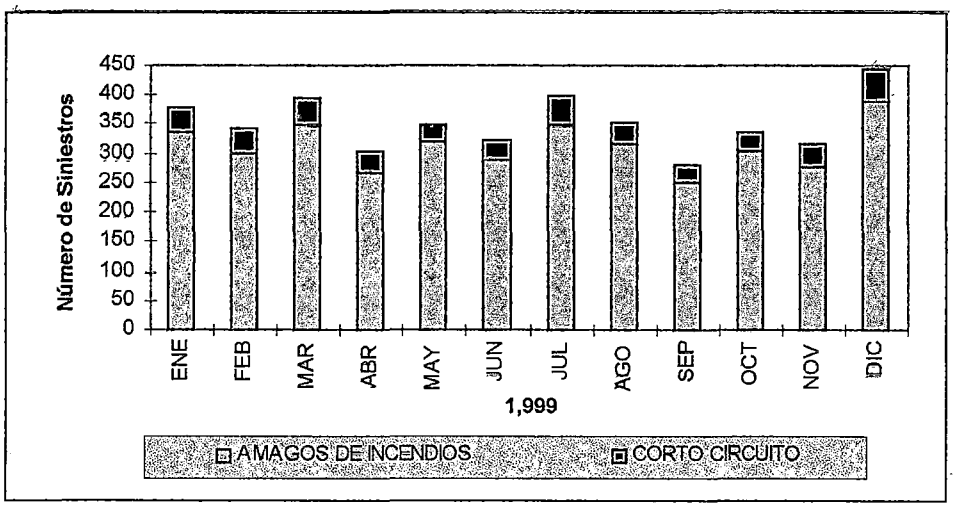
2.1.2 ALTO ÍNDICE DE INCENDIOS EN EL PERÚ

Tabla 2.1 : Cantidad de Incendios por Tipo de Siniestro Durante 1,999

TIPOS	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	TOTAL
Amagos de Incendio	334	300	349	266	320	289	349	315	250	301	277	389	3739
Cortos Circuitos	43	43	46	35	27	34	50	37	30	33	38	53	469
TOTAL	377	343	395	301	347	323	399	352	280	334	315	442	4208

Fuente: Cuerpo General de Bomberos Voluntarios del Perú

Gráfico 2.4 : Cantidad de Incendios por Tipo de Siniestro Durante 1,999



Fuente: Cuerpo General de Bomberos Voluntarios del Perú

2.1.3 INSEGURIDAD EN EL INTERIOR DE LAS EMPRESAS

El mayor porcentaje de robos, sabotajes y/o fraudes que ocurren en las empresas son internos, los cometen los mismos trabajadores o se vinculan directamente con quienes cometen el delito, facilitándoles información, esto debido a posibles venganzas personales y/o deplorables motivos económicos. Los robos, sabotajes y/o fraudes en el interior de las empresas pueden ser cometidos también por personal ajeno a la empresa, lo que actualmente a proliferado en gran número a través de empresas contratistas, de tal manera que no se puede conocer los antecedentes de los trabajadores por la gran cantidad de éstos y la falta de control.

Además existe el peligro de incendio, pues cada vez más empresas cuentan con equipos eléctricos o electrónicos con los que pueden producir incendios (o explosiones) si a éstos se les realiza un mal mantenimiento o si se enfrentan a problemas en la red eléctrica, etc.

2.1.4 ALTOS COSTOS Y BAJA EFICIENCIA DEL SERVICIO DE VIGILANCIA HUMANA

Las empresas peruanas e internacionales no dispuestos a rendirse ante una creciente tasa de crimen y violencia, han contratado de forma apresurada a compañías de seguridad privadas para que les brinden únicamente servicios de vigilancia humana de tal suerte que puedan batallar contra aquellos que amenazan el funcionamiento de los negocios, lo cual genera altos gastos, repercutiendo sobre la utilidad de la organización. Esta forma de seguridad se ha convertido en una manera sencilla y tradicional de brindar seguridad.

Existen un gran número de compañías privadas con alrededor de 120,000 agentes que se especializan en seguridad en el Perú. Los líderes de la industria advierten, sin embargo, que una buena fracción del total no está equipada con los recursos necesarios para hacer un buen trabajo. El crecimiento de esta industria ha permitido que varios contendientes no calificados entren a competir en el mercado, haciendo que el servicio de estas empresas no sea el conveniente y hasta fatídico para los intereses del cliente.

El Servicio de Seguridad Tradicional o Servicio de Vigilancia Humana no es barato. El costo promedio diario de un vigilante de 24 horas para una empresa mediana se encuentra alrededor de los S/.60,00 (US $ 17,24), es decir S/. 1.800,00 mensuales por vigilante (US $ 517,20), lo que anualmente representa un total de S/. 21.600,00 (US $ 6.207).

2.2 FORMULACIÓN DEL PROBLEMA

Debemos hacernos estas preguntas para poder formular el problema correctamente:

¿Afectan los riesgos a la rentabilidad de la empresa?
¿Es confiable contar únicamente con un servicio de vigilancia humana?
¿Es rentable contar únicamente con un servicio de vigilancia humana?
¿Existen otros medios que combinados con servicio de vigilancia humana hagan más eficiente y de menor costo el sistema de seguridad?

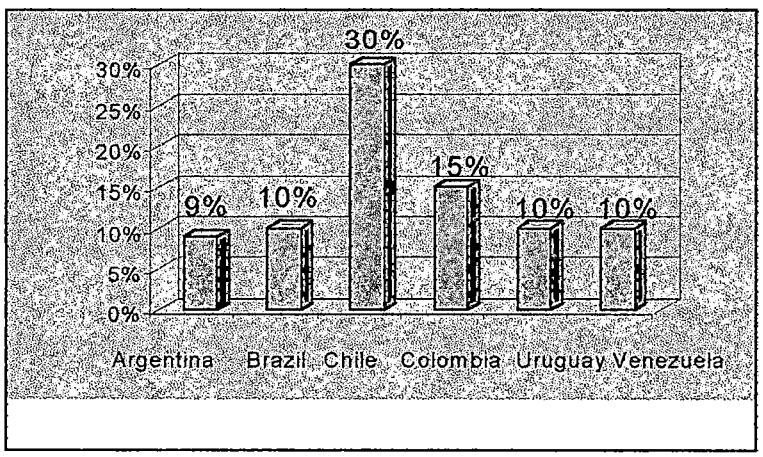
El problema de inseguridad afecta a todo tipo de organización, no lucrativas u organizaciones industriales o comerciales, puesto que de una u otra manera inciden negativamente sobre las actividades normales de la organización, pudiendo incluso ser definitivas en la disolución de ésta, determinando la perdida de muchos puestos de trabajo, bienes y/o información. Así mismo el ser humano tiene ciertas limitaciones para cubrir eficientemente todos los riesgos ya que estos han ido cambiando y existen ciertas distorsiones de los factores humanos que disminuyen la eficiencia.

Debemos tomar en cuenta que usar el Servicio de Vigilancia Humana sólo representa un gasto más no una inversión, es decir no se pueden recuperar estos desembolsos de dinero. Esto afectará definitivamente la estructura de costos del producto o servicio que brinde cualquier empresa, incrementando el precio al usuario o cliente, pudiendo afectar negativamente la rentabilidad del negocio.

Por una falta de conocimiento de las bondades que ofrecen los Sistemas de Seguridad Modernos, en el Perú éstos no se encuentran muy difundidos, pero se aprecia cada día mas el interés por tener edificios inteligentes y la entrada de normas internacionales a ser aceptadas por los

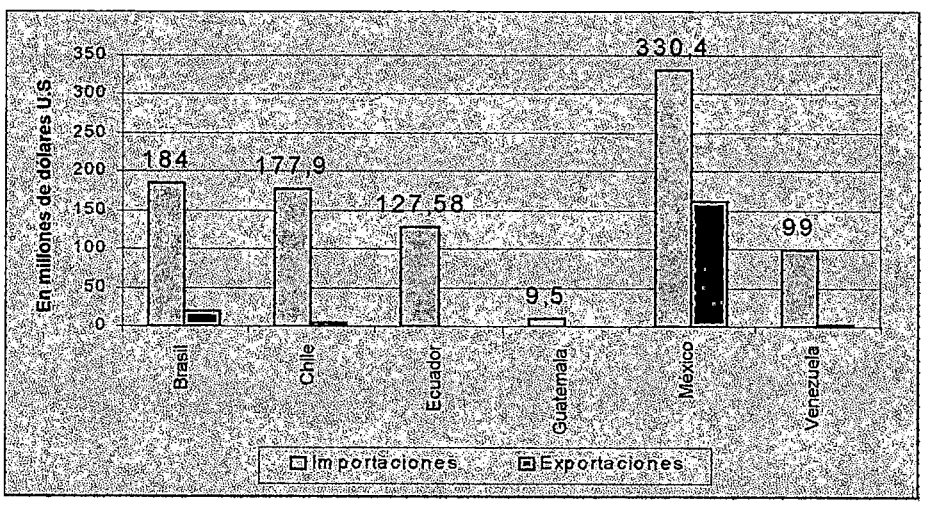
reglamentos nacional, así como el ingreso de mayor cantidad de proveedores de estos sistemas a nuestro mercado nacional. En las siguientes gráficas tratamos de mostrar el panorama económico en cuanto a seguridad en nuestro medio ambiente como país: América Latina.

Gráfico 2.5 : Tasa estimada de crecimiento anual del mercado de la seguridad para países latinoamericanos seleccionados para 1,999



Fuente: STAT Resourses Inc. Revista Ventas de Seguridad Mayo/Junio 1999

Gráfico 2.6 : Importaciones y exportaciones estimadas de equipos de seguridad en 1998 para países latinoamericanos



Fuente: United States Department of Commerce, International Trade Administration
Revista: Ventas de Seguridad Mayo/Junio 1999

2.3 JUSTIFICACIÓN E IMPORTANCIA

2.3.1 JUSTIFICACIÓN

Como podemos observar el perfil delictivo y de siniestrabilidad que se ha mostrado anteriormente es impactante, así como son altos los gastos que genera mantener un sistema de seguridad tradicional, que no es muy confiable.

Tomando en cuenta los cambios vertiginosos que sufre nuestra sociedad en cuanto a problemas de inseguridad, es que se hace necesario afrontar éstos con soluciones de ingeniería; es decir, analizar los riesgos, cualificándolos y cuantificándolos según sea el caso, de tal forma que se aplique una metodología que nos permita medir los efectos negativos de la ocurrencia de cualquier riesgo asociado al tema de inseguridad, con la clara intención de reducir al mínimo cualquier pérdida humana o patrimonial; teniendo en cuenta siempre que toda aplicación tiene un grado de certidumbre menor al 100% y seleccionar las mejores medidas de seguridad factibles: humanas, técnicas y económicas para afrontar los posibles riesgos, minimizando costos y aumentando la calidad de la seguridad existente.

2.3.2 IMPORTANCIA

El alto índice de inseguridad que existe en el Perú así como en la mayoría de los países del mundo, nos obliga a conseguir un sistema de seguridad adecuado que nos permita mejorar la eficacia y confiabilidad del sistema de seguridad tradicional, de tal manera de poder lograr una mejor protección, al menor costo posible y con la calidad necesaria para competir globalmente. De esta situación real y palpable se desprende la importancia de contar con una metodología técnica y profesional que sirva de guía o soporte a las organizaciones que estén conscientes que el problema de

inseguridad se debe atacar con ciencia y no con meras suposiciones o medidas urgentes, sin la más mínima idea de cuánto afecta a la organización el no actuar y cuánto el hacerlo, basado en una decisión técnica.

2.4 DEFINICIÓN DEL PROBLEMA

Se estudió el problema de inseguridad por delincuencia expresada en Robos, Sabotaje y/o Fraudes así como Siniestros (Incendios) en las organizaciones con locales o instalaciones distribuidos geográficamente y se analizó las condiciones en las que actualmente operan contra la posible ocurrencia de los riesgos, de tal manera que nos permitió configurar un sistema de seguridad adecuado tanto técnica como económicamente.

Las decisiones tomadas para configurar el sistema de seguridad propuesto en esta tesis fueron hechas a través del uso de la Gestión de Riesgos; sin embargo las decisiones sobre como diseñar el sistema de seguridad dependerán además de la propia política que asuma cada organización frente a los riesgos que puedan sufrir. El Diseño del Sistema de Seguridad comprenderá: las Medidas de Prevención (manuales, normas, capacitación, señalización, etc.), Medidas de Protección (vigilantes, uso de aparatos de detección, control de accesos, etc.) y/o de Transferencia a los Seguros (pólizas contra incendios, robos, vandalismo, etc.). Además deben tomarse en cuenta todas las reglamentaciones al respecto que parten de las municipalidades, Defensa Civil, Compañía General de Bomberos, etc.

2.5 PLANTEAMIENTO DEL PROBLEMA

La presente tesis presenta una propuesta metodológica que nos permite la implantación de un Sistema de Seguridad que utilice todas las medidas existentes: Físicas, Electrónicas, Humanas y Económicas (Integral) y que además permita reducir los efectos negativos en menor tiempo que la

seguridad tradicional a través de acciones tomadas automáticamente, derivadas de decisiones programadas previamente (Inteligente). A este diseño lo hemos denominado Sistema Integral Inteligente de Seguridad (SIIS). Probaremos la metodología para el caso de la configuración y evaluación de un Sistema de Protección en las Instalaciones Remotas de Uso Telefónico de Empresas de Telecomunicaciones, presentado sus beneficios y ventajas en comparación a la Seguridad Tradicional.

2.6 ALCANCES

El presente trabajo de tesis extiende su aplicación a la protección de la Planta Interna de las Empresas de Telecomunicaciones, específicamente a las Instalaciones Remotas de Uso Telefónico que operan como Centrales Telefónicas. En el Apéndice A se explica y detalla cómo interactuan y operan estas centrales telefónicas.

La metodología aplicada en este trabajo de tesis no sólo es aplicable a Instalaciones Remotas de Uso Telefónico, sino también a otros tipos de organizaciones que tienen locales o sucursales distribuidos geográficamente en diferentes zonas, tales como Bancos, Cadenas de tiendas, Sub-estaciones eléctricas, etc.

La condición de que sean organizaciones con locales geográficamente distantes, estriba en el hecho de la justificación económica de una central que monitoree a varios locales, de tal manera de diluir costos. Esta condición no implica que el número de locales deba ser grande, sino que simplemente condiciona, desde un inicio, la aplicación de la metodología a un determinado tipo de organización.

CAPÍTULO III

OBJETIVOS DEL ESTUDIO Y METODOLOGÍA DE TRABAJO

3.1 OBJETIVOS DEL ESTUDIO

El rol de la seguridad es el de protección de los activos de cualquier tipo de daño, mediante la aplicación cuidadosa de medidas efectivas en costo, las que satisfagan las necesidades del negocio y necesidades de los accionistas, gerentes y empleados, suponiendo que sus necesidades son honestas y legales. Por lo tanto, la seguridad se mide por su habilidad de disminuir o eliminar la exposición de la organización a las riesgos.

3.1.1 OBJETIVOS GENERALES

- Reducir los costos que implica mantener un sistema de protección únicamente a través de los Servicios de Vigilancia Humana en las instalaciones distribuidas geográficamente de determinadas empresas. Anualmente por este rubro las empresas que mantienen este sistema manejan un alto presupuesto de gasto.

- Elevar la calidad del sistema de seguridad existente en las Instalaciones Remotas de Uso Telefónico, a través de medidas de protección más eficientes que tener únicamente como medida de seguridad el Servicio de Vigilancia Humana.

3.1.2 OBJETIVOS ESPECÍFICOS

- Analizar y evaluar el nivel de riesgo en las Instalaciones Remotas de Uso Telefónico.

- Realizar un diagnóstico de las deficiencias actuales de la protección en las Instalaciones Remotas de Uso Telefónico, teniendo únicamente como medida de seguridad, el Servicio de Vigilancia Huamana.

- Diseñar un Sistema de Seguridad que cubra en forma Integral, e Inteligente, los riesgos en las Instalaciones Remotas de Uso Telefónico.

- Demostrar que tecnológicamente es posible implementar un Sistema Integral e Inteligente de Seguridad que disminuya los riesgos que pueda reducir los daños y pérdidas que un incidente o contigencia pueda causar en las Instalaciones Remotas de Uso Telefónico.

- Demostrar que es rentable implementar un Sistema Integral e Inteligente de Seguridad, que pueda atender de forma conjunta o independientemente cada una de los riesgos presentes en las instalaciones remotas estudiadas, específicamente en los siguientes rubros: Seguridad contra riesgos de robos, sabotajes, fraudes y protección contra incendios.

- Evitar o disminuir las consecuencias negativas o perjuicios provenientes de la ocurrencia de eventos dañinos contra los bienes de las Empresas de Telecomunicaciones, en busca de un mejor servicio y una reducción sustancial del lucro cesante.

3.2 METODOLOGÍA DEL TRABAJO

En las Empresas de Telecomunicaciones, el sistema de seguridad, además de garantizar un nivel de protección adecuado frente a los riesgos derivados de la dinámica de su propia actividad (por ejemplo incendios por sobrecargas), es necesario considerar riesgos que sean consecuencia de acciones humanas que pueden catalogarse como comportamientos antisociales, calificables penalmente como faltas o delitos (robo, sabotaje, fraude, etc.). Además, también deben considerarse los inevitables accidentes por falta de cuidado y/o atención en las operaciones humanas.

Para garantizar un nivel idóneo de seguridad en las instalaciones es necesaria la implantación de medidas de seguridad que deben estar diseñadas de acuerdo a una metodología técnica científica que haga frente a los riesgos que afectan o pueden afectar a la empresa, que cubra e la problemática de un estudio previo de seguridad, dando como resultado la cuantificación de los daños potenciales y la manera más económica posible para prevenirlos, enfrentarlos o disminuir sus consecuencias.

A continuación mostramos las etapas a seguir para desarrollar la metodología propuesta en esta tesis, a través de un flujograma.

3.2.1 FLUJOGRAMA DE LA METODOLOGÍA DE TRABAJO

3.2.1.1 REALIZAR LA GESTIÓN DE RIESGOS

Esta primera etapa o procedimiento comprende las siguientes sub etapas o sub procedimientos:

- Identificación del bien
- Identificación de riesgos

- Análisis de riesgos
- Evaluación de riesgos
- Políticas ante los riesgos (Decisiones)

3.2.1.2 DESARROLLAR EL ANÁLISIS TÉCNICO

Diseñar las medidas de seguridad adecuadas a los riesgos, las que deben ser la combinación de medidas de seguridad: Humanas, Físicas, Electrónicas y Económicas, que estén de acorde con el análisis y evaluación de riesgos, así como un análisis técnico del bien a proteger; pero que cumplan con ciertas normativas.

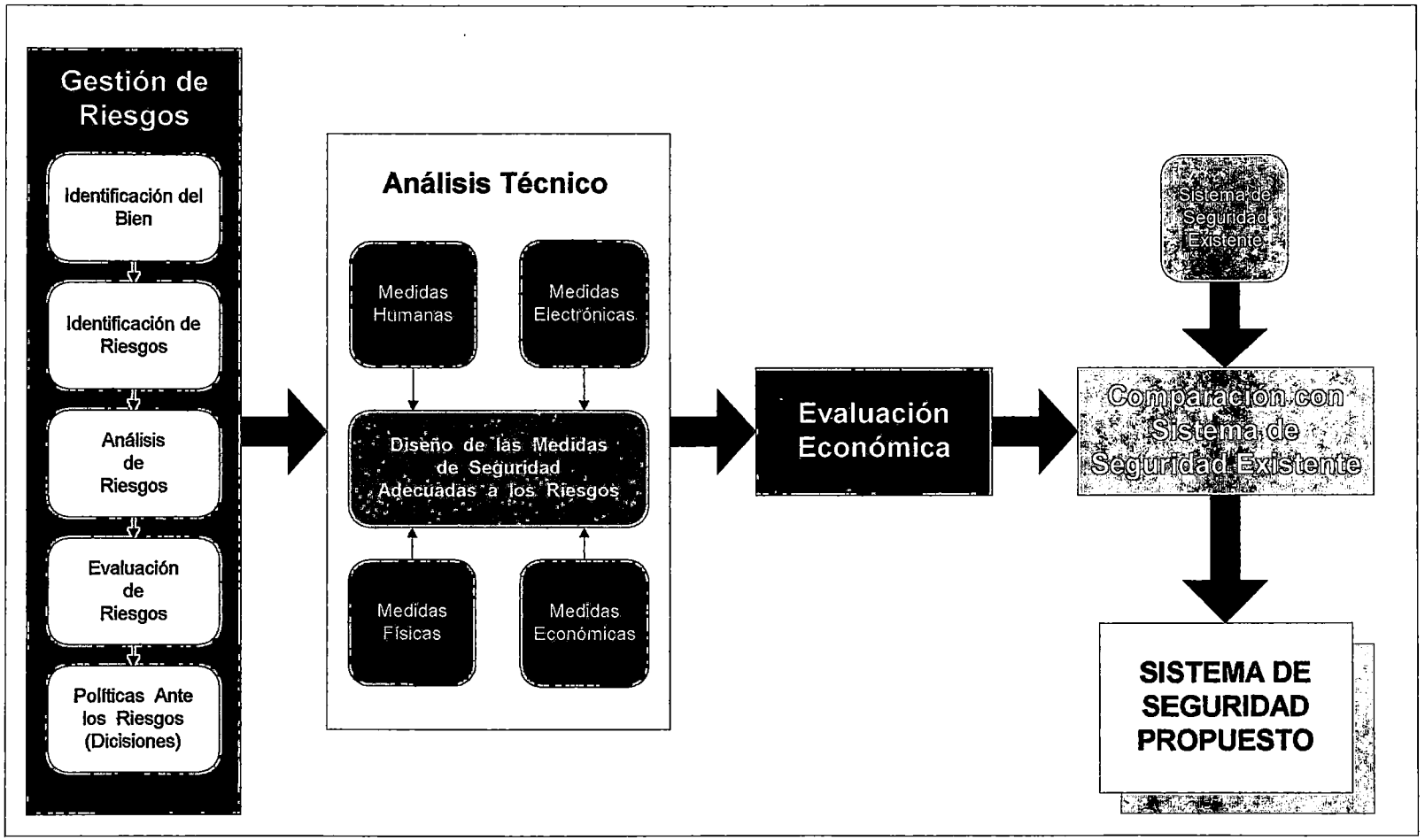
3.2.1.3 REALIZAR LA EVALUACIÓN ECONÓMICA

Desarrollar la evaluación económica de la implantación del sistema de seguridad diseñado.

3.2.1.4 COMPARAR LA SEGURIDAD EXISTENTE Y EL NUEVO SISTEMA PROPUESTO

Realizar esta comparación para evaluar el incremento del nivel de seguridad en las instalaciones y la disminución de costos obtenida.

Gráfica 3.1 : Flujograma de la Metodología de Trabajo



Fuente: Elaboración Propia

CAPÍTULO IV

GESTIÓN DE RIESGOS

4.1 GENERALIDADES

Las empresas sufren pérdidas enormes resultantes de una gran variedad de riesgos que causan problemas, tanto en términos de pérdidas financieras enormes para el gobierno como para el accionista, lo que significa pérdida de empleo que afecta a comunidades enteras. Entender cuales son estos riesgos, la evaluación de los efectos dañinos y la prevención de su ocurrencia, o por lo menos suavizar su impacto, es de lo que trata la "Gestión de Riesgos".

Los riesgos, los que son de preocupación diaria para todo tipo de negocios, pueden cuantificarse, jerarquizarse en términos de importancia, y hasta tratarse como costos efectivos para la ventaja financiera de una organización.

Hasta tiempos relativamente recientes, no se realizaba ninguna Gestión de Riesgos, y en todo caso su estudio carecía del rigor de estar apoyado en un principio y en un método técnico y científico; las decisiones y políticas frente a los riesgos, si es que existían, distaban bastante de ser óptimas e incluso racionales.

4.2 MÉTODO PARA LA GESTIÓN DE RIESGOS

El método que se empleó tuvo por objeto la identificación, análisis y evaluación de los factores que puedan influir en la manifestación de un riesgo, con la finalidad de que la información obtenida nos permita calcular la severidad y probabilidad del riesgo y de esta manera tomar la decisión del sistema de seguridad a diseñar. Este método es de tipo secuencial y cada fase del mismo, se apoyará en los datos obtenidos en las fases que la preceden, el desarrollo del mismo es:

- Identificación del bien
- Identificación de riesgos
- Análisis de riesgos
- Evaluación de riesgos
- Políticas ante los riesgos

4.3 IDENTIFICACIÓN DEL BIEN

Esta fase consiste en desarrollar la descripción de cada componente de la Instalación Remota de Uso Telefónico (IRUT) a la que se le brindará protección, empezando por explicar brevemente la actividad a la que esta destinada el bien objeto del estudio para una mejor comprensión.

4.3.1 ACTIVIDAD

El bien en estudio está dedicado a la operación de las telecomunicaciones. Desarrolla sus actividades en el interior y el exterior de sus instalaciones, pero la tesis esta dirigida a las actividades internas. La descripción detallada del proceso de producción o actividad se explica en el apéndice A (Red Telefónica).

4.3.2 DISTRIBUCIÓN DE LA INSTALACIÓN

Las Instalaciones Remotas de Uso Telefónico se distribuyen de la siguiente manera: El fondo del terreno es ocupado por la salas con equipos de telefonía, a un lado de la zona delantera se encuentran las edificaciones complementarias (energía, servicios higiénicos) y la zona media del terreno se reserva para un patio y una torre.

A continuación indicamos los componentes de cada uno de los ambientes de la IRUT que se tuvieron en cuenta para el estudio son:

4.3.2.1 Ambiente A

Constituido por:

- Distribuidor principal
- Baterías
- Rectificador
- La acometida de cables desde la Cámara Principal mediante ductos.

4.3.2.2 Ambiente B

Constituido por:

- Conmutador
- Transmisor
- El sistema de aire acondicionado

4.3.2.3 Sala de Grupo Electrógeno

Constituido por:

- El grupo electrógeno

4.3.2.4 Sala de Subestación Eléctrica

Constituido por:

- Transformador

4.3.2.5 Patio

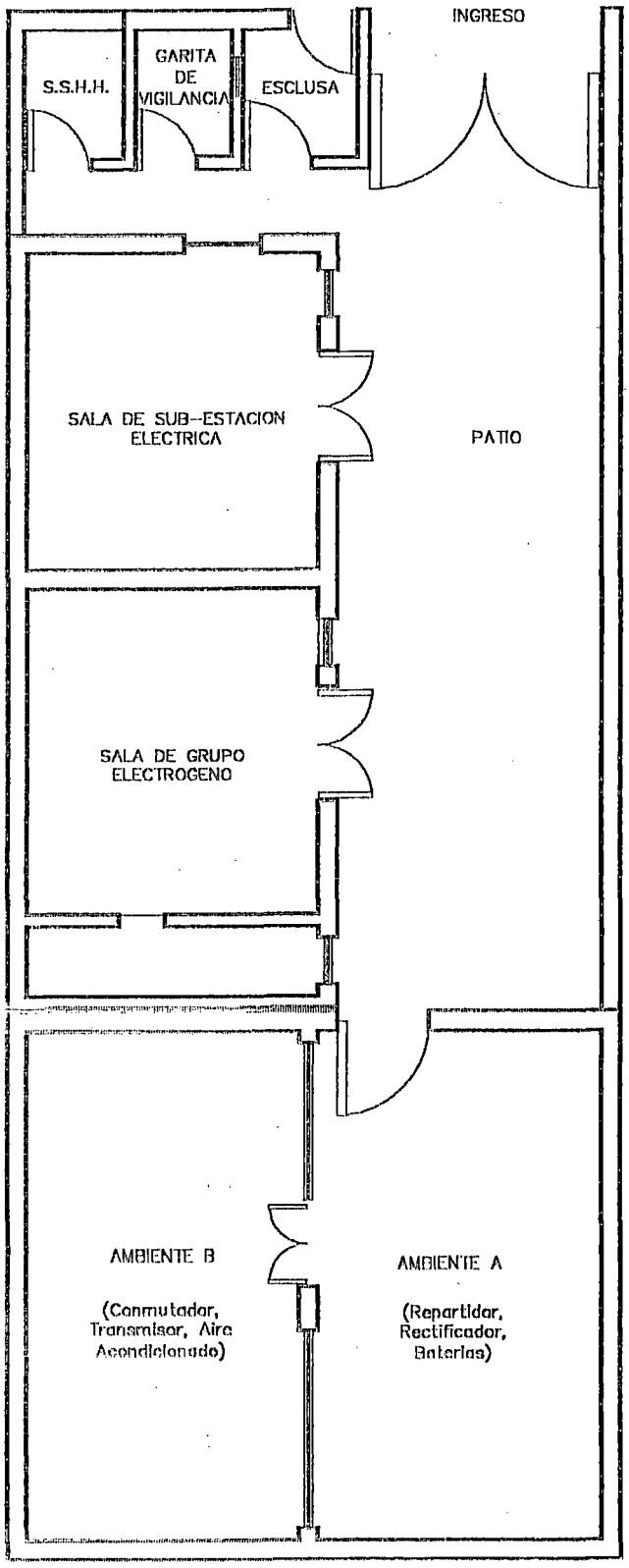
Constituido por:

- Patio de maniobras
- Tanque de combustible
- Antena de transmisión

Básicamente, estos ambientes unidos conforman la infraestructura de una Instalación Remota de Uso Telefónico típica.

Con el objeto de explicar de una manera precisa la distribución física de los ambientes en una Instalación Remota de Uso Telefónico, en la siguiente página mostramos un esquema de esta distribución:

GRÁFICO 4.1 DISTRIBUCIÓN FÍSICA DEL BIEN



4.4 IDENTIFICACIÓN DE RIESGOS

Para identificar los riesgos en la Instalación Remota de Uso Telefónico, primero se identificaron las amenazas en cada ambiente, que podrían tener impacto en nuestras operaciones, para reconocer los riesgos en cada ambiente. Para esto utilizamos el método de Causa - Efecto o Amenaza - Riesgo, que se muestra a través de tablas para cada ambiente.

En consecuencia, es necesario ser capaz de identificar dichos riesgos que se tendrán que ser enfrentados, para manejar adecuadamente los riesgos probables de crear pérdida y/o disminuciones de ganancias.

4.4.1 AMBIENTE A

Tabla 4.1 : Tabla de Riesgo - Amenaza para el Ambiente A

Riesgo	Amenaza
Incendio	• Baterías: desprendimiento de gases explosivos • Distribuidor Principal: corto circuito o sobrecarga eléctrica. • Rectificador: corto circuito o sobrecarga eléctrica.
Sabotaje	• Rectificador: desconectado, dañado, manipulado, variar parámetros de operación. • Distribuidor Principal: corte de los cables telefónicos o daño temporal de los mismos.
Fraude	• Distribuidor Principal: llamadas fraudulentas afectando a los abonados, dar de alta el servicio a un abonado suspendido.

Fuente : Elaboración Propia

4.4.2 AMBIENTE B

Tabla 4.2 : Tabla de Riesgo - Amenaza para el Ambiente B

Riesgo	Amenaza
Incendio	• Conmutador, transmisor y aire acondicionado: corto circuito o sobre carga eléctrica. • Conmutador y transmisor: gases corrosivos debido a la combustión de cables. • Aire acondicionado: corto circuito o sobre carga eléctrica.
Sabotaje	• Conmutador y transmisor: desconectados, dañados, variar sus parámetros de operación.

Fuente : Elaboración Propia

4.4.3 SALA DE GRUPO ELECTRÓGENO

Tabla 4.3 : Tabla de Riesgo - Amenaza para la Sala de Grupo Electrógeno

Riesgo	Amenaza
Incendio	• Grupo electrógeno: corto circuito o sobrecarga eléctrica. • Grupo electrógeno: calentamiento por encima del punto de ignición del combustible. • Grupo electrógeno: fricción en las partes del generador. • Tablero general: corto circuito o un sobrecarga eléctrica.
Robo	• Grupo electrógeno: robo de las piezas comerciales (por ejemplo : generador).
Sabotaje	• Tablero general: desconectarlo.

Fuente : Elaboración Propia

4.4.4 SALA DE SUB ESTACIÓN ELÉCTRICA

Tabla 4.4 : Tabla de Riesgo - Amenaza
para la Sala de Sub Estación Eléctrica

Riesgo	Amenaza
Incendio	• Transformador : corto circuito, explosión, calentamiento y autocombustión del aceite refrigerante.
Sabotaje	• Transformador: Desconexión de cables, daño, manipulación maliciosa.

Fuente : Elaboración Propia

4.4.5 PATIO

Tabla 4.5: Tabla de Riesgo - Amenaza
para el Patio

Riesgo	Amenaza
Incendio	• Tanque de combustible: aumento de temperatura sobre el punto de ignición del combustible almacenado por trabajos negligentes con fuego.
Robo	• Tanque de combustible: robo de Diesel.

Fuente : Elaboración Propia

En las tablas anteriores hemos señalado las amenazas para cada riesgo en cada ambiente de la IRUT, las explicaciones de porque dichas amenazas pueden producir dichos riesgos, se encuentran contenidas en el Apéndice B (Riesgo - Amenazas en Edificios de Uso Telefónico).

Como se observa, empleando el método causa - efecto obtuvimos la información de las condiciones en que se pueden producir los riesgos, es

decir las amenazas. Esta información la hemos resumido en el siguiente cuadro para poder contar con una visión panorámica de la identificación de los riesgos que nos permita continuar con el siguiente paso; Análisis de Riesgos.

Tabla 4.6: Matriz Resumen Ambiente - Bien - Riesgo en las Instalaciones Remotas de Uso Telefónico

		Riesgo			
Ambiente	**Bien**	**Incendio**	**Robo**	**Sabotaje**	**Fraude**
Ambiente A	Baterías	■			
	Distribuidor Principal	■		■	■
	Rectificador	■		■	
Ambiente B	Conmutador	■		■	
	Transmisor	■		■	
	Aire Acondicionado	■			
Sala Grupo Electrógeno	Grupo Electrógeno	■	■		
	Tablero General	■		■	
Sub Estación E.	Transformador	■		■	
Patio	Tanque de Combustible	■	■		

Fuente : Elaboración Propia

4.5 ANÁLISIS DE RIESGOS

El análisis de riesgo se realizó luego de contrastar de forma sistemática los riesgos sobre cada uno de los ambientes de la Instalación Remota de Uso Telefónico.

El análisis nos permitió evaluar el riesgo en cada ambiente de la instalación, clasificándola en cuanto a su nivel de peligrosidad.

4.5.1 CONSIDERACIONES PARA EL ANÁLISIS DE RIESGOS

Las amenazas de algún modo son concretas y siempre están ahí, sin embargo, el que vayan a afectar o no nuestras operaciones dependerán de las características del bien, de nuestra ubicación, de nuestros procesos, de la actitud de nuestra fuerza de trabajo hacia la empresa, y muchos otros factores.

Para el análisis de riesgos se analizó la mayor cantidad de información confiable (análisis de antecedentes, información registrada y catálogo de riesgos) y se complementó con una inspección ordenada, minuciosa y sistemática a dichas instalaciones y se tuvo las siguientes consideraciones que inciden en el análisis de riesgos, durante el estudio:

4.5.1.1 UBICACIÓN

Concepto	Información
Zona	Área Urbana
Enlaces de comunicación	Telefónica
Desarrollo Urbano	Continuo

4.5.1.2 PROCESO DE PRODUCCIÓN

Concepto	Información
Aporte calor	No
Energía	Permanente
Tipo	Automático

4.5.1.3 ALTURAS

Concepto	Información
Plantas	Primera

4.5.1.4 ACCESOS

Concepto	Información
Al Patio	Puerta a la calle
Ambiente A	Puerta al patio
Ambiente B	Puerta al ambiente A
Sala Grupo Electrógeno	Puerta al patio
Sub Estación Eléctrica	Puerta al patio

4.5.1.5 ABERTURAS EXTERIORES

Concepto	Información
Al Patio	Sin Techo
Ambiente A	Techado
Ambiente B	Techado
Sala Grupo Electrógeno	Techado
Sub Estación Eléctrica	Techado

4.5.1.6 CONSTRUCCIÓN DEL EDIFICIO

Concepto	Información
Estructura	Hierro
Cerramiento	Hormigón
Cubierta	Concreto

4.5.1.7 MEDIDAS DE SEGURIDAD

Concepto	Información
Incendio	
Extintores Manuales	Si
Detección Automática	No
Extinción Automática	No
Columnas Hidrantes	No
Mangueras Contra Incendio	No
Conexión al Central Control	No
Robo o Sabotaje	
Vigilancia Humana	Si
Sistema de alarma de robo	No
Conexión a la Central de Control	No
Vigilancia Móvil	No

4.5.1.8. NÚMERO DE PERSONAS EMPLEADAS

Concepto	Información
Personal Propio	Si
Contratistas	Si
Modalidad	Temporal
Permanencia	Mínima

4.5.1.9. VALOR DEL BIEN

Concepto	Información
Valor del Activo	500.000 Dólares
Ingresos Anuales	1.200.000 Dólares

(*) Ver Anexo 01 (Valores de Activos e Ingresos)

4.5.1.10 STATUS ECONÓMICO

Concepto	Información
Índice Desempleo	Altos
Establecimiento Comerciales	Mínimos

4.5.1.11 CONDICIONES SOCIALES Y PANORAMA PSICOLÓGICO

Concepto	Información
Nivel de delincuencia	Alta
Condiciones Sociales	No favorable
Panorama psicológico de la fuerza laboral	No favorable

4.5.1.12 CONDICIONES LABORALES

Concepto	Información
Relación Empleador-Empleado	Mala
Negociaciones Colectivas	Reclamos sucesivos
Violencia en problemas laborales en el pasado	No

4.5.1.13 UBICACIÓN DE LA POLICÍA Y DE LOS BOMBEROS

Concepto	Información
Distancia	Mediana (10 Km.)
Accesibilidad	Difícil
Brigadas	No existe
Tiempo de reacción	De 30min. a 1 hora

4.5.1.14 PLAN DE FLUJO OPERACIONAL

Concepto	Información
Densidad	Cero personas
Turnos	Durante las 24 horas
Control de Contratas	Escaso

4.5.2 MÉTODO PARA EL ANÁLISIS DEL RIESGO

El método que se utilizó para el análisis de riesgos es un método cuantitativo o de esquema de puntos, para lo cual se emplearon los siguientes criterios:

4.5.2.1 CRITERIO DE FUNCIÓN (F)

¿Los daños alteran la actividad?

Es el criterio que indica el nivel de alteración del proceso normal, pudiendo afectarlo totalmente o parcialmente. En la siguiente tabla se representan los diferentes niveles del criterio y sus valores:

Tabla 4.7: Niveles y Cuantificación del Criterio de Función

Nivel	Valor
Gravemente	3
Medianamente	2
Levemente	1

Fuente : Elaboración Propia

4.5.2.2 CRITERIO DE SUSTITUCIÓN (S)

¿Los bienes pueden ser sustituidos?

Es el criterio que indica el nivel de dificultad para sustituir los bienes siniestrados, este nivel de dificultad se expresa a través del costo y tiempo de sustitución, tales como : Lugar donde se encuentra el bien a sustituir, la dimensión de la obra para la sustitución, la calificación del personal que realizará los trabajos de sustitución, plazo que llevarán los trabajos de sustitución y porcentaje de paralización del proceso para la sustitución. A continuación se muestran los niveles del criterio y sus valores:

Tabla 4.8: Niveles y Cuantificación del Criterio de Sustitución

Nivel	Valor
Difícilmente	3
Sin mucha dificultad	2
Fácilmente	1

Fuente : Elaboración Propia

4.5.2.3 CRITERIO DE PROFUNDIDAD (P)

¿Nivel de efectos psicológicos, perturbación, efectos sobre la imagen?

Es el criterio que indica el nivel de perturbación o efectos psicológicos

negativos en los clientes debido a la ocurrencia del riesgo. A continuación se muestran los niveles y sus valores:

Tabla 4.9 : Niveles y Cuantificación del Criterio de Profundidad

Nivel	Valor
Grave perturbación	3
Perturbación limitada	2
Perturbación leve	1

Fuente : Elaboración Propia

4.5.2.4 CRITERIO DE EXTENSIÓN (E)

¿Cuál es el alcance de los daños según su amplitud?

Es el criterio que indica la dimensión alcanzada por los efectos resultantes de la manifestación del riesgo. En la siguiente tabla se representa los diferentes niveles del criterio, así como su cuantificación:

Tabla 4.10: Niveles y Cuantificación del Criterio de Extensión

Nivel	Valor
Nacional	3
Regional	2
Local	1

Fuente : Elaboración Propia

4.5.2.5 CRITERIO DE AGRESIÓN (A)

¿La probabilidad de que el riesgo se manifiesta es?

Es el criterio que indica la probabilidad de ocurrencia de un riesgo. Se puede establecer utilizando datos históricos de la empresa, de asociaciones,

de empresas de seguros, de la policía o de otras fuentes.

Mientras que la probabilidad dependerá significativamente de la naturaleza del riesgo en relación a la situación actual de la empresa, otros factores, tales como las tendencias criminales, deben tomarse en cuenta. La siguiente tabla representa los diferentes niveles del criterio; así como su cuantificación:

Tabla 4.11 : Niveles y Cuantificación del Criterio de Agresión

Nivel	Valor
Alta	3
Mediana	2
Baja	1

Fuente : Elaboración Propia

4.5.2.6 CRITERIO DE VULNERABILIDAD (V)

¿La probabilidad de que se produzcan daño es?

La vulnerabilidad al riesgo, se establece por el examen físico del lugar y la evaluación de los sistemas de protección actuales.

El criterio de Vulnerabilidad indica la probabilidad de que se produzca daño luego de manifestado el riesgo.

La siguiente tabla representa los diferentes niveles del criterio; así como su cuantificación:

Tabla 4.12 : Niveles y Cuantificación del Criterio de Vulnerabilidad

Nivel	Valor
Alta	3
Mediana	2
Baja	1

Fuente : Elaboración Propia

4.6 EVALUACIÓN DEL RIESGO

En esta sección indicamos los factores del riesgo para la evaluación del riesgo:

- **Severidad del Riesgo,** es el factor que está en función de la importancia del suceso y los daños ocasionados a las instalaciones, afectado por la vulnerabilidad de la instalación.

- **Probabilidad de que el riesgo se manifieste,** es el factor que está en función de la frecuencia de manifestación del riesgo. Es decir está dado por el criterio de Agresión.

El procedimiento para cuantificar los factores del riesgo considerados es el siguiente:

4.6.1 SEVERIDAD DEL RIESGO (Se)

- **Importancia del suceso (I),** Lo definimos como la multiplicación del Criterio de Función con el Criterio de Sustitución

$$I = F \times S$$

- **Daños ocasionados (D),** lo definimos como la multiplicación del Criterio

de Profundidad con el Criterio de Extensión.

$$D = P \times E$$

Carácter del Riesgo (C), Por tanto podemos definir un termino auxiliar que estaría definido por la adición de los factores Importancia del Suceso con los Daños ocasionados.

$$C = I + D$$

Este termino se entiende como la medida que indica el nivel de perdida a sufrir por la ocurrencia de un riesgo. (es susceptible de ser valorizado en unidades monetarias).

Por lo tanto la Severidad del Riesgos estaría definido por el Carácter del Riesgo afectado por la Vulnerabilidad de la instalación quedaría:

$$Se = C \times V$$

$$Se = (F \times S + P \times E) \times V$$

La Severidad del riesgo es la expresión que indica la magnitud total del daño (C) que se produciría en el caso de la manifestación de un riesgo, pues es el perjuicio económico multiplicado por la probabilidad de daño (V), con lo cual se consigue una medida expresada en unidades monetarias. Recuérdese que la Vulnerabilidad es una medida probabilística (adimensional).

- **Clasificación de la severidad del riesgo,** haciendo un análisis de los valores máximos y mínimos que pueden tomar los factores del cálculo de

la Severidad del Riesgo, llegamos a la conclusión que el valor de ésta se encuentra entre 2 y 54. Por lo tanto, dividiendo este intervalo en tres partes semejantes, de tal manera que podamos clasificar el grado de severidad del riesgo, obtuvimos la siguiente tabla:

Tabla 4.13: Tipo de Severidad del Riesgo

Valor mínimo	Valor máximo	Nivel
38	54	Grande
20	37	Normal
2	19	Pequeña

Fuente : Elaboración Propia

4.6.2 PROBABILIDAD DEL RIESGO (Pr)

Como se menciono anteriormente esta probabilidad está dada por el nivel del Criterio de Agresión.

$$\mathbf{Pr = A}$$

4.6.3 CÁLCULO DE LA EVALUACIÓN DEL RIESGO

Con los valores para cada factor y usando las tablas y fórmulas antes descritas, procedemos a realizar los cálculos de la evaluación de riesgos para cada ambiente de la Instalación Remota de Uso Telefónico evaluada de tal manera de poder construir la matriz para la evaluación de riesgos. Para conseguir este propósito nos ayudamos de las tablas mostradas en las siguientes páginas, en las que mostramos cómo logramos los resultados finales de la evaluación.

Se han diseñado estas tablas siguiendo el orden lógico operacional de izquierda a derecha, de tal manera que en cada tabla ha sido confeccionada para cada ambiente de la Instalación Remota de Uso Telefónico estudiada.

La primera columna llamada "Tipo Riesgo" indica sólo los riesgos a los que está sujeto el ambiente en estudio.

La segunda columna denominada "Análisis" esta dividida a su vez en dos columnas: la primera, "Criterio" indica el criterio que se está analizando y la segunda, "Valor", indica el valor que se ha otorgado a el criterio para el riesgo en el ambiente que se está analizando. El significado de los valores otorgados está contenido en las tablas de cada criterio, explicadas anteriormente.

La tercera columna, "Evaluación", contiene las columnas ID, C, V, Se, A, y Pr, estas columnas significan :

ID : Indica el valor de la importancia (I) y de los daños ocasionados (D)
C : Carácter del riesgo
Se : Severidad del riesgo
V : Criterio de Vulnerabilidad
A : Criterio de Agresión

Las Justificaciones de los valores dados a los criterios en el análisis, se encuentran en el anexo 02 (Análisis de Riesgos en Edificios de Uso Telefónico).

Tabla 4.14: Tabla de Análisis y Evaluación de Riesgos - Ambiente A

TIPO RIESGO	ANÁLISIS		EVALUACIÓN							
	CRITERIO	VALOR	I	D	C	V	Se		A	Pr
Incendio	F	3	I	9	15	3	45	Grande	2	Mediana
	S	3								
	P	3	D	6						
	E	2								
Sabotaje	F	3	I	9	15	3	45	Grande	2	Mediana
	S	3								
	P	3	D	6						
	E	2								
Fraude	F	1	I	1	3	2	6	Pequeña	1	Baja
	S	1								
	P	2	D	2						
	E	1								

Fuente : Elaboración Propia

Tabla 4.15 : Tabla de Análisis y Evaluación de Riesgos - Ambiente B

TIPO RIESGO	ANÁLISIS		EVALUACIÓN							
	CRITERIO	VALOR	I D		C	V	Se		A	Pr
Incendio	F	3	I	9	15	3	45	GRANDE	2	MEDIANA
	S	3								
	P	3	D	6						
	E	2								
Sabotaje	F	3	I	9	15	3	45	GRANDE	2	MEDIANA
	S	3								
	P	3	D	6						
	E	2								

Fuente : Elaboración Propia

Tabla 4.16 : Tabla de Análisis y Evaluación de Riesgos - Sala de Grupo Electrógeno

TIPO RIESGO	ANÁLISIS		EVALUACIÓN							
	CRITERIO	VALOR	I	D	C	V	Se		A	Pr
Incendio	F	2	I	4	8	3	24	NORMAL	3	ALTA
	S	2								
	P	2	D	4						
	E	2								
Robo	F	2	I	2	6	2	12	PEQUEÑA	2	MEDIANA
	S	1								
	P	2	D	4						
	E	2								
Sabotaje	F	2	I	2	6	2	12	PEQUEÑA	2	MEDIANA
	S	1								
	P	2	D	4						
	E	2								

Fuente : Elaboración Propia

Tabla 4.17: Tabla de Análisis y Evaluación de Riesgos - Sala de Sub Estación Eléctrica

TIPO RIESGO	ANÁLISIS		EVALUACIÓN							
	CRITERIO	VALOR	I	D	C	V	Se		A	Pr
Incendio	F	3	I	9	13	2	26	NORMAL	3	ALTA
	S	3								
	P	2	D	4						
	E	2								
Sabotaje	F	3	I	6	10	2	20	NORMAL	1	BAJA
	S	2								
	P	2	D	4						
	E	2								

Fuente : Elaboración Propia

Tabla 4.18: Tabla de Análisis y Evaluación de Riesgos - Patio

TIPO RIESGO	ANÁLISIS		EVALUACIÓN							
	CRITERIO	VALOR	ID		C	V	Se		A	Pr
Incendio	F	1	I	1	2	2	4	PEQUEÑA	1	BAJA
	S	1								
	P	1	D	1						
	E	1								
Robo	F	1	I	1	2	2	4	PEQUEÑA	2	MEDIANA
	S	1								
	P	1	D	1						
	E	1								

Fuente : Elaboración Propia

Tabla 4.19 Matriz Severidad y Probabilidad del Riesgo en la IRUT

AMBIENTES	RIESGO	Se	Pr
Ambiente A	Incendio	Grande	Mediana
	Sabotaje	Grande	Mediana
	Fraude	Pequeño	Baja
Ambiente B	Incendio	Grande	Mediana
	Sabotaje	Grande	Mediana
Sala Grupo Electrógeno	Incendio	Normal	Alta
	Robo	Pequeño	Mediana
	Sabotaje	Pequeño	Mediana
Sala Sub Estación Eléctrica	Incendio	Normal	Alta
	Sabotaje	Normal	Baja
Patio	Incendio	Pequeño	Baja
	Robo	Pequeño	Mediana

Fuente : Elaboración Propia

4.7 POLÍTICAS ANTE LOS RIESGOS

En esta sección trataremos sobre la decisión que se tomó en función de la clase de los factores de riesgo hallados, de tal manera que determinamos las medidas de seguridad para la protección de la instalación remota de uso telefónico, para hacer frente a la materialización de los riesgos, con los mínimos daños o pérdidas.

Las recomendaciones o "tratamientos" del riesgo se realizan en base al tipo de seguridad que el bien a proteger requiera. Estas recomendaciones o tratamientos corresponden a una o a la combinación de las cinco categorías siguientes :

4.7.1 EVASIÓN

Siempre y cuando se trate de productos y/o servicios nuevos NO realizar actividades arriesgadas ya que crean riesgos superiores al beneficio esperado. Es decir no insistir en el proyecto.

Cuando se trate de un negocio ya establecido, el significado de Evasión se entiende como la total eliminación del riesgo através de evitar las operaciones que estén sujetas a este riesgo, por ejemplo, cuando se trate de un negocio de compra al detalle, en lugar de recibir dinero efectivo se podrían recibir únicamente tarjetas de crédito o débito. Sin embargo, esta decisión de Evasión, si se toma como única medida, generalmente va en contra de las operaciones naturales del negocio. En el ejemplo anterior, se nota que si sólo se aceptan tarjetas en lugar de efectivo el negocio se limita a un mercado pequeño, no por segmentación estratégica sino por otra razón distinta a la estrategia del negocio. Por esta razón casi es imposible tomar esta decisión sola, es más común tomar la combinación de esta decisión con otras.

4.7.2 DISMINUCIÓN

Se refiere a la disminución del riesgo, no necesariamente a su eliminación, mediante la implementación de medidas de protección humanas, físicas y/o electrónicas o también mediante el uso de procedimientos que podrían modificar aquellos propios del negocio, por supuesto, en una medida

razonable que no altere en gran medida el desarrollo normal de las operaciones. Esta decisión podría ir acompañada por otras como la de Evasión en un intento de mix de decisiones. Esta es la alternativa más común que usan la mayoría de la empresas, no sólo en el Perú sino en el mundo, por estar más cerca al razonamiento intuitivo del significado de seguridad.

4.7.3 ACEPTACIÓN

Mediante esta decisión la Empresa se hace responsable de la pérdida. No será necesaria una acción inmediata, pero habrá que vigilar los cambios que puedan aumentar el riesgo. Se debe tener presente que existen muchos momentos en los que indiscutiblemente se deben aceptar los efectos nocivos de la ocurrencia de un riesgo, por ello en esta decisión debe prevalecer el sentido de costo de oportunidad en mayor medida que en otras decisiones, pues la organización o empresa ha aceptado la pérdida. Es decir se debe contrapesar el costo de invertir en seguridad (aparatos, procedimientos, personas, etc.) contra el costo de lo que se quiere proteger (capital de trabajo y humano) y la frecuencia con la que se puede presentar la manifestación del riesgo.

4.7.4 TRANSFERENCIA

Mediante esta decisión la Empresa puede optar por la transferencia de parte del daño a una empresa de seguros; suscribiendo pólizas de seguros que cubran las posibles pérdidas. Esta decisión depende del valor del activo y/o lucro cesante que se estime que podría manifestarse, pues están en consideración los montos de las primas (costos) así como la probabilidad de que el riesgo suceda y el monto de la indemnización (beneficio).

4.7.5 DISEMINACIÓN

Por esta técnica se trata de minimizar el potencial de pérdida tanto como sea posible. Por ejemplo, no permitiendo que una cantidad de dinero se acumule en la caja registradora de una tienda de venta al detalle, sino que luego de que se ha obtenido una cierta cantidad, tal vez la denominada "caja chica", el administrador de la tienda guarde el exceso de dinero diseminándolo (entiéndase repartiéndolo) en distantes partes de la tienda, de tal manera que si sufre un robo, la pérdida sea menor.

Sin embargo el concepto de diseminación también tiene otra connotación, la cual significa que se puede diseminar el riesgo de un proceso encargando a terceros una parte o más partes del proceso, de tal manera de repartir el riesgo. Un ejemplo sería la subcontratación de la producción de componentes vitales en un proceso de manufactura en varias empresas, protegiéndose de la falla de una de ellas.

4.7.6 MATRIZ DE DECISIONES

La Matriz de Decisiones nos sirvió de guía para adoptar las políticas de seguridad asumidas para las instalaciones en estudio según los factores del riesgo, para lo cual puede tomarse una de las medidas de seguridad o la combinación de ellas.

El uso de la Matriz de Decisiones es una simple herramienta para la priorización del potencial de perdidas, es decir sirve como una ayuda para la toma de decisiones acerca de las políticas frente al riesgo. En la tabla de Matriz de Decisiones que mostramos a continuación usamos los resultados de la Matriz de la Evaluación de Riesgos de la IRUT, de la tabla 4.19.

La cuantificación o priorización del potencial de perdidas debe tomar en cuenta el hecho que hay conceptos intuitivos de control de seguridad, tales como la instalación de una simple alarma para un pequeño almacén, y conceptos de control de seguridad basados en detallados análisis costo / beneficio.

Tabla 4.20: Matriz de Decisiones

SEVERIDAD DEL RIESGO	PROBABILIDAD QUE EL RIESGO SE MANIFIESTE		
	Alta	Mediana	Baja
Grande	Evasión ó Disminución (Nivel de Seguridad Máxima)	Disminución (Nivel de Seguridad Alta) ó Evasión	Transferencia y / ó Disminución (Nivel de Seguridad Baja)
Normal	Evasión ó Disminución (Nivel de Seguridad Alta)	Disminución (Nivel de Seguridad Media) ó Transferencia	Diseminación ó Transferencia y / ó Disminución (Nivel de Seguridad Mínima)
Pequeña	Disminución (Nivel de Seguridad Baja)	Disminución (Nivel de Seguridad Mínima) ó Aceptación	Aceptación

Fuente : Adaptación Propia de "Decision Matrix : A Risk Handling Decision Aid", Risk Analysis And The Security Survey by James F. Broder, CPP. Editorial : Butterworth-Heinemann, 1984

Como podemos observar el nivel de seguridad que la matriz recomienda disminuye en sentido vertical desde arriba hacia abajo y en sentido horizontal desde la izquierda hacia la derecha. La explicación radica en lo siguientes puntos :

- En sentido vertical, la severidad disminuye de arriba a abajo y teniendo en cuenta que este valor representa el producto del valor del bien a ser protegido por el grado de vulnerabilidad existente y que las medidas de seguridad que se tomen sólo tendrán efecto sobre la vulnerabilidad del sistema, se deduce que se debe instaurar o trasladar a niveles de seguridad más altos mientras más grave sea la severidad del riesgo, con el claro propósito de reducirla.

- En sentido horizontal la probabilidad de riesgo disminuye de izquierda a derecha y sí se toma en cuenta el criterio económico se podrá dilucidar que no tiene sentido invertir en niveles de seguridad altos cuanto más baja es la probabilidad de ocurrencia. Por ello el nivel de seguridad debe bajar en sentido horizontal de izquierda a derecha, empezando en una valor mayor de acuerdo al tipo de severidad que se tenga. En este caso es que entran a tallar el tipo de decisiones diferentes a los niveles de seguridad (Evasión, Disminución, Transferencia, etc.), lo cual puede incluso determinar el no usar ningún nivel de seguridad (aceptación)

En la siguiente página mostramos en una tabla las decisiones tomadas en base a la Matriz de Decisiones, en las Instalaciones Remotas de Uso Telefónico.

De la Tabla 4.1 y de acuerdo a la Matriz de Decisiones de la tabla 4.20 se han decidido las siguientes acciones

Tabla 4.21 : Decisiones Tomadas para la seguridad de una instalación remota de uso telefónico

AMBIENTE	RIESGO	EVASION	DISMINUCIÓN	DISEMINACIÓN	ACEPTACION	TRANSFERENCIA
AMBIENTE A	Incendio		Si (Alto)			
	Sabotaje		Si (Alto)			
	Fraude				Si	
AMBIENTE B	Incendio		Si (Alto)			
	Sabotaje		Si (Alto)			
SALA GRUPO ELECTRÓGENO	Incendio		Si (Alto)			
	Robo		Si (Mínimo)			
	Sabotaje		Si (Mínimo)			
SUB ESTACIÓN ELÉCTRICA	Incendio		Si (Alto)			
	Sabotaje		Si (Mínimo)			SI
PATIO	Incendio		-		Si	
	Robo		-		Si	

Fuente : Elaboración Propia

CAPÍTULO V

ANÁLISIS TÉCNICO DEL SISTEMA DE SEGURIDAD PROPUESTO SISTEMA INTEGRAL INTELIGENTE DE SEGURIDAD (SIIS)

5.1 CRITERIOS PARA DISEÑO DEL SISTEMA DE SEGURIDAD

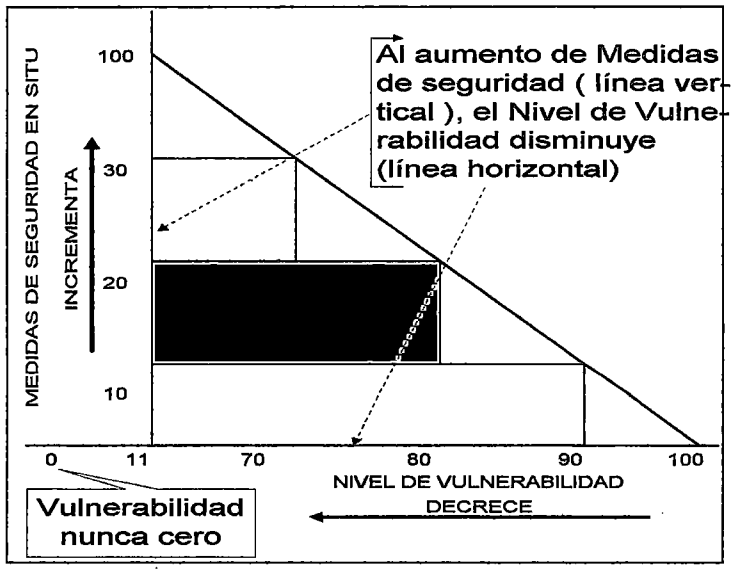
5.1.1 Cuando los niveles de medidas de seguridad aumentan, las vulnerabilidades disminuyen

El nivel de vulnerabilidad contra los riesgos se reduce con la implementación de medidas de seguridad. Algunas de estas medidas tienen una gran capacidad para compensar vulnerabilidades más que otras. El nivel de vulnerabilidad y el valor relativo de cada medida de seguridad mencionada para reducirla, puede ser expresada numéricamente.

5.1.2 Toda medida de seguridad tiene vulnerabilidades

Un nivel de vulnerabilidad de cero nunca podrá ser obtenido, ya que toda la medida de seguridad tiene propiamente vulnerabilidades. Una o más vulnerabilidades pueden ser identificadas con una medida de seguridad establecida.

Gráfica 5.1 : Relación Medidas de Seguridad - Vulnerabilidad

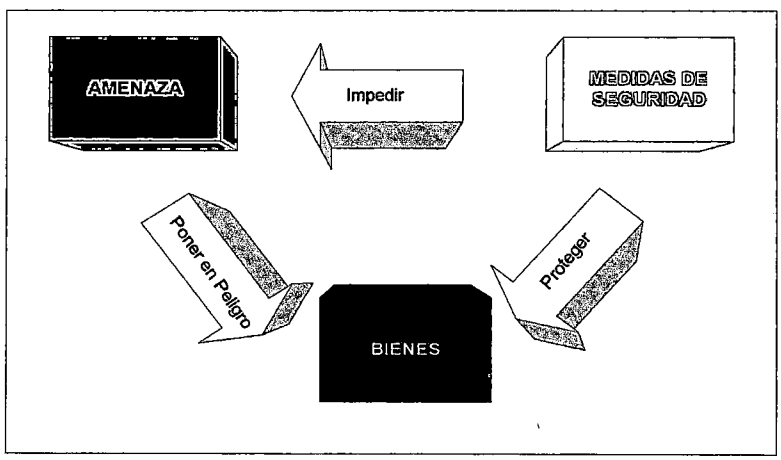


Fuente : Elaboración Propia

5.1.3 Un aceptable nivel de vulnerabilidad puede obtenerse con la implementación de las medidas de seguridad

Existe una gran variedad de medidas de seguridad que pueden lograr un nivel arbitrario sobre las vulnerabilidades. Añadiendo estas medidas, los niveles de vulnerabilidad pueden ser ajustados a un nivel proporcional por su importancia, sensibilidad o nivel de clasificación.

Gráfica 5.2 : Interacción de las Medidas de Seguridad



5.2 MEDIDAS DE SEGURIDAD

Como se ha mencionado anteriormente, los riesgos son aquellos eventos futuros, y por tanto inciertos que generarían pérdidas, la vulnerabilidad a estos eventos productores de pérdidas es la debilidad de nuestra seguridad. En consecuencia, para disminuir la vulnerabilidad se implementó una combinación de medidas de seguridad. Habiendo analizado y evaluado los riesgos, se tomó la decisión de que medida se adoptó dada las circunstancias. Los tipos de protección se basan en la utilización de las medidas de seguridad que se pueden clasificar en :

Medidas de Seguridad Técnicas

- Medidas de Seguridad Físicas (Apéndice C)
- Medidas de Seguridad Electrónicas (Apéndice D).

Medidas de Seguridad Humanas (Apéndice E)

- Servicios de Vigilancia Humana : Vigilancia Fija, Vigilancia Móvil, Manejos de Centros de Control.

Medidas de Seguridad Económicas (Apéndice F)

- Póliza de Seguros, Fondos de Autoseguros.

5.3 CONCEPTO DE LAS CUATRO "D" DE LAS MEDIDAS TÉCNICAS Y HUMANAS

Para el diseño de las medidas técnicas y humanas se utilizó el concepto de las 4D´s de la seguridad :

- Demorar
- Detectar
- Disuadir

- Detener.

A continuación explicamos cada concepto:

5.3.1 DEMORAR

Utilizar medidas de seguridad implementadas que tomarán tiempo para ser siniestradas por las amenazas y este tiempo se utilizará para responder al evento y evitar o disminuir la pérdida resultante.

La medición de la efectividad de este factor se expresa por el tiempo de retardo.

Las medidas de seguridad de demora son:

- Puertas
- Rejas
- Cercos
- Puertas Corta fuego
- Sellos de agujeros y pase de cables resistentes al fuego.
- Vigilancia fija

5.3.2 DETECTAR

Utilizar medidas implementadas que identifican lo más tempranamente posible un evento programado como : intrusión, presencia de humo, rotura de vidrios, fugas de agua, etc.; de manera que se generen respuestas al evento para impedir su ocurrencia o propagación. En el caso de una intrusión, el dispositivo de alarma debe ser colocado en el punto más lejano del blanco. En el caso de incendio lo más cercano, según normas internacionales.

La medición de la efectividad de la detección considera dos factores:

- La capacidad de percibir la acción del adversario
- El tiempo de detección, necesario para activar la alarma

Las medidas de seguridad de detección son:

- Iluminación
- Centro Receptor de Alarmas
- Sistemas de alarma perimetral, periférica, volumétrica conectadas a una Central de Alarmas Remota
- Sistema de detección automática de incendios conectada a una Central de Alarmas Remota
- Sistemas de alarma perimetral, periférica, volumétrica conectadas a una Central de Alarmas local.
- Sistema de detección automática de incendios conectada a una Central de Alarmas local
- Servicio de Vigilancia Fija, comunicación vía radio
- Servicio de Vigilancia Fija, comunicación vía teléfono
- Servicio de Manejo de Centro de Control

5.3.3 DISUADIR

Son medidas que dan la apariencia, efectiva o supuesta, de que una amenaza, especialmente delincuencial, tendrá grandes posibilidades de ser detectado. El agresor evaluará los beneficios / pérdida personales y se arrepentirá.

Las medidas de seguridad disuasivas son:

- Vigilancia Fija

- Cercos perimetrales
- Publicidad o Señalización
- Iluminación

5.3.4 DETENER

La detención de la amenaza es la última meta de cualquier medida de seguridad, la medición de la efectividad de la respuesta se expresa por el tiempo que esta respuesta toma (tiempo transcurrido desde la detección de la acción del adversario hasta su neutralización).

Las medidas de seguridad de detención son:

- Seguridad de apoyo exterior (Policía, Bomberos, etc.)
- Servicio de Vigilancia Móvil
- Vigilantes fijos
- Mangueras Contra Incendio
- Extintores Manuales de Incendios
- Sistemas automáticos de extinción de incendios

5.4 CARACTERÍSTICAS DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y HUMANAS

Al realizar el diseño del sistema de seguridad se consideraron las siguientes características de las medidas de seguridad, existiendo dos opciones: Protección en serie y protección redundante.

5.4.1 PROTECCIÓN EN SERIE

Para que la amenaza logre su objetivo debe superar las medidas de seguridad en secuencia.

La protección en serie provoca los siguientes efectos:

- Aumenta la incertidumbre de la amenaza sobre el sistema de protección.
- Requiere mayores preparativos para el ataque.
- Crea etapas adicionales en las que la amenaza puede fallar o desistir al ser detectado o interceptado.

5.4.2 PROTECCIÓN REDUNDANTE

Para evitar que zonas queden desprotegidas por razones de fallas o averías, es importante contemplar la existencia de medidas redundantes en especial en instalaciones de alto riesgo. Por ejemplo, proteger una puerta de acceso con sensores electromagnéticos y con sensores infrarrojos que apunte hacia ésta.

5.5 ESTILO DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y HUMANAS

Al realizar el diseño se consideró también los estilos de los sistemas de seguridad de acuerdo a la instalación que se está protegiendo, existiendo dos caminos bien diferenciados : Enmascarado y visto.

Es importante tener en cuenta que se usó un sistema mixto, con el fin de no descubrir todo el despliegue y mantener un aceptable nivel de disuasión.

5.5.1 ESTILO ENMASCARADO

Con el sistema enmascarado las medidas quedan ocultas, para

garantizar la inviolabilidad, para no afectar con ellas la imagen que se desea dar o simplemente para no dar con el una idea del valor de los bienes que se custodian.

5.5.2 ESTILO VISTO

En el sistema visto se persigue ante todo la disuasión, se parte de la base que no se ignora el valor de los bienes o valores que se custodian, o es muy sencillo tener la idea de éste. La imagen no sólo queda deteriorada sino que incluso queda potenciada. Este sistema tiene como punto vulnerable, la mayor facilidad para conocer el despliegue y las rutinas.

5.6 NIVELES DE LAS MEDIDAS DE SEGURIDAD TÉCNICAS Y HUMANAS

El nivel de seguridad establecido estará en función del riesgo y de la disponibilidad de recursos para garantizar su seguridad.

Los niveles de seguridad pueden clasificarse de la siguiente manera:

5.6.1 NIVEL DE SEGURIDAD MÍNIMO

El objetivo que se establece es **Demorar** el acceso no controlado a una instalación o impedir actividades externas no autorizadas y en el caso de incendio, consiste en detectar la propagación del fuego, calor o humo.

En este nivel de protección basta contar con medidas físicas básicas de seguridad u ordinarias.

5.6.2 NIVEL DE SEGURIDAD BAJO

Se establece cuando se **Demora y Disuade** la amenaza que actúa

contra la instalación. Las medidas de seguridad físicas deben ser más resistentes que las del anterior nivel, deben ser complementadas con elementos básicos de disuasión e intrusión.

5.6.3 NIVEL DE SEGURIDAD MEDIO

Las medidas de seguridad asociadas a este nivel deben **Demorar, Disuadir y Detectar y Detener** el intento de agresión. Este sistema protegería la mayoría de las actividades externas no autorizadas. Contempla el establecimiento de una zona de seguridad (perimetral) perfectamente determinada e identificada mas allá de los confines del ambiente protegido complementado con un sistema de disuasión como la iluminación. En el caso de protección contra incendios los ambientes deben ser hermetizados con respecto al exterior.

Es necesaria la existencia de elementos de detección básicos que anuncien a una Central Remota, que coordine con las fuerzas de apoyo exterior para la detención.

5.6.4 NIVEL DE SEGURIDAD ALTO

Su funcionalidad permite **Demorar, Disuadir, Detectar y Detener,** la mayoría de las actividades externa e internas no autorizadas.

Para casos distinto a medidas contra incendio, para alcanzar este nivel de protección es preciso incorporar los siguientes elementos :

- Sistema de cerco eléctrico monitoreado
- Sistema de detección perimetral, periférico y volumétrico monitoreado
- Iluminación de alta seguridad monitoreado
- Circuito cerrado de televisión monitoreado
- Control de accesos al local o dentro del local monitoreado

- Servicio de Seguridad Móvil
- Servicio de Seguridad a través del manejo del Centro de Control

Para el caso de las medidas contra incendio se incorporará los siguientes elementos :

- Sistema de detección de respuesta rápida monitoreado
- Sistema de extinción automática de incendios monitoreado
- Materiales resistentes y retardantes al fuego
- Planes de seguridad que permitan prever las situaciones de incidencia que se produzcan
- Coordinación con fuerzas de apoyo exterior

Para ambos un Centro de Recepción de Alarmas con recepción y control no redundantes.

5.6.5 NIVEL DE SEGURIDAD MÁXIMO

Este sistema es diseñado para **Demorar, Disuadir, Detectar y Detener** todas las actividades internas o externas no autorizadas, además de las medidas citadas en el nivel anterior (nivel alto) este sistema esta caracterizado por:

- Un sistema de alarma sofisticado en serie y redundante potente para ser burlado por un solo individuo.
- Para el caso de incendio estará protegido con:
    - Sistemas de detección de respuesta muy rápida
    - Sistema de extinción interior y exterior
    - Materiales resistentes al fuego con resistencia mínima de 3 horas
- Para ambos casos deberán contar con Centro de Recepción de Alarmas en uno o más locales protegidos, con recepción y control redundante y un sitio para la fuerza de respuesta (reacción) en la misma instalación con

individuos altamente entrenados, 24 horas al día y equipados para operaciones de contingencia; dedicados a neutralizar o contener cualquier amenaza contra el bien protegido hasta el arribo de asistencia fuera del sitio.

5.7 CONCEPCIÓN DEL SISTEMA DE SEGURIDAD PROPUESTO CON LAS MEDIDAS TÉCNICAS Y HUMANAS

El sistema propuesto para la protección de las IRUT estará diseñado de tal manera que deberá realizar las funciones de detección, retardo y respuesta en un período de tiempo menor que el requerido por el adversario para alcanzar su objetivo de acuerdo a lo siguiente:

- Básicamente la detección será realizada a través de medidas de seguridad electrónicas.
- La demora a que se propague en forma rápida el siniestro estará basado en las medidas de seguridad físicas.
- La acción o rapidez de respuesta efectiva al riesgo se dictará por el nivel operativo de las medidas de seguridad electrónicas implementadas.
- Los hombres de seguridad están incluidos en este contexto pero através del servicio de los grupos de reacción o vigilancia móvil, pues el elemento humano nunca será descartado pero si reducido y sustituido por medidas de seguridad electrónicas que pueden detectar riesgos.
- La seguridad estará centralizada, a través de una Central Receptora de Alarma y Teleservicios, gracias al estado actual de la tecnología permite una intercomunicación entre lugares muy alejados entre sí, y que expertos muy cualificados sigan el suceso y puedan dar instrucciones al respecto o manipular los mandos que accionan las correspondientes medidas de seguridad.

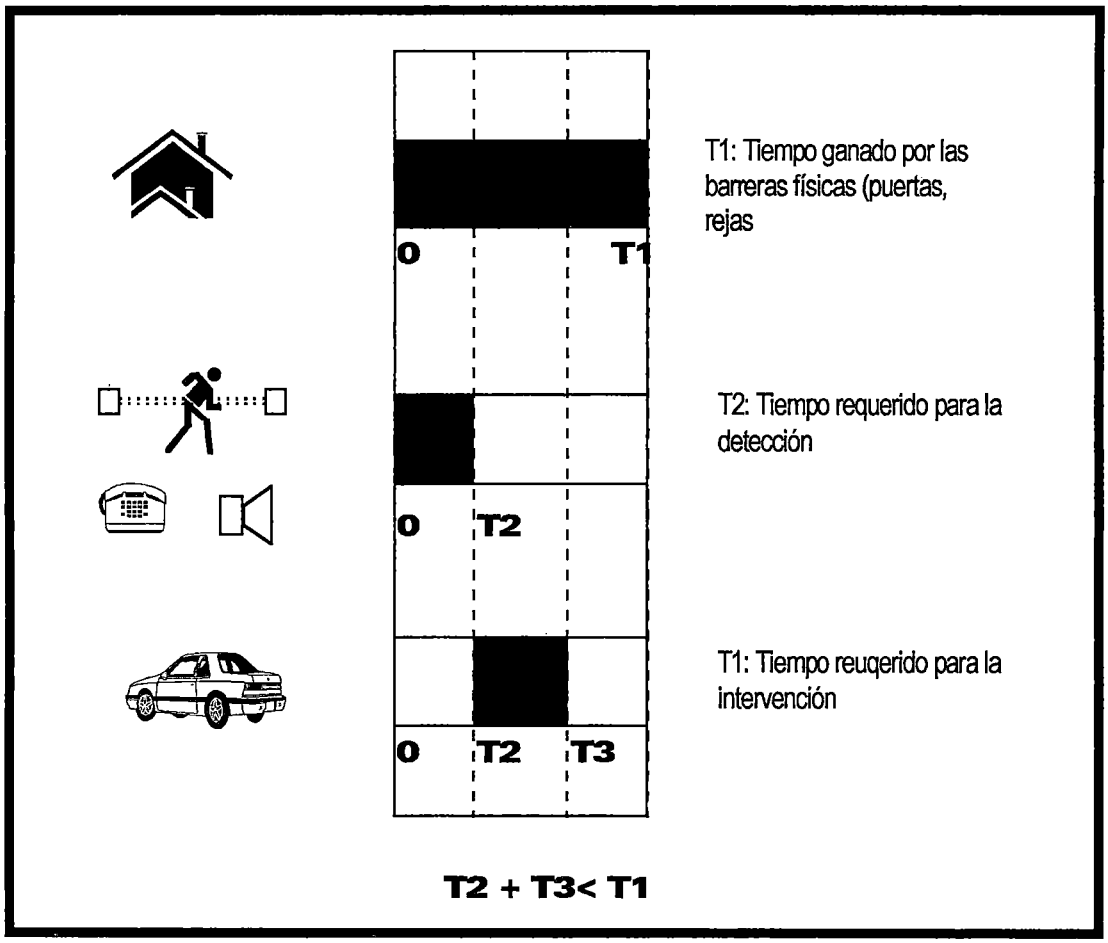
Para mostrar como afecta al tiempo de ocurrencia de un riesgo las

medidas de seguridad tomadas, se ha confeccionado un esquema.

En este esquema se muestra como el Sistema Propuesto al cual le hemos denominado Sistema Inteligente Integrado de Seguridad debe tener un tiempo de acción menor al tiempo de ocurrecia del riesgo para que sea totalmente justificado. Es decir un sistema de este tipo debe tomar un lapso desde que detecta hasta que reacciona menor al tiempo que tomaría el riesgo en afectar los bienes resguardados desde su comienzo.

En la siguiente página se muestra el esquema citado:

Gráfico 5.3: Tiempo de Ocurrencia del Riesgo y Acción del SIIS

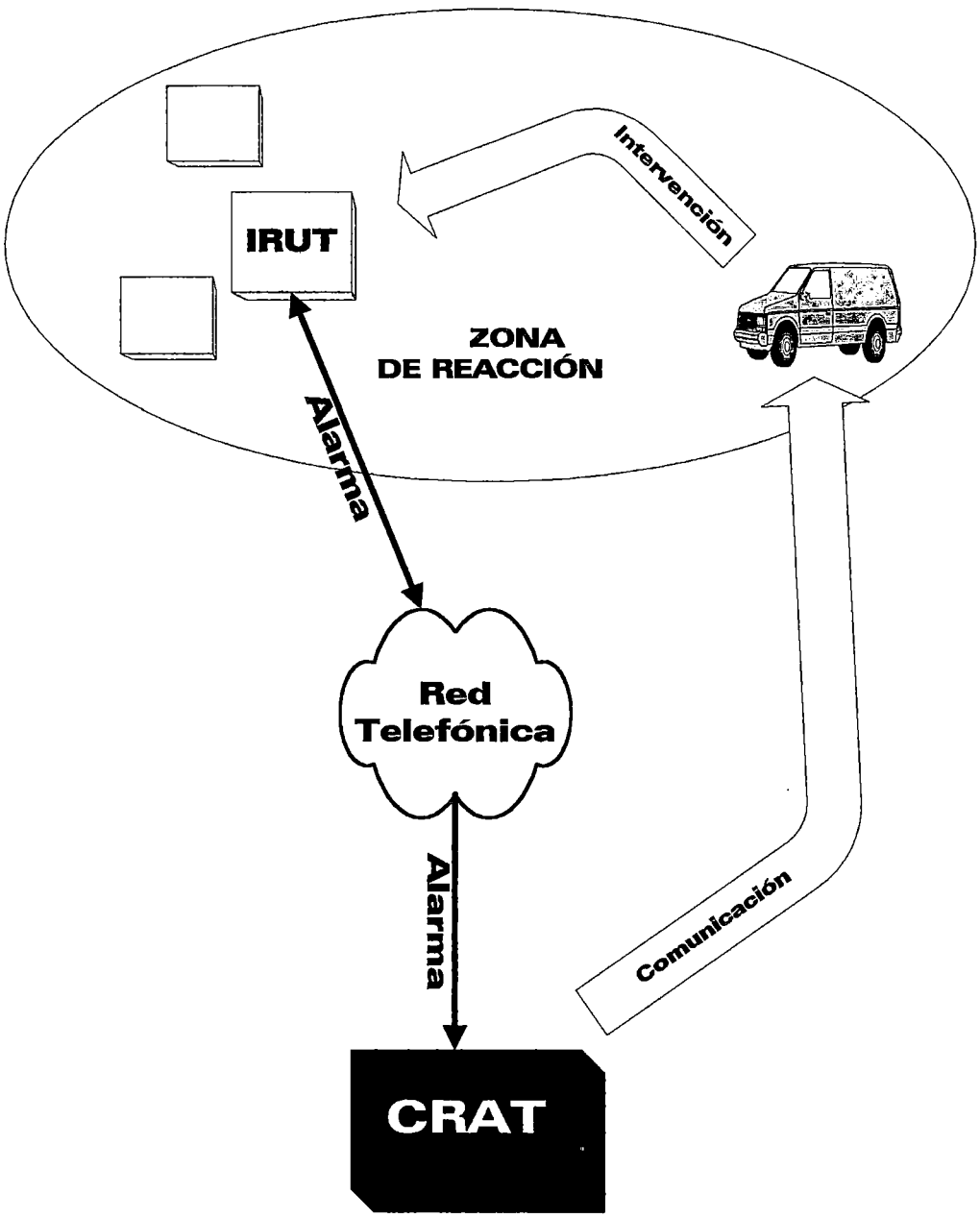


Fuente: Elaboración Propia

En el siguiente esquema se representa como estarían controladas las Instalaciones Remotas de Uso Telefónico (IRUT), las cuales estarían centralizadas para su supervisión y control a través de las líneas de comunicación telefónica con una Central de Recepción de Alarmas y Teleservicios (CRAT) y se crearán anillos de reacción que consisten en las

zonas sobre las cuales tendrían cobertura los servicios de Vigilancia Móvil y se contaría con el apoyo de elementos externos o complementarios como las policía, bomberos, serenazgo, etc.

Gráfico 5.4: Control de las IRUT através de la CRAT



Fuente: Elaboración Propia

A continuación se muestra la tabla que describe las medidas de seguridad tomadas para la instalación en estudio.

5.8 ASIGNACIÓN DE MEDIDAS DE SEGURIDAD TÉCNICAS Y HUMANAS SEGÚN EL NIVEL DE SEGURIDAD

Tabla 5.1 : Tabla de Medidas de Seguridad según nivel de seguridad en una IRUT

AMBIENTE	RIESGO	NIVEL DE SEGURIDAD	DEMORAR	DISUADIR	DETECTAR	DETENER
AMBIENTE A	INCENDIO	ALTO	Sellos Pasa Cables Puertas Corta Fuego	Señales de Prevención Mantenimiento Protección Técnica	Detectores de Incendio Estación de Alarma Sirena Monitoreo Remoto	Sistema Automático de Extinción Fuerzas de Apoyo Externo: Bomberos Vigilancia Móvil
	SABOTAJE	ALTO	Cerco Puerta Blindada Interna Puerta Blindada Externa Lectora Interna Lectora Externa	Cerco Eléctrico Exterior Cámara Externa Iluminación	Detector Infrarrojo Pasivo Contacto Magnético Detector Sísmico Cerco Eléctrico Sensor Haz Fotoeléctrico Monitoreo Remoto Cámara Interna	Vigilancia Móvil Fuerza de Apoyo Externo: Policías
AMBIENTE B	INCENDIO	ALTO	Sellos Pasa Cables Puerta Corta Fuego	Señales de Prevención Mantenimiento Protección Técnica	Detectores de Incendio Estación de Alarma Sirena Monitoreo Remoto	Sistema Automático de Extinción Fuerzas de Apoyo Externo: Bomberos Vigilancia Móvil
	SABOTAJE	ALTO	Puerta Blindada Interna Puerta Blindada Externa Lectora Interna Lectora Externa	Cámara Externa	Detector Infrarrojo Pasivo Contacto Magnético Monitoreo Remoto Cámara Interna	Vigilancia Móvil Fuerza de apoyo externo: Policía

AMBIENTE	RIESGO	NIVEL DE SEGURIDAD	DEMORAR	DISUADIR	DETECTAR	DETENER
SALA GRUPO ELECTRÓGENO	INCENDIO	ALTO	Sello Pasa Cable Puerta Corta Fuego	Señales de Prevención Mantenimiento Protección Técnica	Detector de Incendio Estación Manual de Alarma Sirena Monitoreo Remoto	Sistema Automático de Extinción Fuerzas de Apoyo Externo: Bomberos Vigilancia Móvil
	ROBO	MÍNIMO	Puerta Cerramiento Básico			
	SABOTAJE	MÍNIMO	Puerta Cerramiento Básico			
SALA SUB ESTACIÓN ELÉCTRICA	INCENDIO	ALTO	Sello Pasa Cable Puerta Corta Fuegos	Señales de Prevención Mantenimiento Protección Técnica	Detector de Incendio de Estación Manual de Alarma Sirena Monitoreo Remoto	Sistema Automático de Extinción Fuerza de Apoyo Externo: Bomberos Vigilancia Móvil
	SABOTAJE	MÍNIMO	Puertas Cerramiento Básico			

Fuente : Elaboración Propia

Además de los dispositivos señalados, se necesita una unidad de control conformada por una unidad principal de control, fuente de energía, baterías, unidad de control de alarmas de incendio, de intrusión, etc. y equipos de transmisión a través de equipo de conectividad y envío de señales o modem y una línea de Red Telefónica Conmutada para la transmisión de señales a la Central Remota de Alarmas y Teleservicios.

5.8.1 CONFIGURACIÓN MEDIDAS TÉCNICAS EN LA IRUT

Tabla 5.2 (A) Instalaciones Electrónicas de Vigilancia y Detección e Instalaciones Físicas en la IRUT

SISTEMA	MEDIDAS	ELEMENTO	LUGAR	Nro.
CONTRA INCENDIOS	ELECTRÓNICA	DETECTORES DE HUMO	Ambiente A	2
			Ambiente B	2
			Sub Estación Eléctrica	1
		DETECTORES TÉRMICOS	Sala Grupo Electrógeno	1
		DETECTORES DE LLAMA	Sala Grupo Electrógeno	1
		ESTACIÓN MANUAL	Ambiente A	1
			Patio	1
		SENSOR DE INUNDACIÓN	Ambiente B	1
			S.S.H.H.	1
		SISTEMA AUTOMÁTICO DE EXTINCIÓN (Gas)	Ambiente A	1
			Ambiente B	1
		SISTEMA AUTOMÁTICO DE EXTINCIÓN (Polvo)	Sala Grupo Electrógeno	1
			Sub Estación Eléctrica	1
		SIRENAS	Patio	1
	FÍSICAS	PUERTAS CORTA FUEGO	Ambiente A	1
			Ambiente B	1
			Sala Grupo Electrógeno	1
			Sub Estación Eléctrica	1
		SELLOS PASA CABLES	Ambiente A	1
			Ambiente B	1
			Sala Grupo Electrógeno	1
			Sub Estación Eléctrica	1
CONTRA INTRUSIÓN (ROBO Y SABOTAJE)	ELECTRÓNICAS	CONTACTOS MAGNÉTICOS	Ambiente A	1
			Ambiente B	1
			Sala Grupo Electrógeno	1
			Sala Sub Estación Eléctrica	1
			Ingreso Principal (Patio)	1
		DETECTORES INFRARROJOS PASIVOS (PIR)	Ambiente A	1
			Ambiente B	1
		SENSOR DE HAZ FOTOELÉCTRICO	Area Perimetral	4
		LECTORAS	Ambiente A	1
			Ambiente B	1
			Ingreso Principal (Patio)	1

Tabla 5.2 (B) Instalaciones Electrónicas de Vigilancia y Detección e Instalaciones Físicas

SISTEMA	MEDIDAS	ELEMENTO	LUGAR	Nro.
		CÁMARAS GIRATORIAS	Ambiente A	1
			Ambiente B	1
		CÁMARA FIJA	Ingreso Principal (Patio)	1
	FISICAS	CERCO ELÉCTRICO	Área Perimetral	1
		PUERTAS BLINDADAS	Ambiente A	1
			Ambiente B	1
			Ingreso Principal (Patio)	1
		PUERTAS CON CERRAMIENTO BÁSICO	Sala Grupo Electrógeno	1
			Sala Sub Estación Eléctrica	1

Fuente : Elaboración Propia

Tabla 5.3 Configuración de la Unidad de Control en la IRUT

LUGAR	COMPONENTE	CANTIDAD
AMBIENTE B	Unidad Principal de Control (Tarjeta Madre)	1
	Unidad de Control de Alarmas de Incendio	1
	Unidad de Control de Alarmas de intrusión	1
	Unidad de Control de Vídeo	1
	Fuente de Energía	1
	Batería	1

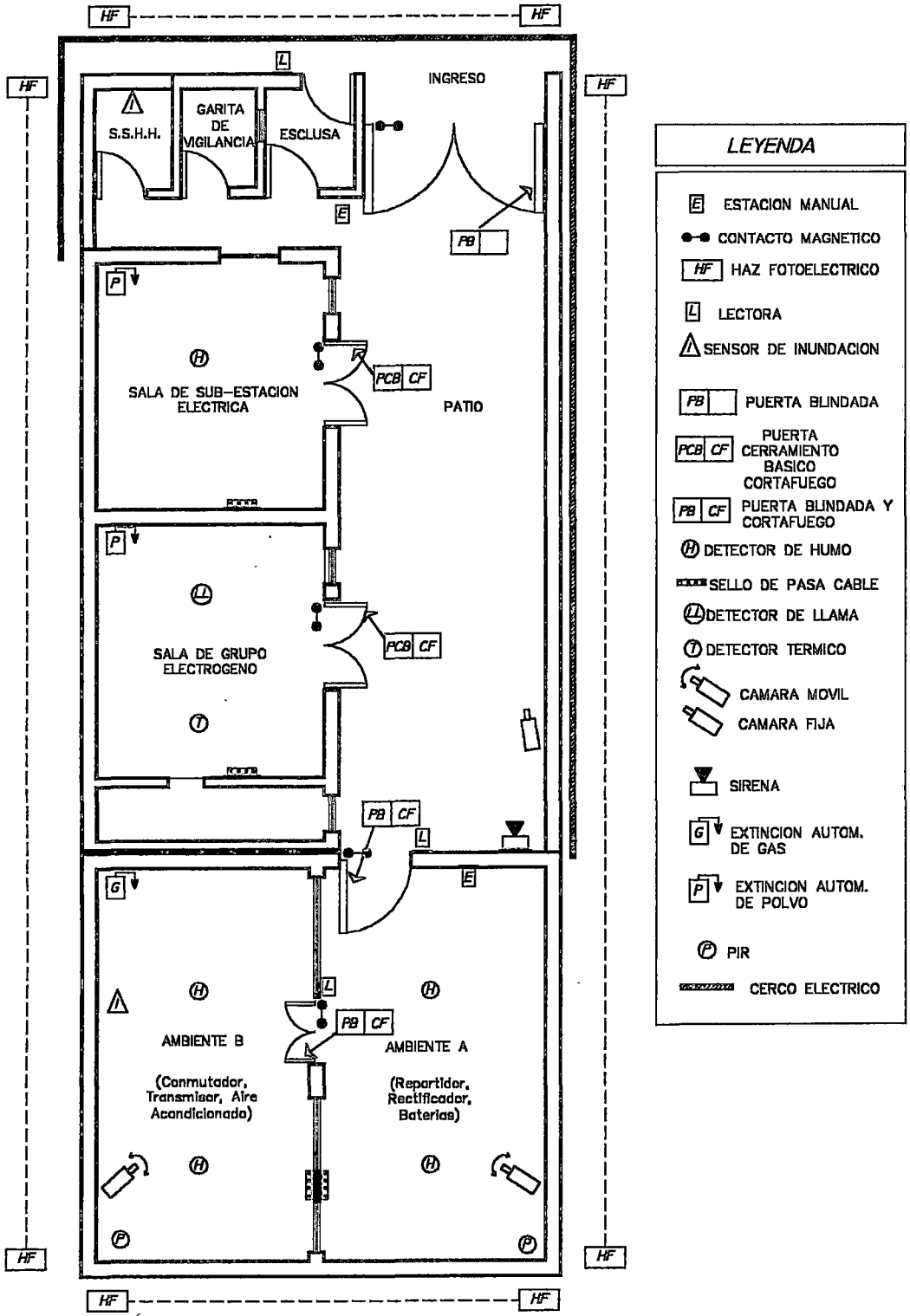
Fuente : Elaboración Propia

Tabla 5.4 Configuración del Equipo de Transmisión en la IRUT

LUGAR	COMPONENTE	CANTIDAD
AMBIENTE B	Equipo de Conectividad y envío de Señales (Modem)	1
	Línea Telefónica RTC	1

Fuente : Elaboración Propia

GRÁFICO 5.5 CONFIGURACIÓN DE LAS MEDIDAS DE SEGURIDAD TÉCNICA EN LA IRUT



5.8.2 CONFIGURACIÓN MEDIDAS TÉCNICAS EN LA CRAT

La configuración, arquitectura y componentes de una CRAT, según el Apéndice D (Medidas de Seguridad Electrónica), están directamente relacionados con la prestación de los tipos de servicios previstos a establecer, así como su extensión, dimensionamiento, atención geográfica, etc.

La configuración, la arquitectura básica de una CRAT, se estructura en cuatro artes:

5.8.2.1 SERVICIOS ESTABLECIDOS

Se entenderá por servicios establecidos el diseño y desarrollo de los servicios diferenciados por bloques de actividad o funcionalidad. Los servicios que tendrá la Central Receptora de Alarmas y Teleservicios será:

- Telealarma
- Televigilancia
- Telemando

5.8.2.2 OPERATIVA FUNCIONAL

Se caracteriza, porque dispondrá de medios de vigilancia, recepción y control no redundantes y de gestión totalmente automatizada. Sus equipos y programas informáticos disponen de características de puesto y multitarea permitiendo, por tanto, un tratamiento automatizado y personalizado para cada tipo de señal y nivel de seguridad y prioridad. Tendrá una capacidad para monitorear como máximo 200 Instalaciones Remotas de Uso Telefónico.

5.8.2.3 INSTALACIONES ESPECÍFICAS

Para su operativa funcional la CRAT cuenta con lo siguiente:

- **Equipos de recepción y control de señales remotas**: Dos módulos de comunicaciones por línea conmutada, cada módulo de comunicaciones controla cuatro líneas telefónicas conmutadas (RTC) incluyendo sus correspondientes módems, y circuitos de adaptación, marcación y protección. Incluye asimismo la circuitería necesaria para la conexión de fonía y los correspondientes pasos de fonía a datos y viceversa.

- **Sistemas de vigilancia o verificación y gestión**: dos procesadores con un software en entorno Windows con su correspondiente sistema operativo, permite supervisar los estados de cada dispositivo o sistema instalado en el local remoto (estado normal, avería, perdida de comunicación, alarma, etc.), permite el archivo de eventos históricos, permite la programación remota de parámetros y bases de datos del sistema. Para lo cual estarán en conexión entre puestos mediante red y software de comunicaciones.

Tabla 5.5 Instalaciones Específicas en la CRAT

Equipos de Recepción y Control de Señales Remotas	2 Módulos
Sistemas de Vigilancia y Gestión	2 Procesadores
Sistemas de Comunicaciones	8 Líneas RTC
Líneas Telefónicas	2 Líneas RTC
Sistema de Emergencia	1 UPS

5.8.2.4 INFRAESTRUCTURA BÁSICA

Se trata de la disposición de los recursos y materiales, para el desarrollo de la actividad de la central y estos son:

- **Iluminación**, contará con iluminación suficiente para la correcta operación de las funciones de los operadores
- **Decoración**, será únicamente a través del pintado de las paredes y el alfombrado de los pisos
- **Mobiliario**, estará conformado por dos mesas sobre las cuales irán los procesadores, la impresora y además dos sillas para los operadores.
- **Fontanería**, es el área destinada en la que implementará los servicios higiénicos.
- **Instalaciones eléctricas**, serán para los puntos suficientes de toma corriente para la iluminación, aire acondicionado y los equipos específicos.
- **Aire acondicionado**, para la adecuada ventilación que permita el correcto desarrollo de las actividades por parte de los operadores durante todos los meses del año.

5.8.3 ASIGNACIÓN DE LOS MEDIOS DE SEGURIDAD HUMANOS

5.8.3.1 SERVICIO DE MANEJO DE CRAT

La disposición del personal operador está en relación directa con los tipos de servicios que se han de establecer o prestar por la CRAT, así como por el dimensionamiento y volumen de éstos, para lo cual nos hemos guiado de lo establecido en el apéndice E (Medidas de Seguridad Humana). Por este motivo, se contará con dos operadores en un puesto de 24 horas, cada uno de los cuales contará con un procesador (Sistema de Vigilancia, Verificación y Gestión)

5.8.3.2 SERVICIO DE VIGILANCIA MÓVIL

La disposición de los puestos de reacción estará en relación directa de las 200 instalaciones que serán monitoreados por la CRAT, así como por el número de incidencias que puedan presentarse, la distancia existente entre

las Instalaciones y los locales de los apoyo externo (policías, bomberos), también se consideró las distancias entre locales y su accesibilidad.

En nuestro caso se contará con 20 grupos de reacción, en promedio 1 grupo de reacción por cada 10 instalaciones, que vigilará las 24 horas del día. El grupo está constituido por una persona, sus equipos (extintores, linternas, etc.) y una unidad móvil, el servicio se realizará a través de un contrato con una empresa que brinde servicio de vigilancia.

5.8.3.3 UNIDADES DE APOYO EXTERNO

Esta conformado por las unidades de Policía, Bomberos.

5.9 ASIGNACIÓN DE MEDIDAS DE SEGURIDAD ECONÓMICA

Según el análisis y evaluación de riesgos de la tabla 4.21 del capítulo IV: Gestión de Riesgos, se debe asegurar el ambiente de la subestación eléctrica contra el siniestro de sabotaje, para lo cual la empresa deberá pagar anualmente una prima de seguro y en caso de que el siniestro logre producir daño, el asegurado (en este caso la Instalación Remota de Uso Telefónico) asume un deducible y la empresa aseguradora la indemnización, tal como se explica en el apéndice F (Medidas de Seguridad Económica).

CAPÍTULO VI

ANÁLISIS ECONÓMICO DEL SISTEMA INTEGRAL INTELIGENTE DE SEGURIDAD

Luego de establecidas las medidas de seguridad (Físicas, Electrónicas, Humanas, Económicas) que constituyen la configuración del Sistema Integral Inteligente de Seguridad, se calcularon los correspondientes presupuestos de inversiones y gastos, que se establecieron teniendo en cuenta, principalmente la dotación de puestos, la disposición del espacio, acondicionamiento de los locales, instalaciones específicas, e infraestructura complementaria para la Instalación Remota de Usos Telefónico (IRUT) y para la Central Remota de Alarmas y Teleservicios (CRAT). Los cálculos que aquí se presentan fueron elaborados a finales de 1999.

6.1 INVERSIÓN DEL SISTEMA PROPUESTO

6.1.1 ACONDICIONAMIENTO DE LA CRAT

Se tuvo en cuenta, una serie de aspectos diferenciados según las características de los servicios que se han de ubicar y establecer en la CRAT, electricidad, iluminación, fontanería, aire acondicionado, decoración, mobiliario. Además se tuvo en cuenta el establecimiento de los adecuados programas de mantenimiento que se detallan más adelante. Estos desembolsos se pueden apreciar en la tabla 6.1, preparada para una mejor visión y análisis.

Tabla 6.1 Costo de Acondicionamiento de la CRAT

(US $)

Servicio de Acondicionamiento	Concepto	Cantidad	Costo Unitario Equipo	Costo Total Equipo	Costo Unitario Instalación	Costo Total Instalación
Iluminación	Luminarias	4	20	80	10	40
Aire Acondicionado	Aire Acondicion.	1	3.000	3.000	200	200
Decoración	Alfombras	1	300	300	50	50
	Pintado					100
Mobiliario	Mesa	2	150	300	20	40
	Silla	2	50	100		0
	Estante	1	300	300		0
Fontanería				500	200	200
Instalación Eléctrica						1.000
Total				**4.580**		**1.630**

Fuente : Elaboración Propia

6.1.2 INSTALACIONES ESPECÍFICAS

Son aquellas que corresponden y vienen determinadas por los distintos servicios que vaya a prestar el SIIS y que, por tanto, precisan de instalaciones específicas.

En este sentido, cabe destacar la disposición de equipos y sistemas para la recepción y gestión de señales, sistema de vigilancia y verificación, equipos y programas informáticos especiales, redes de comunicaciones conmutadas, sistema de grabación de audio, videos y datos, sistemas de alimentación eléctrica ininterrumpida, etc.

En la tabla 6.2 se muestran los costos de las medidas de seguridad electrónicas en las Instalaciones Remotas de Uso Telefónico. Estos equipos se han agrupado de acuerdo a la clasificación de los componentes de la Seguridad electrónica (Apéndice D).

Tabla 6.2 : Costo de Instalaciones Especificas Electrónicas en las IRUT

(US $)

Componente Electrónico	Descripción	Cantidad	Costo Unitario Equipos	Costo Total Equipos	Costo Unitario Instalación	Costo Total Instalación
Unidad de Control	Unidad Principal de Control	1	250	250	100	100
	Fuente de Energía	1	150	150	100	100
	Baterías	1	150	150	50	50
	Unidad Control de Lectoras Acceso	1	250	250	100	100
	Unidad de Control de Intrusión	1	250	250	100	100
	Unidad de Control Alarmas Incend.	1	250	250	100	100
	Unidad de Control de Vídeo	1	250	250	100	100
Equipo de Transmisión	Equipo de Conectividad y envío de señales	1	250	250	100	100
Instalaciones de Vigilancia, Detección.	Detector de Humo	5	50	250	15	75
	Detector de Llama	1	30	30	15	15
	Detector de Temperatura	1	30	30	15	15
	Sensor de Inundación	2	30	30	15	15
	Sirenas	1	50	50	15	15
	Estaciones Manuales	2	50	100	15	30
	Sistema de Extinción Gas	2	2000	4.000	500	1.000
	Sistema de Extinción Polvo	2	500	1.000	300	600
	Detector Infrarrojo Pasivo	3	25	75	10	30
	Sensor de Haz Fotoeléctrico	4	300	1.200	50	200
	Contactos Magnéticos	5	5	25	5	25
	Cámaras Fija	2	700	1.400	100	200
	Cámara Móvil	1	1.000	1.000	100	100
	Lectoras Acceso	3	300	900	100	300
Total				**11.890**		**3.330**

Fuente : Elaboración propia

En la Tabla 6.3 se muestran los costos de la línea telefónica para la comunicación de las IRUT con la CRAT

Tabla 6.3 : Costo de Sistema de Comunicaciones en la IRUT (US $)

Componente de Comunicación	Descripción	Cantidad	Costo Unitario Instalación	Costo Total Instalación
Línea Telefónica	Red Telefónica Conmutada	1	200	200
Total				**200**

Fuente : Elaboración propia

En la tabla 6.4 se muestran los costos de las medidas de seguridad física en las IRUT.

Tabla 6.4 Costo de Instalaciones Especifica Física en las IRUT (US $)

Componente Electrónico	Componente	Cantidad	Costo Unitario Equipos	Costo Total Equipos	Costo Unitario Instalación	Costo Total Instalación
Protección Contra Intrusión Sabotaje	Puerta Blindadas Cortafuego	2	1.000	2.000	75	150
	Puertas Cerramiento Básico Cortafuego	2	700	1.400	75	150
	Puerta Blindada	1	500	500	50	50
	Cerco Eléctrico	1	500	500	50	50
Protección Contra Incendio	Puerta Cortafuego	2	500	1.000	50	100
	Sellos Pase Cables	1	1.000	1.000	500	500
	Extintores Manuales	2	200	400	20	40
Total				**6.800**		**1.040**

Fuente : Elaboración propia

En la tabla 6.5 se muestra los costos de los componentes electrónicos que se instalaran en la CRAT

Tabla 6.5: Costo de Instalaciones Especificas Electrónicas en la CRAT (US $)

Concepto	Descripción	Cantidad	Precio Unitario Equipo	Costo Total Equipo
Sistema de Vigilancia, y Gestión	Procesadores	2	1.000	2.000
	Sistema Operativo	2	1.000	2.000
	Impresora	2	250	500
	Software de Gestión	1	20.000	20.000
	Auricular y Micrófono	2	50	100
	Grabadora de Audio	2	500	1.000
Equipos de Recepción y Control de Señales Remotas	Tarjeta para Comunicaciones Red Conmutada	2	300	600
	Tarjeta Controladora de Comunicación	1	300	300
	Tarjeta para Interface Vídeo	1	300	300
	Tarjeta para Interface Grabadoras	1	300	300
Sistema de Emergencia	UPS (Suministro Interrumpido de Potencia)	1	1.000	1.000
Total				**28.100**

Fuente : Elaboración propia

Tabla 6.6 Costo de Sistemas de Comunicaciones en la CRAT (US $)

Componente	Descripción	Cantidad	Costo Unitario	Costo Total
Comunicaciones para el Sistema	Líneas RTC	8	200	1.600
Comunicación para Coordinación	Líneas RTC	2	200	400
Total				**2.000**

Fuente : Elaboración propia

Tabla 6.7 Inversión Intangible por Instalación Específico Electrónica en la CRAT (US $)

Concepto	Descripción	Cantidad	Costo Unitario	Costo Total
Instalación y Conexión de Equipos	Para dos Puestos de Operador Incluye Material Eléctrico	1	2.000	2.000
Puesta en Servicio	Carga de Parámetros Operativos y Configuración del Sistema	1	5.000	5.000
Total				**7.000**

Fuente : Elaboración propia

6.2 GASTOS DEL SISTEMA PROPUESTO

6.2.1 DOTACIÓN DE PUESTOS DE SERVICIO DE VIGILANCIA HUMANA

Se dimensiono el personal preciso, en función de los servicios que se establecieron, sus características y volumen proyectado de trabajo.

Tabla 6.8 Costo por Servicio Puesto de Operador de la CRAT

Cantidad de puestos	2	Operadores
Costo del servicio	1,40	Dólares /Hora
Horas /Puesto	24	Horas/Día
Días/Semana	7	Días
Semanas/Año	52	Semanas

Fuente : Elaboración propia

Tabla 6.9 Costo del Servicio de Vigilancia Móvil para las IRUT

Cantidad de puestos	20	Grupos de Reacción
Costo del servicio	1.380	Dólares/ Mes
Costo combustible	90	Dólares Por Mes
Horas/Puesto	24	Horas/Día
Días/Semana	7	Días
Meses/Año	12	Meses

Fuente : Elaboración propia

Tabla 6.10 Costo por Puesto Administrativo y de Control de la CRAT

Cantidad de puestos	1	Supervisor
Costo del servicio	2,4	Dólares / Hora
Horas/Puesto	8	Horas / Día
Días/Semana	5	Días
Semanas/Año	52	Semanas

Fuente : Elaboración propia

Tabla 6.11 Resumen Costo Anual por tipo de puesto del Servicio de Vigilancia Humana US $

Puesto	Costo Anual
Operador de la CRAT	24.460,80
Vigilancia móvil de la IRUT	352.800,00
Administrativo de la CRAT	49.92,00
Total	**382.252,80**

Fuente : Elaboración propia

6.2.2 COSTOS DE MANTENIMIENTO

Los porcentajes promedios del mantenimiento están en función de los valores iniciales del equipo, que están basados en la indicaciones de los proveedores.

6.2.2.1 COSTO DE MANTENIMIENTO PARA EL CRAT

Tabla 6.12 Costo de Mantenimiento para la CRAT (US $)

Concepto	Valor Inicial	Porcentaje Mantenimiento	Costo de Mantenimiento
Instalaciones Específicas	28.100,00	10%	2.810,00
Acondicionamiento	4.580,00	3%	137,40
Total			**2.947,40**

Fuente : Elaboración propia

6.2.2.2 COSTO DE MANTENIMIENTO PARA LA IRUT

Tabla 6.13 Costo de Mantenimiento para la IRUT

(US $)

Concepto	Valor Inicial	Porcentaje Mantenimiento	Costo de Mantenimiento
Instalaciones Específicas Electrónicas	9.850	5%	492,50
Instalaciones Específicas Físicas	4.250	3%	127,50
Total			**620,00**

Fuente : Elaboración propia

6.2.2.3 COSTO DE MANTENIMIENTO SISTEMA DE COMUNICACIÓN

Tabla 6.14 Costo de Mantenimiento para el Sistema de Comunicaciones

(US $)

Concepto	N° Líneas	Costo Unitario de Mantenimiento	Costo Total Mantenimiento
Comunicaciones CRAT	10	20	200
Comunicaciones IRUT	200	20	4.000
Total			4.200

Fuente : Elaboración propia

6.2.3 DEPRECIACIONES

Las depreciaciones de la inversión fija como los dispositivos y los equipos instalados en las IRUT, así como los equipos de cómputo y hardware necesario para la CRAT, se calcularon en base la mayor tasa de depreciación permitida por la ley del impuesto sobre la renta.

Según información proporcionada por el proveedor, todo el equipo que se ha adquirido tendrá un valor de salvamento al final del quinto año de operación aproximadamente igual al 10%.

Tabla 6.15 Depreciación en la CRAT

(US $)

CONCEPTO	INVERSIÓN INICIAL	TASA %	PERIODOS ANUALES					VALOR RESIDUAL
			1	2	3	4	5	
Instalaciones Específicas	28.100	25%	7.025	7.025	7.025	7.025	0	0
Acondicionamiento	4.580	10%	458	458	458	458	458	2.290
Valor de Salvamento Instalaciones Específicas	28.100	10%						2.810
Total			**7.483**	**7.483**	**7.483**	**7.483**	**458**	**5.100**

Fuente : Elaboración propia

Tabla 6.16 Depreciación en la IRUT

(US $)

CONCEPTO	INVERSIÓN INICIAL	TASA %	PERIODOS ANUALES					VALOR RESIDUAL
			1	2	3	4	5	
Instalaciones Específicas	14.100	25%	2.888	2.888	2.888	2.888	425	0
Valor de Salvamento	14.100	10%						1.410
Total			2.888	2.888	2.888	2.888	425	**3.110**

Fuente : Elaboración propia

6.2.4 GASTOS POR CONSUMO DE ENERGÍA ELÉCTRICA

El gasto por energía eléctrica se basa en las especificaciones técnicas individuales de cada equipo, considerándose las tarifas vigentes de las compañías de energía 0,11 Dólares por Kw - Hr.

6.2.4.1 CONSUMO DE ENERGÍA EN LA IRUT

El consumo de electricidad de los equipos (unidades de control, de vigilancia y detección, equipo de transmisión) en la IRUT, es despreciable,

por los pequeños potenciales consumidos y el tiempo que se emplean.

6.2.4.2 CONSUMO DE ENERGÍA EN LA CRAT

Tabla 6.17 Parámetros del Consumo de Energía del Sistema de Vigilancia y Verificación

Cantidad de Procesadores	2	Computadoras
Consumo de Electricidad por hora	175	Watts
Horas/día	24	Horas
Días/Semana	7	Días
Semanas / año	52	Semanas
Costo Kw-Hora	0,11	Dólares

Fuente : Elaboración propia

Tabla 6.18 Parámetros del Consumo de Energía Equipos de Recepción y Control de Señal Remota

Cantidad de Equipos	2	Receptores
Consumo de electricidad por hora	36	Watts
Horas/Día	24	Horas
Días/Semana	7	Días
Semanas/Año	52	Semanas
Costo Kw-Hora	0,11	Dólares

Fuente : Elaboración propia

Tabla 6.19 Parámetros del Consumo Eléctrico por Iluminación en la CRAT

Cantidad de equipos	4	Luminarias
Consumo de Electricidad por hora	100	Watts
Horas/día	12	Horas
Días/Semana	7	Días
Semanas/Año	52	Semanas
Costo Kw - Hora	0,11	Dólares

Fuente : Elaboración propia

Tabla 6.20 Parámetros del Consumo Eléctrico por Aire Acondicionado

Cantidad de equipos	1	Equipo de AA
Consumo de Electricidad por hora	500	Watts
Horas/día	2	Horas
Días/Semana	7	Días
Semanas/Año	52	Semanas
Costo Kw - Hora	0,11	Dólares

Fuente : Elaboración propia

Tabla 6.21 Resumen del Costo Anual por Energía en la CRAT

(US $)

CONCEPTO	COSTO ANUAL
Sistema de Vigilancia, Verificación y Gestión	336,34
Equipos de Recepción y Control de Señales de Remotas	69,19
Iluminación	192,19
Aire Acondicionado	40,04
TOTAL	**637,76**

Fuente : Elaboración propia

6.2.5 GASTO USO DEL SISTEMA DE COMUNICACIONES

Es el consumo de la red telefónica conmutada por las señales o alarmas que se producen en las IRUT que son recepcionadas y controladas en la CRAT. Dicho consumo está en función al número de eventos que se producen en las instalaciones y al promedio de tiempo de demora por evento.

En este rubro no se ha considerado las instalaciones telefónicas propias de las empresas de telecomunicaciones, las que utilizarían su infraestructura y reducirían el costo.

Tabla 6.22 Costo Anual por el Uso del Sistema de Comunicaciones en la IRUT

(US $)

Número de Eventos por IRUT	1	Por equipo
Número de Instalaciones de Vigilancia, Detección y Control por IRUT	20	Equipos
Eventos/Mes por IRUT	1	Por Mes
Meses/Año	12	Meses
Costo Establecimiento de Comunicación	0,14	Dólares por equipo
Costo por tiempo de Comunicación	0,14	Dólares por equipo
Total	**67,20**	**Dólares**

Fuente : Elaboración propia

6.2.6 OTROS COSTOS

Se consideró también costos de materiales de oficina para la operación de la CRAT, estos costos son :

Tabla 6.23 Otros Costos Anuales de la CRAT

(US $)

Concepto	Cantidad	Unidades	Costo Unitario	Costo Total
Disquetes	24	Cjs	5	120
Cintas de Vídeo	6	Un.	5	30
Cintas de Impresora	12	Un.	10	120
Utiles de Oficina	10	Un.	10	100
Otros Gastos de Oficina	1		10	10
Total				380

Fuente : Elaboración propia

6.2.7 COSTO ANUAL POR SEGUROS

Tabla 6.24 Determinación de la Prima de Seguro por Sabotaje en la Subestación Eléctrica (US $)

Estimado de las Pérdidas Potenciales por Instalación	Costo de Reemplazo Permanente (Inversión Fija: Valor del Bien)	50.000,00
	Costo de Reemplazo (Inversión Intangible: Instalación)	5.000,00
	Costo de Sustitución Temporal	0,00
	Costo de Perdidas Relacionadas: Pagos por Servicios	1.100,00
	Costo de Pérdidas en Inversiones que Generan Ingresos (Lucro Cesante)	50.000,00
	Total	106.100,00
Reconocido		106.100,00
Deducible	33%	35.013,00
Indemnización		71.087,00
Prima de Seguro Anual	0,335%	**355,44**

Fuente : Elaboración propia

Los gastos de capacitación no se tomaron en cuenta debido a que en el contrato de compra del sistema de seguridad se incluyó una cláusula en donde la empresa proveedora se comprometió a capacitar al personal del área técnica de seguridad para que pudieran ellos mismos llevar a cabo la capacitación al personal de operación, sin que ello implicará un pago adicional.

CAPÍTULO VII

EVALUACIÓN ECONÓMICA

Con el sistema propuesto de seguridad a la cual la hemos denominado Sistema Integral Inteligente de Seguridad (SIIS) para la protección de las Instalaciones Remotas de Uso Telefónico (IRUT) es posible reducir, o disminuir considerablemente, los gastos operativos por el Servicio de Vigilancia Fija o Agentes de Seguridad (Apéndice E: Medidas de Seguridad Humana) comunes en los Sistemas de Seguridad Tradicionales. El objetivo de este estudio es el reemplazo de todos los agentes de seguridad que se encuentran en las IRUT por la implementación SIIS, en el lapso de un año.

El tipo de evaluación económica que se realizó consistió:

- Se determinó el Flujo Económico del sistema propuesto SIIS (ver tabla 7.1) con los datos del análisis económico del capítulo VI y el Flujo Económico del Sistema Tradicional (ver tabla 7.2) con los datos del Anexo 4 (Análisis Económico del Sistema Tradicional de Seguridad).

- Se determinó el Flujo Económico del Ahorro obtenido al comparar aritméticamente las dos alternativas de sistemas de seguridad (SIIS - Tradicional). Esto se hizo con la intención de mostrar cuál sería el efecto económico de implantar el SIIS en lugar de utilizar un Sistema de Seguridad Tradicional, por lo cual se decidió la diferencia aritmética de los flujos económicos de los sistemas mencionados. Al ver la tabla 7.3 se

puede notar que a través de los períodos anuales de los flujos económicos de las dos alternativas de seguridad, que los egresos que generan el Sistema Propuesto (SIIS) son menores que los de un Sistema de Seguridad Tradicional, excepto en la inversión inicial, de tal manera que al hacer la diferencia entre los egresos del SIIS y el Sistema Tradicional se consigue un flujo similar al de un proyecto con inversión inicial (flujo negativo) e ingresos (flujo positivo).

Es muy importante destacar que las determinaciones de costos se hicieron en los meses finales de 1999 y para fines de evaluación económica, esto equivale a que son cifras del periodo cero. Estos costos se mantendrán fijos durante los 5 años del horizonte de análisis de la inversión, no se ha considerado el efecto de la inflación y no varía el nivel de empleo del equipo.

Las actividades comerciales de las empresas de telecomunicaciones requieren la, implementación de un sistema de seguridad, por lo tanto, ésta es una inversión y gastos necesarios. Con base en esto, el Costo de Oportunidad del Capital (COK) que se aplicó fue igual al 15% anual, que corresponde a la tasa activa que ofrece el mercado bancario en promedio para proyectos de inversión.

Por el tipo de cifras que se tienen en el Flujo Económico del Ahorro de la comparación entre las dos alternativas de seguridad, se recomienda utilizar el método de Valor Presente (VP), de tal manera que si el VP es mayor que Cero se aceptará el sistema propuesto y si la Tasa Interna de Retorno (TIR) del flujo de comparación que se encuentre por iteración es mayor al Costo de Oportunidad del Capital (COK) se podrá afirmar que el ahorro de implementar el SIIS en lugar de un Sistema de Seguridad Tradicional es rentable.

Tabla 7.1 Flujo Económico del Sistema de Seguridad Propuesto (Sistema Integral Inteligente de Seguridad - SIIS) US $

CONCEPTO		PERIODOS ANUALES					
		0	1	2	3	4	5
NÚMERO DE INSTALACIONES		200					
INVERSIÓN	CENTRO DE RECEPCIÓN DE ALARMAS Y TELESERVICIOS (CRAT)						
	Acondicionamiento CRAT	4.580,00					
	Instalación acondicionamiento CRAT	630,00					
	Equipamiento específico CRAT	28.100,00					
	Instalación equipamiento específico CRAT	7.000,00					
	Instalación eléctrica CRAT	1.000,00					
	Comunicaciones CRAT	2.000,00					
	INSTALACIONES REMOTAS DE USO TELEFÓNICO (IRUT)						
	Equipamiento específico electrónico IRUT	2.378.000,00					
	Instalación equipamiento específico electrónico IRUT	674.000,00					
	Equipamiento específico físico IRUT	1.360.000,00					
	Instalación del equipamiento específico físico IRUT	208.000,00					
	Comunicaciones IRUT	40.000,00					
	SUB TOTAL INVERSIÓN	**3.770.680,00**					
GASTOS	VALOR DE SALVAMENTO						
	Valor de salvamento de la CRAT						-5.100,00
	Valor de salvamento de la IRUT						-917.800,00
	SUB TOTAL VALOR DE SALVAMENTO						**-922.900,00**
	MANTENIMIENTO						
	Mantenimiento de la CRAT		2.947,40	2.947,40	2.947,40	2.947,40	2.947,40
	Mantenimiento de la IRUT		159.700,00	159.700,00	159.700,00	159.700,00	159.700,00
	SUB TOTAL MANTENIMIENTO		**162.647,40**	**162.647,40**	**162.647,40**	**162.647,40**	**162.647,40**
	SERVICIO DE VIGILANCIA HUMANA (SVH)						
	Operadores CRAT		24.460,80	24.460,80	24.460,80	24.460,80	24.460,80
	Vigilancia Móvil IRUT		352.800,00	352.800,00	352.800,00	352.800,00	352.800,00
	Administrativo CRAT		4.992,00	4.992,00	4.992,00	4.992,00	4.992,00
	SUB TOTAL SVH		**382.252,80**	**382.252,80**	**382.252,80**	**382.252,80**	**382.252,80**
	CONSUMO ELÉCTRICO (CRAT + IRUT)		**637,76**	**637,76**	**637,76**	**637,76**	**637,76**
	CONSUMO DEL SISTEMA DE COMUNICACIONES		**13.440,00**	**13.440,00**	**13.440,00**	**13.440,00**	**13.440,00**
	OTROS GASTOS CRAT		**380,00**	**380,00**	**380,00**	**380,00**	**380,00**
	SEGUROS						
	PRIMA SEGURO CONTRA SABOTAJE (Subestación Eléctrica)		71.087,00	71.087,00	71.087,00	71.087,00	71.087,00
	SUB TOTAL SEGUROS		**71.087,00**	**71.087,00**	**71.087,00**	**71.087,00**	**71.087,00**
TOTAL		**3.770.680,00**	**630.444,96**	**630.444,96**	**630.444,96**	**630.444,96**	**-292.455,04**
VALOR PRESENTE NETO		**4.717.552,06**					

Fuente : Elaboración Propia

Tabla 7.2 Flujo Económico del Sistema de Seguridad Tradicional US $

CONCEPTO		PERIODOS ANUALES					
		0	1	2	3	4	5
NÚMERO DE INSTALACIONES		200					
INVERSIÓN	CENTRAL DE CONTROL (CC)						
	Acondicionamiento CC	1.240,00					
	Instalación acondicionamiento CC	1.390,00					
	Equipos informáticos CC	1.000,00					
	Instalación eléctrica CC	1.000,00					
	Comunicaciones CC	400,00					
	INSTALACIONES REMOTAS DE USO TELEFÓNICO (IRUT)						
	Protección física IRUT	460.000,00					
	Instalación protección IRUT	310.000,00					
	Comunicaciones IRUT	40.000,00					
	OTRAS INVERSIONES						
	Camionetas Servicio de Vigilancia Móvil	20.000,00					
	TOTAL INVERSIÓN	**835.030,00**					
GASTOS	SERVICIO DE VIGILANCIA HUMANA (SVH)						
	Vigilancia fija IRUT		2.096.640,00	2.096.640,00	2.096.640,00	2.096.640,00	2.096.640,00
	Operadores CC		12.230,40	12.230,40	12.230,40	12.230,40	12.230,40
	Inspectores IRUT		28.800,00	28.800,00	28.800,00	28.800,00	28.800,00
	SUB TOTAL SVH		**2.137.670,40**	**2.137.670,40**	**2.137.670,40**	**2.137.670,40**	**2.137.670,40**
	MANTENIMIENTO						
	Mantenimiento de la CC		107,20	107,20	107,20	107,20	107,20
	Mantenimiento de la IRUT		27.100,00	27.100,00	27.100,00	27.100,00	27.100,00
	Mantenimiento otras inversiones (vehículos)		1.000,00	1.000,00	1.000,00	1.000,00	1.000,00
	SUB TOTAL MANTENIMIENTO		**28.207,20**	**28.207,20**	**28.207,20**	**28.207,20**	**28.207,20**
	VALOR DE SALVAMENTO						
	Valor de salvamento de la CC						-620,00
	Valor de salvamento de la IRUT						-300.000,00
	Valor de salvamento de otras inversiones (vehículos)						-10.000,00
	SUB TOTAL VALOR DE SALVAMENTO		**0,00**	**0,00**	**0,00**	**0,00**	**-300.620,00**
	CONSUMO ELÉCTRICO CC		**264,26**	**264,26**	**264,26**	**264,26**	**264,26**
	CONSUMO DEL SISTEMA DE COMUNICACIONES		**61.320,00**	**61.320,00**	**61.320,00**	**61.320,00**	**61.320,00**
	OTROS GASTOS						
	Combustible (vehículos)		7.200,00	7.200,00	7.200,00	7.200,00	7.200,00
	Gastos de oficina		260,00	260,00	260,00	260,00	260,00
	SUB TOTAL OTROS GASTOS		**7.460,00**	**7.460,00**	**7.460,00**	**7.460,00**	**7.460,00**
	SEGUROS						
	PRIMA SEGURO CONTRA SABOTAJE (Subestación Eléctrica)		142.174,00	142.174,00	142.174,00	142.174,00	142.174,00
	SUB TOTAL SEGUROS		**142.174,00**	**142.174,00**	**142.174,00**	**142.174,00**	**142.174,00**
	TOTAL	**835.030,00**	**2.377.095,86**	**2.377.095,86**	**2.377.095,86**	**2.377.095,86**	**2.076.475,86**
VALOR PRESENTE NETO		**7.525.185,00**					

Fuente : Elaboración Propia

Tabla 7.3 Determinación del Valor Presente y de la Tasa Interna de Retorno del Flujo Económico del Ahorro entre el Sistema de Seguridad Propuesto y el Tradicional

DESCRIPCIÓN	PERIODOS ANUALES					
	0	1	2	3	4	5
Sistema de Seguridad Tradicional	835.030,00	2.377.095,86	2.377.095,86	2.377.095,86	2.377.095,86	2.076.475,86
Sistema de Seguridad Propuesto	3.770.680,00	630.444,96	630.444,96	630.444,96	630.444,96	- 292.455,04
Flujo económico del Ahorro	-2.935.650,00	1.746.650,91	1.746.650,91	1.746.650,91	1.746.650,91	2.368.930,91
Costo de Oportunidad del Capital (COK)	15,00%					
Valor Presente Neto (VPN)	2.092.861,87	**VPN > 0**				
Tasa Interna Retorno (TIR)	53,94%	**TIR > COK**				

Fuente : Elaboración Propia

CAPÍTULO VIII

ANÁLISIS BENEFICIO COSTO

La manifestación de cualquier riesgo, siempre implica el resultado de una pérdida, por pequeña que sea; por lo tanto reduce las utilidades. Se deben analizar los riesgos según su posible impacto sobre los activos y/o procesos normales de producción, de tal manera que se realicen las acciones en contra, las cuales deben ser efectivas en costos.

8.1 CUANTIFICACIÓN MONETARIA DE LAS PÉRDIDAS

Se cuantificaron las consecuencias en términos monetarios para permitir la evaluación de las contra medidas de seguridad efectivas en costo, es decir, si el costo de implementar el Sistema Integral Inteligente de Seguridad no es superior al beneficio o al valor de las perdidas.

Se pudo cuantificar fácilmente la pérdida inmediata, ya que se mantenían registros de dichas pérdidas debido a que los eventos dentro de la empresa siempre se informan cuando sucede una pérdida.

Se puede definir el termino "total del costo de perdida" como el valor de la pérdida si todo lo que se podría perder o destruir ha sido calculado, pero modificado por un grado de practicabilidad, por esto queremos decir, la esperanza razonable de la pérdida total.

El cálculo total del costo de la pérdida puede ser establecido como

$$K = (Cp + Ct + Cr + Cd) - (I - Ci)$$

Donde:

K = Es el total del costo de la pérdida

Cp = Es el costo de reemplazo permanente

Ct = Es el costo de sustitución temporal

Cr = Es el costo total de pérdidas relacionadas

Cd = Es el costo de pérdidas en inversiones que generan ingresos

I = Es la cantidad de seguros (indemnizaciones)

Ci = Es el costo proporcional compartido del seguro (deducible)

El costo de Reemplazo Permanente es el costo de reemplazar los bienes siniestrados más el costo de instalarlos.

El costo de Sustitución Temporal, es el costo de contratar un bien o equipo hasta que el original esté en condiciones normales de operación.

El costo de Pérdidas Relacionadas es el costo adicional que involucra, por ejemplo, remover los escombros o mantener vigilancia humana adicional luego del siniestro.

El costo de Pérdidas en Inversiones que Generan Ingresos se refiere a las pérdidas por los daños a los bienes que paralizan la operación normal de la instalación o parte de ellas de tal forma que se deja de percibir un ingreso y por lo tanto no se genera un lucro. Es por esto, que a ésta pérdida se le conoce más como Lucro Cesante.

Las Indemnizaciones, representa el valor de la cada indemnización recibida de una empresa aseguradora, por sufrir un siniestro que cubre toda o parte de la pérdida.

El Deducible, es la cantidad monetaria que se debe desembolsar cuando se efectúa una indemnización y de acuerdo a condiciones particulares contenidas en las pólizas contra siniestros contratadas.

Para calcular el valor del Reemplazo Permanente se consideró el valor del bien, para lo cual se tomó el valor de compra inicial y el valor de la instalación o montaje como un porcentaje de este valor, igual al 10%.

Para el Costo de Sustitución Temporal se tomaron en cuenta sólo los bienes que pueden ser sustituidos temporalmente en un lapso razonable por el tiempo que dure conseguir el reemplazo permanente o reparación de los bienes siniestrados; para ello se consideró un 5% del valor del bien.

Para calcular el Costo de Pérdidas Relacionadas (pagos por servicios de terceros) se tomó en cuenta lo que costaría pagar a un vigilante durante el tiempo que dure la puesta en marcha normal de la Instalación Remota de Uso Telefónico siniestrada, así como los gastos generados por la remoción y limpieza de ésta.

Para el caso del Lucro Cesante se hizo el cálculo suponiendo que la instalación dejará de operar un lapso de 15 días, debido a la manifestación de un riesgo.

A continuación mostramos las tablas de cálculo de los diferentes costos descritos anteriormente, las cuales nos servirán más adelante para determinar cuál es el valor del ratio Beneficio / Costo.

Tabla 8.1 Costo de Reemplazo Permanente (Inversión Fija: Valor del Bien)
(US $)

Ambientes	Equipos	Valor
Ambiente A	Baterías	20.000,00
	Rectificador	30.000,00
	Distribuidor	10.000,00
Ambiente B	Conmutador	80.000,00
	Transmisor	100.000,00
	Aire Acondicionado	5.000,00
Sala Grupo Electrógeno	Grupo Electrógeno	200.000,00
	Tablero General	2.500,00
Sala Subestación Eléctrica	Transformador	50.000,00
Patio	Tanque de Combustible	2.500,00
Total Inversión Fija		500.000,00

Fuente : Elaboración Propia

Tabla 8.2 Costo de Reemplazo Permanente (Inversión Intangible: Instalación o Montaje)
(US $)

Ambientes	Equipos	Valor
Ambiente A	Baterías	2.000,00
	Rectificador	3.000,00
	Distribuidor	1.000,00
Ambiente B	Conmutador	8.000,00
	Transmisor	10.000,00
	Aire Acondicionado	500,00
Sala Grupo Electrógeno	Grupo Electrógeno	20.000,00
	Tablero General	250,00
Sala Subestación Eléctrica	Transformador	5.000,00
Patio	Tanque de Combustible	250,00
Total Inversión Intangible		50.000,00

Fuente : Elaboración Propia

Tabla 8.3 Costo de Sustitución Temporal
(US $)

Ambientes	Equipos	Valor
Ambiente A	Baterías	1.000,00
	Rectificador	
	Distribuidor	
Ambiente B	Conmutador	
	Transmisor	
	Aire Acondicionado	250,00
Sala Grupo Electrógeno	Grupo Electrógeno	10.000,00
	Tablero General	
Sala Subestación Eléctrica	Transformador	
Patio	Tanque de Combustible	0,00
Total Inversión Intangible		11.250,00

Fuente : Elaboración Propia

Tabla 8.4 Costo de Pérdidas Relacionadas (Pagos por Servicios)
(US $)

Concepto	Valor
Remoción y Limpieza	5.000,00
Vigilancia Humana	500,00
Total Servicios	5.500,00

Fuente : Elaboración Propia

Tabla 8.5 Costo de Pérdidas en Inversiones que Generan Ingresos (Lucro Cesante)

Ingreso por Línea Telefónica de Abonado	1,667	Dólares / día
Número Líneas por IRUT	2.000	Líneas telefónicas
Tiempo Sin Servicio por Siniestro	15	días
Lucro Cesante Por IRUT	50.000	Dólares americanos

Fuente : Elaboración Propia

8.2 COSTO DEL SISTEMA DE SEGURIDAD

La justificación del costo para un sistema de seguridad radica en el hecho de que el costo de protección es substancialmente menor que la pérdida incurrida sin la protección en Instalaciones Remotas de Uso Telefónico, pues según se puede observar de la tabla 8.1, la inversión en activos fijos asciende a U.S. $ 500.000 por Instalación Remota Uso Telefónico; lo cual significa que el activo fijo de 200 Instalaciones Remotas de Uso Telefónico está valorizado en U.S. $ 100.000.000 y de la tabla 7.1 podemos obtener que el valor presente de la inversión en instalación y mantenimiento del Sistema Integral inteligente de Seguridad es U.S $ 4.717.552 en un horizonte de 5 años (tiempo del estudio), es decir el costo del sistema de seguridad propuesto representa tan sólo el 4,71% del activo protegido.

El valor del costo de seguridad está dado por los montos de inversión y gastos de operación y mantenimiento que involucra el sistema de protección, los cuales se expresan a través de los medios de servicio de vigilancia humana, medidas de seguridad electrónica, medidas de seguridad física y medidas económicas.

8.3 RATIO BENEFICIO / COSTO

Esta es la proporción entre el probable costo de las pérdidas que pueden ocurrir sin contar con un sistema de seguridad y el costo real de establecer y mantener este sistema. Por ello el ratio debe ser mayor que 1, de tal manera que muestre que el beneficio de invertir en un sistema de seguridad y su mantenimiento es mayor al costo de esta inversión, dicho de otra forma esto significa que, un sistema de seguridad económicamente factible debe ser uno tal que, su costo de instalación y mantenimiento sea menor en comparación con las posibles pérdidas.

Tabla 8.6 Cálculo del Ratio Beneficio / Costo
US $

	Concepto	Valor
Pérdidas Potenciales	Costo de Reemplazo Permanente (Inversión Fija: Valor del Bien)	500.000,00
	Costo de Reemplazo (Inversión Intangible: Instalación o Montaje)	50.000,00
	Costo de Sustitución Temporal	11.250,00
	Costo de Pérdidas Relacionadas: Pagos por Servicios de Terceros	5.500,00
	Costo de Pérdidas en Inversiones que Generan Ingresos (Lucro Cesante)	50.000,00
	Deducible	18.150,00
	Indemnización	36.850,00
	Costo de la Pérdida por IRUT	598.050,00
	Número de Instalaciones Protegidas	200
	Total Perdida Anual	**119.610.000,00**
Sistema de Seguridad Propuesto	Valor Presente Neto	4.617.754,03
	Tiempo (Años)	5
	Valor Presente Neto Anual	**923.550,81**
Ratio Beneficio / Costo del Sistema Propuesto:		**129,51**
Sistema de Seguridad Tradicional	Valor Presente Neto del Sistema Tradicional	7.325.588,94
	Tiempo (Años)	5
	Valor Presente Neto Anual	**1.465.117,79**
Ratio Beneficio / Costo Sistema Tradicional:		**81,63**

Fuente : Elaboración Propia

CAPÍTULO IX

ANÁLISIS COMPARATIVO

9.1 SISTEMA DE SEGURIDAD TRADICIONAL

Como sabemos el Sistema de Seguridad Tradicional consiste en la protección de instalaciones únicamente a través del servicio de vigilancia humana fija que para cumplir cabalmente sus funciones deberán cumplir con las características de comportamiento mencionadas en el apéndice E (responsabilidad, lealtad, identificación, etc.), pero muchas veces estos comportamientos de ética, son desviados debido a ciertos factores que pueden reducir la eficiencia del ser humano (factores fisiológicos, psicológicos, sociológicos, etc.) como se detalla en el anexo 03 (distorsión de factores humanos que disminuyen la eficiencia del servicio de vigilancia fija).

Líneas abajo citamos algunos ejemplos que nos demuestran las desventajas de tener un Sistema de Seguridad Tradicional y no contar en nuestras instalaciones con el Sistema Inteligente Integral de Seguridad con todos las medidas que existen en el campo de la seguridad.

9.1.1 DESVENTAJAS DEL SISTEMA DE SEGURIDAD TRADICIONAL

Procedemos a detallar algunas de las desventajas más importantes en contar con un Sistema de Protección basado únicamente en el Servicio de Vigilancia Humana Fija.

9.1.1.1 NO ES CONFIABLE

- Efectuar actividades ajenas al trabajo, dentro de la instalación.
- Falsear información sobre su trabajo, datos personales o de cualquier naturaleza a favor o en contra de otros trabajadores.
- Retrasarse a la hora de entrada al trabajo.
- Penetrar en ambientes restringidos sólo a personal autorizado.
- Ejecutar actos que puedan afectar los intereses de la Empresa.
- Sacar bienes sin la debida autorización.
- Faltar injustificadamente a sus labores
- Ausentarse sin permiso del área de trabajo.
- Causar intencionalmente o por descuido perjuicios a los bienes de la Empresa.
- Cometer dentro de las horas de trabajo actos contrarios a la disciplina.
- Hacer uso indebido o exagerado del sistema de teléfonos para asuntos particulares.
- Acostumbrarse a que no existan alarmas y no atenderlas de inmediato.

9.1.1.2 DETECCIÓN TARDÍA

- No identificar inmediatamente la amenaza.
- Puede detectar presencia de intrusos cuando ya han efectuado daño.

9.1.1.3 NO TIENE COBERTURA TOTAL

- Permanece en su puesto de trabajo dejando áreas desprotegidas
- En su inspección no revisa totalmente las áreas
- No es especialista en los equipos para detectar anomalías inmediatamente
- No puede estar en todos los ambientes al mismo tiempo

9.1.1.4 NO ES INTEGRADO

- No hay interconexión entre los elementos de defensa.
- Demoras en los planes ya que el vigilante será el que detecte, el que avise y el que accione.
- El Servicio de Vigilancia Humana no está capacitado para detectar problemas tan comunes como desperfectos en los sensores de incendio por presencia de polvo, o descarga de baterías en equipos de detección en el caso de que éstos no estén conectados con la Central de Control.

9.1.1.5 LIMITACIONES LEGALES

- Debemos observar que por ley a los agentes de seguridad privada no se les permite portar armas a menos que cuenten con un permiso especial de la DISCAMEC. Incluso si se les entrega este permiso, no se les permite usar sus armas de fuego en propiedad pública. En otras palabras, el arma sólo puede ser usada con medida disuasiva más no como medida de detención o eliminación del riesgo, en el caso de intrusión (robo o sabotaje).
- Adicionalmente a esto debemos mencionar que la situación actual del país ha determinado que muchas empresas de vigilancia particular con el fin de reducir costos operativos, opten por contratar personal no cualificado para el puesto de vigilante.

9.1.2 VENTAJAS DEL SISTEMA DE SEGURIDAD TRADICIONAL

9.1.2.1 CONTROL TEMPRANO

- Actúa inmediatamente controlando la ocurrencia de una amenaza, siempre y cuando la detecte y además no tenga dificultades frente a la dimensión de una amenaza mayor.

9.2 SISTEMA DE SEGURIDAD PROPUESTO (SIIS)

9.2.1 VENTAJAS

9.2.1.1 ES CONFIABLE

- Esta conformado por un conjunto de operaciones que obedecen a rutinas y procedimientos de decisión de acción previamente programados.
- No se distrae ni está sujeto a fatiga y opera en vigilancia permanente las 24 horas del día.
- Un grupo reducido de personas controlan varias instalaciones a la vez (lo que representa un menor costo y una mayor productividad) teniendo comunicación con grupos de reacción. Por esta razón se puede considerar al sistema como Integral, pues integra un conjunto de medidas de seguridad humanas, electrónicas, físicas y económicas con procedimientos de apoyo o ayuda en casos que lo ameriten.
- Controla estrictamente el ingreso a zonas restringidas mediante el uso de tarjetas de banda magnética y claves personales.
- Permite el chequeo directo de quienes ingresan al local por parte de los operadores de la Central de Control a través del circuito de televisión, de tal forma que se pueda establecer quien o quienes se encuentran en determinado ambiente y en determinado momento.

9.2.1.2 DETECCIÓN TEMPRANA

- Los sistemas electrónicos estarán permanentemente supervisando los ambientes.

9.2.1.3 COBERTURA TOTAL

- Las alarmas podrán mostrarse en tiempo real en la CRAT a través de un

sistema de plano digital y verificarse, con el fin de dar instrucciones al grupo de reacción.

9.2.1.4 SIMPLIFICACIÓN DE LAS TOMAS DE DECISIONES

- Es inteligente porque tiene programados algunas acciones de respuestas frente a la presencia de determinadas amenazas. Esta facultad de toma de decisiones hace que este sea un sistema Inteligente, en un grado básico por supuesto.
- A través de las cámaras de televisión se puede capturar el momento de inicio del fuego, las que automáticamente se direccionaran hacia esta presencia de fuego, debido a los sensores de humo. Esta utilidad permite activar el sistema automático de extinción y dar al grupo de apoyo (bomberos) información para atacar el foco del incendio de inmediato y además dichas imágenes será útil en las investigaciones posteriores.

9.2.1.5 DISMINUCIÓN EN COSTOS

- La manera centralizada puede verificar el estado de cada elemento o equipo electrónico que lo conforma automáticamente, de tal manera que no sea necesario el desplazamiento de personal de mantenimiento hasta la IRUT. De esta manera también indica cuando es necesario el mantenimiento correctivo y a que equipo.
- Las compañías de seguros disminuyen los costos de las primas de seguros al reemplazar el sistema de seguridad únicamente con agentes de vigilancia por complementar con sistemas de seguridad electrónicos por ser estos últimos de más confianza

9.2.1.6 ES INTEGRADO

- Posee en un sola infraestructura, medidas de seguridad físicas y

electrónicas contra incendio, robo y/o sabotaje y es controlado por un sólo equipo de operadores en la CRAT, los cuales interaccionan apoyándose mutuamente para una detección y reacción más temprana.

- Permite hacer las coordinaciones en el menor tiempo posible con los elementos de apoyo externos e internos.

9.2.1.7 DISMINUCIÓN EN PROBABILIDADES / TAMAÑO DE PÉRDIDAS

Al realizar el reemplazo del Sistema de Seguridad Tradicional con el Sistema de Seguridad Propuesto aumentamos la eficiencia de la protección a la instalación, por lo tanto la vulnerabilidad con este nuevos sistema es menor.

9.2.1.8 MEJORAMIENTO DE LAS RELACIONES PÚBLICAS

En instalaciones con medidas de seguridad técnicas, hace que el cliente se sienta más cómodo y seguro, se siente protegido en forma permanente, él y sus propiedades. Muchas veces los agentes de vigilancia no son muy corteses con los clientes.

9.2.1.9 MEJORAMIENTO DE RELACIONES INDUSTRIALES

El trabajador es consiente que la empresa le proporciona un lugar de trabajo con la implantación de Sistemas de Seguridad Modernos que lo protegen de cualquier atentado externo o siniestros que puedan afectar su vida.

9.2.1.10 MEJORAMIENTO DE LA PRODUCTIVIDAD

A través de este Sistema de Seguridad propuesto se disminuye e incluso se elimina las demoras en las producción provocados por siniestros.

CAPÍTULO X

CONCLUSIONES Y RECOMENDACIONES

10.1 CONCLUSIONES

10.1.1 Se consiguieron los objetivos generales de la presente tesis, pues:

- Se demostró que el sistema de seguridad propuesto (SIIS) reduce notablemente los costos de operación al comparar los valores presentes de la inversión y gastos en 5 años de cada uno de los sistemas de seguridad, a través del criterio de ahorro, el cual muestra el efecto de usar la alternativa propuesta en lugar de la tradicional (Capítulo VII: Evaluación Económica) .

- Se demostró que el SIIS eleva la calidad del sistema de seguridad en la IRUT a través del uso de tecnología, la que permite la obtención de ventajas comparativas notables con respecto al sistema tradicional. (Capítulo IX : Análisis Comparativo)

10.1.2 Con el SIIS se podrá elevar notablemente la calidad de la protección en las IRUT, debido a que combina una serie de medidas de seguridad según el análisis y evaluación de riesgos de cada ambiente y la repercusión de uno sobre otros, además como se

10.1.3 detalla en el Anexo 03, la eficiencia del ser humano en el aspecto de seguridad puede verse disminuida por la distorsión de los factores fisiológicos, psicológicos o sociológicos, o no al alcanzar los niveles de detección que conseguiríamos con los sistemas electrónicos. Por ejemplo, en el caso de incendio la detección del agente de vigilancia es más tardía que los sistemas de protección electrónica.

10.1.4 El análisis y evaluación de riesgos que exponemos presenta una metodología a través del esquema de puntos, por lo cual es sencilla su aplicación, pero es necesario que se tenga un conocimiento empírico o profundo de la instalación que se intenta proteger. Además podemos concluir que esta metodología no es solamente aplicable para casos de instalaciones remotas de uso telefónico, sino que también puede aplicarse a cualquier tipo de empresa que por su naturaleza de operaciones tenga diseminados locales o instalaciones alejadas geográficamente.

10.1.5 Se puede concluir que el ser humano como medida de seguridad debe pertenecer al sistema de seguridad como un elemento de este y no como una alternativa excluyente.

10.1.6 Es factible diseñar un sistema de seguridad que cubra todos los riesgos debido a que existen medidas de seguridad técnicas (físicas, electrónicas, económicas) y humanas que combinadas cubran todo tipo de riesgo. Inclusive si el riesgo es imposible de evitar se puede optar por una medida totalmente económica: el Seguro, y a consecuencia de implementar medidas de seguridad más eficientes se reduciría la vulnerabilidad, teniendo un efecto económico positivo en la reducción de primas.

10.1.7 Al llevar a cabo el trabajo de la tesis, hemos podido observar que de acuerdo a la concepción adoptada del SIIS con las medidas de seguridad tomadas se pueden evitar la manifestación de riesgos, ya que las medidas de seguridad de demora generarían un tiempo mayor al tiempo de detección y reacción. Más aún podrían impedir el intento a través de los medios de disuasión utilizando elementos físicos electrónicos y humanos.

10.1.8 Al revisar los resultados obtenidos por la proyección del Flujo Económico del Ahorro resultado de la comparación entre el sistema de seguridad propuesto y el tradicional, vemos que se consigue un Valor Presente del Ahorro mayor a cero **(VP = $ 2.007.865,45 > 0)** y una Tasa Interna de Retorno del ahorro mayor que el Costo de oportunidad del Capital **(TIR = 53,94% > COK = 15 %).** Esto significa que el ahorro que se obtendría por implementar el SIIS en lugar de optar por el Sistema de Seguridad Tradicional (basado únicamente en vigilantes) nos reportaría US$2.007.865,45 a valores actuales, resultantes de un período de análisis de 5 años y el rendimiento de este ahorro sería 3.5 veces mayor que el COK, es decir nos resultaría 3.5 veces más beneficioso.

10.1.9 Al invertir en un sistema de seguridad, considerado muchas veces un gasto necesario, disminuimos la vulnerabilidad ya que a medida que complementamos medidas de seguridad estamos reduciendo la probabilidad de que se produzca daño, lo que representa para una empresa de telecomunicaciones, en la cual está basada esta tesis, una importante salvaguarda pues debido a sus grandes ingresos diarios y al gran activo que posee en importancia y costo, un siniestro que afecten estos bienes e interrumpan sus operaciones diarias representaría costos elevados de reemplazo, lucro cesante, deducibles y demás gastos relacionados, los que se pueden

observar en el capítulo VIII (Análisis Beneficio Costo).

10.2 RECOMENDACIONES

10.2.1 Este trabajo de tesis no debe ser tomado como un texto de prevención de amenazas, pues como se citó en el capítulo V (Análisis Técnico del Sistema de Seguridad) se pueden reducir los daños (con la disminución de la vulnerabilidad) a través de la implantación de medidas de seguridad eficientes. En esto radica la diferencia entre un análisis técnico científico del tema de seguridad y un simple conocimiento intuitivo.

10.2.2 El Capítulo VII (Evaluación Económica) puede ser utilizado como referencia para proyectos que originen disminución de costos, que se produzca de la elección de dos alternativas de inversión excluyentes entre si, debido a que utiliza el criterio de análisis de ahorro como una nueva alternativa, la que es combinación de las dos primeras.

10.2.3 Para un correcto análisis de riesgos, en cuanto a la identificación de los riesgos se recomienda que éstas sean hechas por técnicos relacionados al bien en protección y para el análisis de riesgos, en cuanto a su cuantificación, se recomienda apoyarse en registros históricos de sucesos relacionados. Para acumular un registro de pérdidas sufridas por siniestros, cada Empresa debe tener una política de registro de estas pérdidas. De tal forma que esta política requiera que todas las pérdidas reportadas se hagan en una forma estandarizada, normalmente en un formato especial. Entre la información que debe ser reportada están:

- La descripción del activo
- La fecha y hora de la pérdida o el intervalo durante el cual ocurrió

- El valor del activo y el medio para valorizarlo (libro de depreciación, reemplazo comercial, factura, etc.)
- Las circunstancias de la pérdida (cómo ocurrió).

10.2.4 Como se ha podido observar, utilizar tecnología en el campo de seguridad no sólo aumenta el grado de certidumbre sino que reduce también los gastos, considerablemente, en empresas con instalaciones alejadas entre sí. Por esto recomendamos seguir todos los pasos de la metodología aquí descrita de tal manera de mejorar la performance, reducir costos y tener certeza de contar con el sistema de seguridad requerido, de acuerdo a los riesgos.

10.2.5 No es suficiente hacer el análisis beneficio costo únicamente, pues en empresas con activos tan costosos como es el caso de empresas de telecomunicaciones siempre resultaran grandes los ratios beneficio / costo. Por ello se recomienda tomar este dato sólo para efectos comparativos con otras propuestas, pues solo no tiene mayor información que la obvia sobre el impacto económico de una alternativa de inversión en seguridad.

10.2.6 En esta tesis se han dado tres niveles para cada factor en el análisis de riesgo (Grande, Mediano y Bajo), sin embargo se pueden aumentar estos niveles a 4 ó 5, teniendo como base el criterio meticuloso de cada empresa. Se debe tener en cuenta que a mayor niveles para los factores se obtendrán también mayores rangos en el tipo de Severidad del Riesgo y Probabilidad del Riesgo, con lo cual la Matriz de Decisiones tendrá más filas y más columnas, lo que podría, a la larga, generar más confusión que ayuda. Por ello recomendamos utilizar niveles de 3 ó 4 y en un caso de necesaria exactitud, niveles de 5 para cada factor. Se debe tener en cuenta, que sin excepción, cada factor debe tener el mismo

número de niveles.

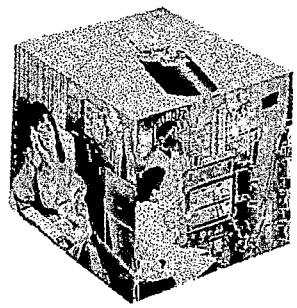
10.2.7 Al diseñar un sistema de seguridad, se recomienda siempre tener presente las denominadas 4 D's de la seguridad : Demorar, Detectar, Disuadir y Detener. De tal forma que se utilicen las medidas necesarias y correctas. Observar que el hecho de usar medidas más elaboradas para un ambiente puede generar redundancia de seguridad para otro ambiente conexo, sin embargo esta redundancia se pude considerar pasiva pues si no existiera el ambiente conexo, de igual manera se tendría que contar con las medidas más elaboradas.

10.2.8 A fin de diseñar medidas de seguridad adecuadas a los riesgos es necesario realizar un análisis y evaluación de riesgos a fin de adoptar políticas más confiables y rentables y no sólo implantar medidas de seguridad en forma apresurada sin ninguna lógica.

APÉNDICE A

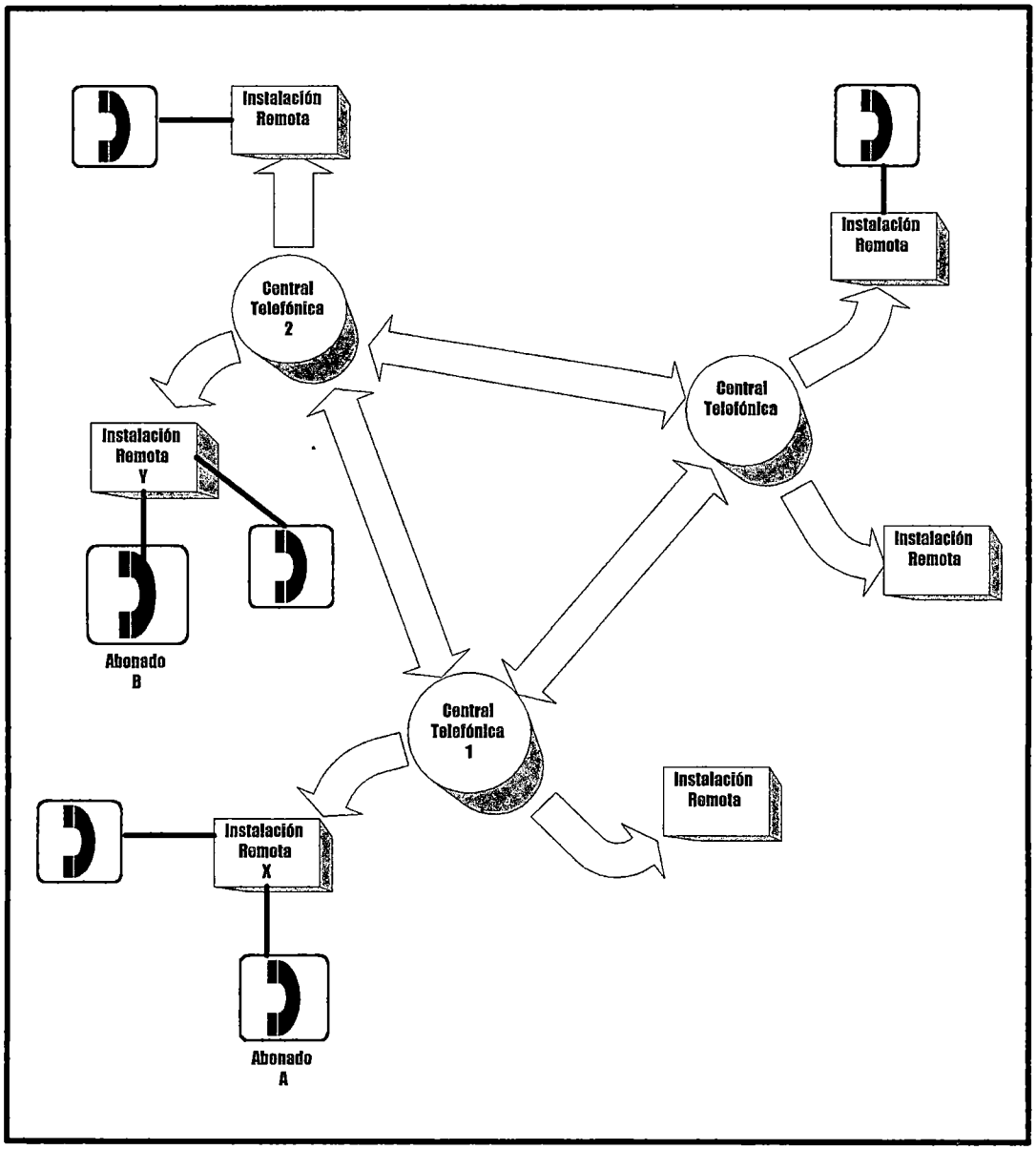
RED TELEFÓNICA

La Red Telefónica es la que utilizamos para la comunicación a distancia entre dos abonados.



En una manera básica la podemos representar como se muestra en el gráfico A1. Para la comunicación del abonado A con el abonado B, se presenta la siguiente secuencia, el abonado marca el número del abonado B, esta información la recibe la Instalación Remota de Uso Telefónico X, y esta la comunica a la Central Telefónica Cabecera 1, la cual se comunica con la Central Telefónica Cabecera 2 y la Central Telefónica Cabecera 2 envía la información a la Instalación Remota de Uso Telefónico Y quien establece la comunicación con el abonado B, si éste no esta ocupado.

Gráfico A.2 Esquema de la Red Telefónica



De acuerdo a las funciones operativas, la red telefónica se puede diferenciar en Planta Interna y Planta Externa, los componentes de ambas plantas son:

A.1 PLANTA EXTERNA

Se denomina así al conjunto de construcciones, instalaciones y equipos que se ubican fuera de los Edificios de Uso Telefónico. Forma el

conjunto de elementos e instalaciones que sirven de vinculo entre el abonado y su correspondiente central, como así también el vinculo entre dos centrales.

En general, la Planta Externa está constituida por:

- Medios conductores: Cables telefónicos
- Medios de interconexión: Armarios, cajas de dispersión
- Medios de soporte: Postes
- Medios de protección: Cámaras y canalizaciones subterráneas
- Medio de conexión: Galería de cables

A.1.1 CABLES TELEFÓNICOS

Se denomina a aquellos elementos de la planta externa que, constituidos por un número variable de conductores metálicos o de fibras de vidrio, posibilitan la transmisión de señales bien eléctricas u ópticas con el fin de enlazar entre si a cada uno de los abonados con la Central Telefónica o Instalación Remota de Uso Telefónico a que pertenece y entre Centrales Telefónicas. En el primer caso se habla de Redes de Abonado y en el segundo de Redes de Enlace.

En la red de cables se puede distinguir tres partes que son:

- **Red Primaria**, une el Distribuidor Principal de la Central Telefónica con el Armario a través de cables primarios que generalmente se instalan en canalizaciones o directamente enterrados.

- **Red secundaria**, une el Armario con las Cajas de Dispersión a través de cables secundarios generalmente instalados sobre Postes.
- **Red de abonados**, este cable se divide en dos secciones, la acometida

externa que va expuesta a la intemperie en forma aérea y la acometida interna que va dentro del inmueble del abonado sobre paredes o en ductos.

A.1.2 ARMARIOS

Es el punto donde llegan los cables de la red primaria que vienen desde el Distribuidor Principal y que sirve, también, como punto de salida de los cables de la red secundaria.

A.1.3 CAJAS DE DISPERSIÓN

Son el último punto de la red de cables a partir del cual se distribuyen los pares que van a los domicilios de los abonados.

A.1.4 CÁMARAS

Son estructuras de concreto en las que se alojan los cables y empalmes primarios y secundarios y para realizar bifurcaciones de las canalizaciones.

A.1.5 CANALIZACIONES SUBTERRÁNEAS

Los sistemas de canalización aseguran, la flexibilidad de las redes subterráneas, y la protección de los cables contra daños de origen mecánico y contra la corrosión.

A.1.6 POSTES

En la actualidad se utilizan como soportes de las líneas o cables aéreos.

A.1.7 GALERÍA DE CABLES

En ella se realizan los empalmes de los cables de planta externa con los cables que ingresan al Distribuidor Principal en la planta interna.

A.2 PLANTA INTERNA

Se denomina así, al conjunto de equipos e instalaciones que se ubican dentro de los Edificios de Uso Telefónico, la cual puede ser Central Telefónica Cabecera o Instalación Remota de Uso Telefónico.

Debido a la gran cantidad de clientes y a las distancias entre ellos, no es posible que cada servicio telefónico se a conectado a una misma Central Telefónica Cabecera, por esta razón se instalan una serie de Instalaciones Remotas de Uso Telefónico en diferentes localidades, los cuales están interconectados entre sí formando una Red Telefónica, mediante la cual todo abonado tiene acceso a cualquier otro abonado.

- **Central Telefónica Cabecera;** Centro de conmutación al que están conectadas las Instalaciones Remotas de Uso Telefónico y a través del cual se establecen los enlaces entre centrales. Es el encargado de realizar las pruebas de los circuitos telefónicos, la tarifación de llamadas, la comunicación de abonados conectados a una misma central o a diferentes centrales a través de la interconexión con otras centrales.

- **Instalación Remota de Uso Telefónico;** Es una extensión de la Central Cabecera que realiza únicamente la función de comunicación. Se implementa para establecer la comunicación de abonados que se encuentran aglomerados en una misma zona geográfica pero al mismo tiempo alejados de la Central Cabecera. Se enlaza con la Central Cabecera con cable multipar o fibra óptica, minimizando la inversión en

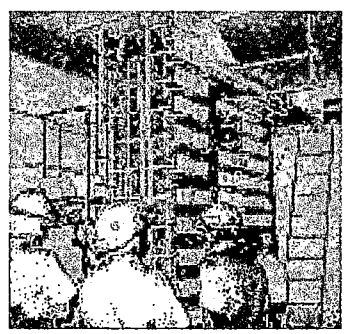
obras de canalización, tendido y conexionado de Red Telefónica.

La Planta Interna está conformada por:

A.2.1 DISTRIBUIDOR PRINCIPAL

Es el elemento físico ubicado en la Central Telefónica, que permite el enlace entre la planta externa y la planta interna.

Gráfico A.3 Distribuidor Principal



A.2.2 CONMUTADOR

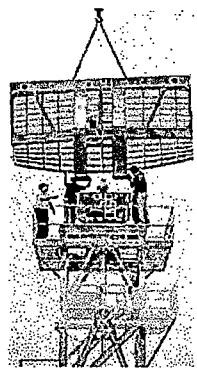
Equipo que permite el establecimiento de los "Caminos de Conversación" entre abonados. Por conmutación se entiende todos aquellos elementos de concentración, procesamiento y expansión del tráfico telefónico.

Gráfico A.4 Conmutador

A.2.3 TRANSMISOR

Es el equipo que genera señales que permitirá llevar comunicaciones que están fuera del rango de la voz humana (300 a 3400 Hz). Los medios de transmisión pueden ser por medios físicos (par metálico, cable coaxial, fibra óptica) o medios de transmisión inalámbricos (sistema de radio, microondas, sistemas de satélites, telefonía celular).

Gráfico A.5 Transmisor inalámbrico



A.2.4 SISTEMAS DE ENERGÍA

Contiene equipos que proveen de energía eléctrica suficiente para el funcionamiento de los equipos de conmutación, de transmisión y alimentan toda la planta telefónica.

La carga se efectúa con corriente alterna de 220 voltios y alimentan la planta con 48 voltios de corriente continua.

El sistema de energía esta conformado por:

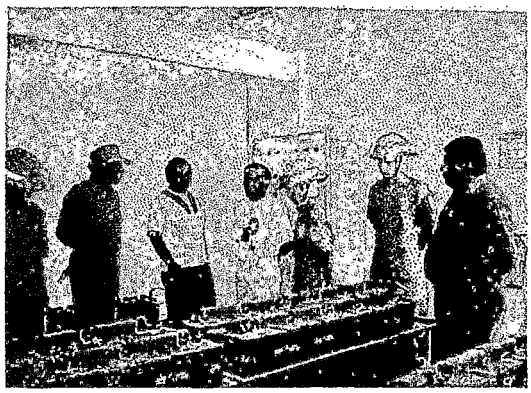
- Baterías
- Rectificador
- Grupo electrógeno

- Tanque de combustible
- Transformador

A.2.4.1 BATERÍAS

Esta conformado por una banco de baterías, las cuales suministran energía ininterrumpidamente alimentando con 48 Voltios de CC.

Gráfico A.6 Sala de Baterías



A.2.4.2 RECTIFICADOR

La característica básica de estos rectificadores viene dada por su alimentación mediante corriente alterna 220 V y su salida en corriente continua de 48 V.

A.2.4.3 GRUPO ELECTRÓGENO

El grupo electrógeno fijo es necesario como un medio de suministro de energía secundaria para suplir el suministro de corriente alterna. La potencia necesaria a obtener de los grupos electrógenos es aquella que garantiza el equipo de telecomunicaciones, el equipo de climatización y un 30% más para atender otras necesidades de la central.

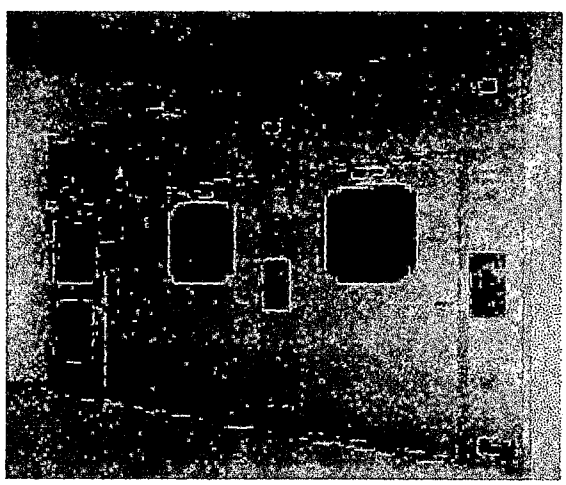
A.2.4.4 TANQUE DE COMBUSTIBLE

Es un tanque donde se almacena el combustible (diesel) para el suministro de los grupos electrógenos. Los depósitos son de capacidad variable en función de la potencia de la Central Telefónica a la que alimenta.

A.2.4.5 TRANSFORMADOR

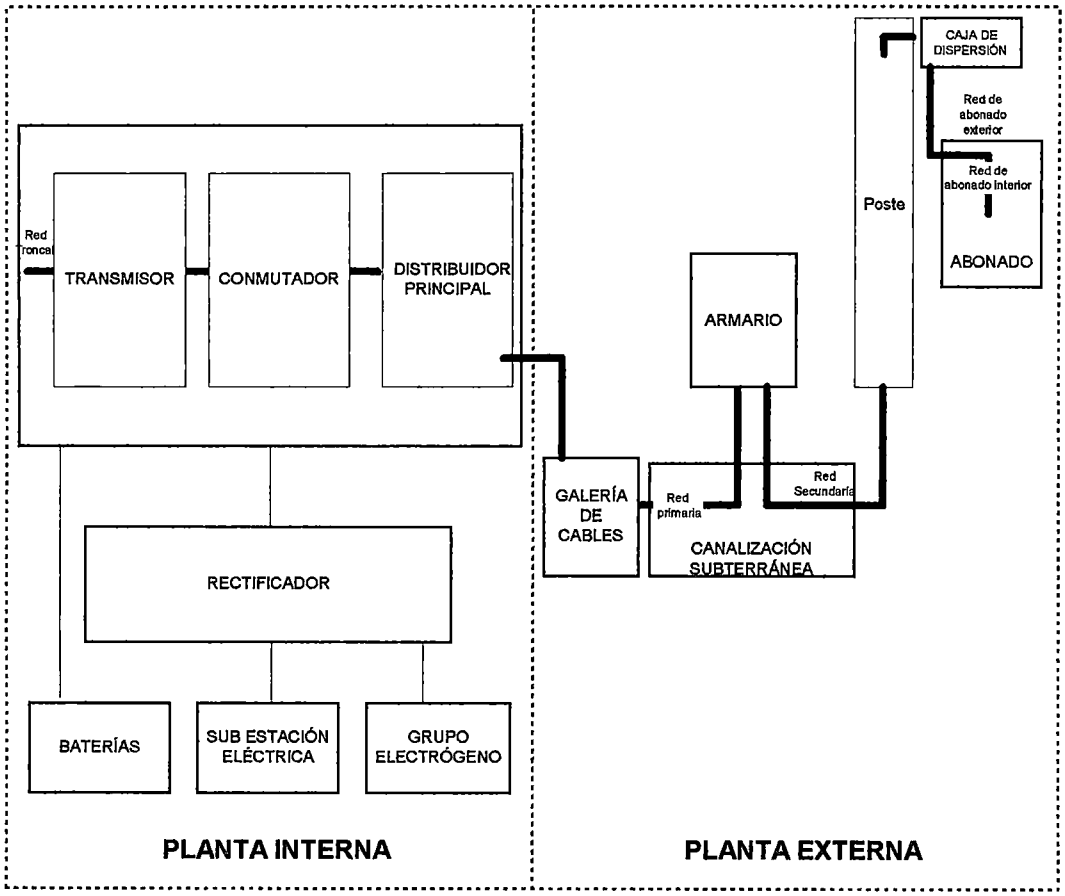
Es una máquina eléctrica estática de corriente alterna que transfiere constante la potencia eléctrica modificando la intensidad y la tensión. Actualmente el transporte de la energía eléctrica desde las centrales productoras a las centrales telefónicas se realiza a tensión elevada, normalmente comprendida entre los 220000 a 320000 V. Luego de que la energía ha llegado a los centros de consumo se reduce de nuevo su tensión 220 V a través del transformador instalado en la central telefónica.

Gráfico A.7 Sala de Su Estación Eléctrica



En el gráfico A.8, que sigue en la página siguiente, mostramos mediante un esquema, como están ensamblados o unidos los componentes de la Red Telefónica

Gráfico A.8 Componentes de la Red Telefónica



Fuente: Elaboración Propia

APÉNDICE B

RIESGO - AMENAZA EN EDIFICIOS DE USO TELEFÓNICO

Los riesgos que pueden ocurrir en los Edificios de Uso Telefónico son:

- Incendio
- Robo
- Sabotaje
- Fraude

B.1 RIESGO DE INCENDIO

Es un fuego fuera de control que destruye total o parcialmente un bien, por efecto de la llama, el humo, el calor o los gases producidos por la combustión de ciertos materiales. En el presente estudio no se considera como riesgo de incendio al que es producido en forma intencionada por el ser humano.

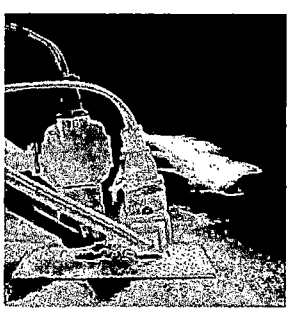


Gráfico B.1 Riesgo de Incendio

B.1.1 AMENAZAS DEL RIESGO DE INCENDIO

B.1.1.1 Flama Abierta

Puede ser producido por soplete de oxiacetileno, soldadores mal empleados, colillas de cigarro no extinguidas y toda fuente de llama.

B.1.1.2 Chispa Eléctrica

Puede ser producido por aislantes o conductores que no trabajan adecuadamente, sobrecargas de corrientes, fusibles en mal estado o inadecuados para las cargas eléctricas, falta de puestas a tierra o las caídas y subidas de tensión. Por inducción o contacto directo del cable de la red eléctrica con el cable de la red telefónica.

B.1.1.3 Fricción

Pueden ser producidas por calentamientos excesivos debido a máquinas incorrectamente lubricadas (por ejemplo el grupo electrógeno).

B.1.1.4 Calor Excesivo

Pueden producirse por un inadecuado sistema de ventilación en la sala de equipos lo cual podría originar un corto circuito (chispa eléctrica).

El contacto de cualquier sustancia susceptible de inflamarse con un elemento caliente no aislado convenientemente.

Así mismo, todos los conductores eléctricos deben estar lo suficientemente alejados y/o aislados térmicamente de los cuerpos calientes porque los aislantes eléctricos normales son sensibles a las altas

temperaturas, lo que da lugar a la disminución de sus cualidades aislantes y provocando corto circuito.

B.1.1.5 Electricidad Estática

Los incendios debido a chispas estáticas en equipo inadecuadamente conectado a tierra, ascienden al 3% del total de incendio.

B.1.1.6 Sobre Tensiones

Otras fuentes de perturbación son las sobre tensiones que se generan como consecuencia:

- Maniobras de conmutación de subestaciones eléctricas
- Desconexiones de grandes transformadores o grandes consumidores
- Cortocircuitos o fallos de tierra y en general determinadas averías que tienen su origen en maniobras realizadas durante el servicio de suministro
- Descargas eléctricas que se transmiten a través de las líneas telefónicas.

B.1.1.7 Peligro de Explosión

Los riesgos típicos de las baterías se dan como consecuencia de las reacciones químicas que se producen entre los electrodos y electrólito de los acumuladores, emitiendo vapores que son explosivos.

B.1.1.8 Falla Técnica

Omisión, la falta por parte de nuestro empleado, contratista o visitante de llevar a cabo una acción, u omisión de un proceso o procedimiento, o el retraso (vencimiento del plazo) de revisión de un sistema puede producir un incendio.

El error por parte de un empleado o contratista en el mantenimiento de los equipos puede producir un incendio.

B.2 RIESGO DE ROBO

Es apoderarse ilegítimamente de un bien (elemento ajeno) total o parcialmente, sustrayéndolo del lugar donde se encuentra.

La característica propia de este riesgo, es que su manifestación y la forma en que se hace presente, guarda una estrecha relación con la organización social correspondiente a cada etapa histórica y constituye un reflejo de la sociedad misma. Los riesgos actuales que afectan a una Empresa presentan un abanico muy grande de matices, dependientes de factores diversos que, además de los enunciados, se ven particularizados por el sector de actividad, el volumen de negocio, lo atractivo del producto o el valor estratégico del mismo.

Gráfico B.2 Riesgo de Robo

B.2.1 AMENAZAS DEL RIESGO DE ROBO

B.2.1.1 Delincuencia común

Muchas de las instalaciones se encuentran ubicadas en zonas donde existen altos índices de delincuencia lo cual lo analizamos en el capítulo II. Los delincuentes cuales pueden ingresar a las instalaciones por los siguientes accesos:

- **Ventanas o puertas en mal estado,** son lugares preferidos por los delincuentes para introducirse a las instalaciones.
- **Muros bajos sin cercos,** son lugares preferidos por los delincuentes principalmente en horas de la noche o cuando están ubicados en zonas poco transitadas.

B.2.1.2 Empleados deshonestos

Pueden ser propios o contratistas, los motivos para hacerlo van desde el hecho de sentirse mal pagados, pensar que la Empresa les debe algo, consideran el robo como una forma de préstamo, sentimiento de que la empresa les menos valora y buscan un protagonismo, hasta creer que robar está bien hecho porque todo el mundo lo hace.

B.2.1.3 Prostitución

Los lugares donde prolifera la prostitución, atrae a la delincuencia

B.2.1.4 Drogadicción

Los drogadictos para poder suministrarse de droga tiene que robar objetos luego venderlos para obtener a cambio dinero.

B.3 RIESGO DE SABOTAJE

Es la acción de destruir o deteriorar maquinaría, productos, instalaciones, como medio de lucha para impedir o entorpecer el desarrollo de una actividad considerada injusta por quienes realizan esta acción. Los Edificios de Uso Telefónico, pueden ser destruidos sin ingresar en ellos, la suciedad, partículas de metal o gasolina pueden ser introducidos por los

conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

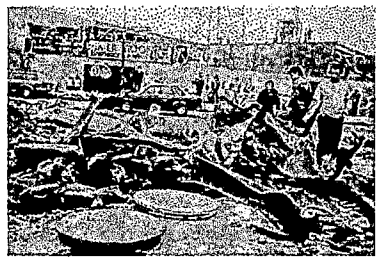


Gráfico B.3 Riesgo de Sabotaje

B.3.1 AMENAZAS DEL RIESGO DE SABOTAJE

- Empleados despedidos en malos terminos
- Competencia desleal
- Sindicatos hostiles
- Pandillas

B.4 RIESGO DE FRAUDE

El riesgo de fraude en los Edificios de Uso Telefónico consiste en utilizar para interés particular los teléfonos de los abonados o dar de alta al servicio de un abonado suspendido.

Gráfico B.4 Riesgo de Fraude (Robo de Línea Telefónica)

B.4.1 AMENAZAS DEL RIESGO DE FRAUDE

- Baja moral entre el personal
- Falta de control con personal contratista

APÉNDICE C

MEDIDAS DE SEGURIDAD FÍSICAS

C.1 DEFINICIÓN

Los dispositivos de defensa física resultan eficaces tanto para entorpecer el acceso del delincuente desde el exterior, como para dificultar su aproximación a locales u objetos vitales, de encontrarse el intruso en el interior del edificio. Por lo general las fachadas del edificio constituyen los límites a partir de los cuales una intrusión puede suponer un grave riesgo.

C.2 IMPORTANCIA

Cualquier obstáculo que se oponga al avance del malhechor y obliga a este a emplear mayor cantidad de tiempo y esfuerzo, sea porque a medida que transcurre el tiempo aumenta la probabilidad de que se le capture, sea porque carezca de los medios necesarios para llevar a cabo su propósito, la dificultad puede llegar a resultar insuperable para ciertos delincuentes, hasta el punto de hacerles desistir de su empeño.

C.3 CARACTERÍSTICAS

Las características constructivas del edificio y las de sus sistemas de cerramiento definen en buena medida la resistencia de la defensa física ante un intento de intrusión o robo.

Es por ello, por lo que al proyectar una nueva construcción, o en cualquier caso, al ocupar una ya existente, debe de verificarse la solidez de las paredes, techos y suelos, así como la resistencia de puertas, ventanas, cerraduras y en general el nivel de protección de que gozan las aberturas existentes.

La facilidad con que pueden abrirse la mayoría de las puertas, las convierten en el medio preferido por el intruso. Muy a menudo esta operación puede llevarse a cabo de forma muy discreta, con la ventaja de que la puerta, una vez abierta, simplifica la huida del malhechor con el botín o luego de realizar algún tipo de sabotaje.

Aparte de la resistencia intrínseca de la puerta (muchas de ellas son huecas, conteniendo cartón en su interior), debería verificarse la calidad de la cerradura, del cerradero y de las bisagras, a fin de adecuar la resistencia del conjunto al nivel de riesgo existente.

La instalación de una puerta robusta, equipada con un dispositivo de cierre eficaz constituye a menudo una medida necesaria, pero no suficiente de defensa física. Ante la imposibilidad de acceder por la puerta, el intruso tratará de hacerlo por otras vías, tales como las ventanas, tragaluces, etc.

La experiencia demuestra que incluso, en ocasiones, el frágil cristal de la ventana puede hacer desistir de su empeño al intruso si la misma se encuentra firmemente sujeta al marco y la cerradura es de seguridad; el delincuente tratará infructuosamente de actuar sobre el cierre practicando previamente un pequeño orificio en el cristal , pero muy raramente aceptará verse descubierto por el ruido, al tratar de realizar un hueco capaz de permitir su acceso. Ello no obstante, si el riesgo, el lugar, etc., exigen un mayor nivel de seguridad podrán emplearse para éstas y otras aberturas, rejas, cristales blindados, etc.

En ocasiones, la naturaleza del bien a proteger exige la adopción de medidas complementarias a las previstas en la periferia del edificio. Sea para reforzar la acción de la defensa física periférica, sea para prevenir el acceso inadvertido del malhechor mediante engaño, puede resultar conveniente crear una segunda barrera de protección física alrededor del objeto o zona de mayor criticidad.

C.4 CLASIFICACIÓN DE LAS MEDIDAS DE SEGURIDAD FÍSICA

Hemos ordenado las medidas de seguridad física en dos grupos, que son los siguientes:

- Protección ante la Intrusión (Robos, Sabotajes, Fraude)
- Control del Fuego (Incendio)

C.4.1 PROTECCIÓN ANTE LA INTRUSIÓN

Esta conformado por los medios de protección ante los riesgos derivados de las actividades antisociales. Estas medidas de seguridad física son:

C.4.1.1 PUERTAS

De acuerdo con la experiencia, el 80% de los robos que se cometen se realizan a través de la puerta. Es por esta razón por lo cual la puerta debe ser objeto de una atención especial a la hora de estudiar la protección contra robo de un local. Es evidente que no sirve de nada poner una cerradura de seguridad sobre una puerta de poca resistencia mecánica, o tener una puerta resistente encuadrada en un marco cuya adhesión al muro es de baja calidad.

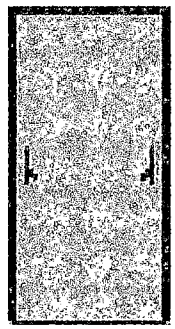


Gráfico C.1 Puerta de Seguridad y Escape

El grado de seguridad esta dado por el nivel de resistencia exigido o determinado que la puerta en su conjunto ha de resistir en función de unos medios de ataque prefijado de ejecución. Pudiendo ser de: Grado A (puerta simple, resistentes al ataque con elementos manuales) y Grado B (puerta blindada, resistentes al ataque con equipos mecánicos).

C.4.1.2 CERRADURAS Y MECANISMOS DE SEGURIDAD

Las cerraduras y mecanismos de seguridad de las puertas y ventanas son dispositivos denominados de apertura y cierre que se componen de elementos maniobrables manuales o mediante elementos electromecánicos o electromagnéticos y que presentan especiales características de protección y seguridad. Esta función asegura el desplazamiento de uno o varios pestillos o elementos de cierre que se alojan o introducen en uno o varios cerraderos dispuestos para tal fin.

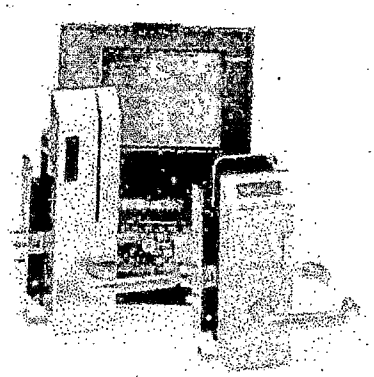


Gráfico C.2 Cerradura de Seguridad

La clasificación general de la cerraduras y mecanismos de aplicación a la protección de la intrusión se realiza en función de:

- Por el elemento de cierre (cerraduras, cerrojos, candados, etc.).
- Por las características de su funcionamiento (Mecánica o eléctrica).
- Por las características específicas ante la forma de agresión o condiciones de ataque a los que se pueden ver sometidos (Intrusión, Fractura, Manipulación o Sabotaje).
- Por la seguridad de la cerradura que esta en función de la constitución o características de fabricación (Cerradura nivel A: Grado de seguridad aceptable, Cerradura nivel B: Grado de seguridad medio-alto, Sabotaje y alteración: Exigencia ante la posibilidad de alteración o bloqueo).

C.4.1.3 VALLADOS Y ENREJADOS

Como definición general se puede decir que los vallados y enrejados son elementos tradicionales para su empleo en cerramientos perimetrales exteriores y siendo utilizados con o sin especiales condiciones de seguridad. Su empleo como elementos de seguridad ante la intrusión no autorizada les confiere un protagonismo diferente y ello ha obligado al estudio y desarrollo de elementos y sistemas especialmente diseñados para tal fin y obviamente con unos niveles y grados de seguridad muy diferentes a los tradicionalmente fabricados o empleados.

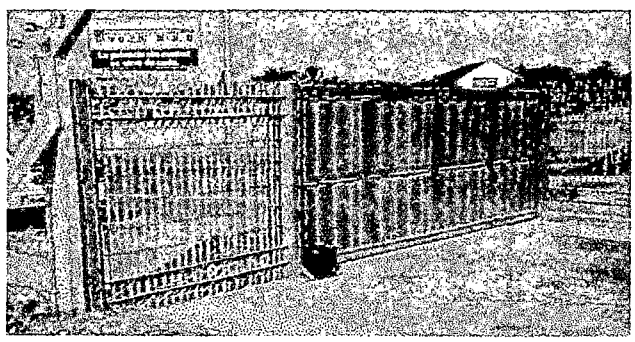


Gráfico C.3 Enrejado

La clasificación general de los vallados y enrejados, de aplicación a la protección ante la intrusión, se realiza en función del tipo de:

- Tipología general (alambrados, mallas, empalizadas de acero, enrejados)
- Material (aceros, aleaciones ligeras, hormigones, maderas)
- Grado de seguridad (Intrusión mediante el levantamiento o realización de hueco por debajo del cerramiento, intrusión mediante la fracturación o realización de hueco sobre el propio cerramiento, intrusión mediante la disposición de elementos que permitan superar la altura y protección del cerramiento, intrusión mediante la fracturación y eliminación de los elementos del cerramiento).

C.4.1.4 ILUMINACIÓN DE SEGURIDAD

Se refiere a la iluminación exterior perimetral fija, que sirve para identificar la amenaza en caso de intrusión y también como medio disuasivo.

C.4.1.5 CERCOS

Los cercos son los encimamientos a base de elementos metálicos que se realiza sobre los muros perimetrales, pudiendo estar energizados o no y monitoreados o no.

C.4.2 PROTECCIÓN ANTE EL INCENDIO

Entre las medidas físicas para controlar el fuego tenemos:

C.4.2.1 SELLOS DE AGUJEROS Y PASACABLES

Son materiales resistentes al fuego, intumecentes con el calor, de tal manera que se expanden impidiendo la propagación del fuego o el humo a

otro ambiente, se clasifican según la resistencia al fuego :

- RF-1 : Resistencia máxima 1 hora
- RF-2 : Resistencia máxima 2 horas
- RF-3 : Resistencia máxima 3 horas

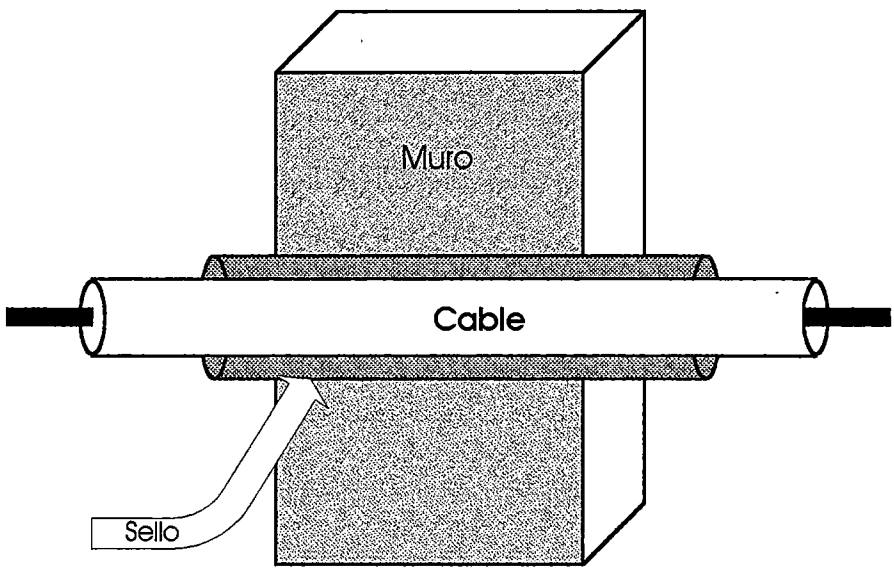


Gráfico C.4 Medidas de hermetización

C.4.2.2 PUERTAS CORTA FUEGO

Son puertas cuyos componentes (marcos, chapas, manijas, hojas, etc.) son resistentes al fuego, debido a que los materiales que se usan en su fabricación son resistentes al fuego y al paso del humo como el asbesto o lana mineral. Se clasifican según su resistencia al fuego en:

- RF60 : Resistencia al fuego 60 minutos
- RF90 : Resistencia al fuego 90 minutos

C.4.2.3 EXTINTORES MANUALES

Son los equipos que contienen un agente que produce la extinción de fuego y un expelente que impulsa al agente con una determinada fuerza tal que cumpla su propósito; este equipo se activa manualmente.

Los extintores se clasifican según el tipo de fuego que intentan apagar (A:: Sólidos combustibles, B : Líquidos inflamables, C : Equipos eléctricos y electrónicos).

Entre los extintores tenemos:

- Extintor de Polvo Químico Seco para apagar fuegos tipo A,B,C
- Extintor de Gas Carbónico para apagar fuegos tipo B, C
- Extintor de Agua, para apagar fuegos tipo A

Gráfico C.5 Extintor Manual

APÉNDICE D

MEDIDAS DE SEGURIDAD ELECTRÓNICA

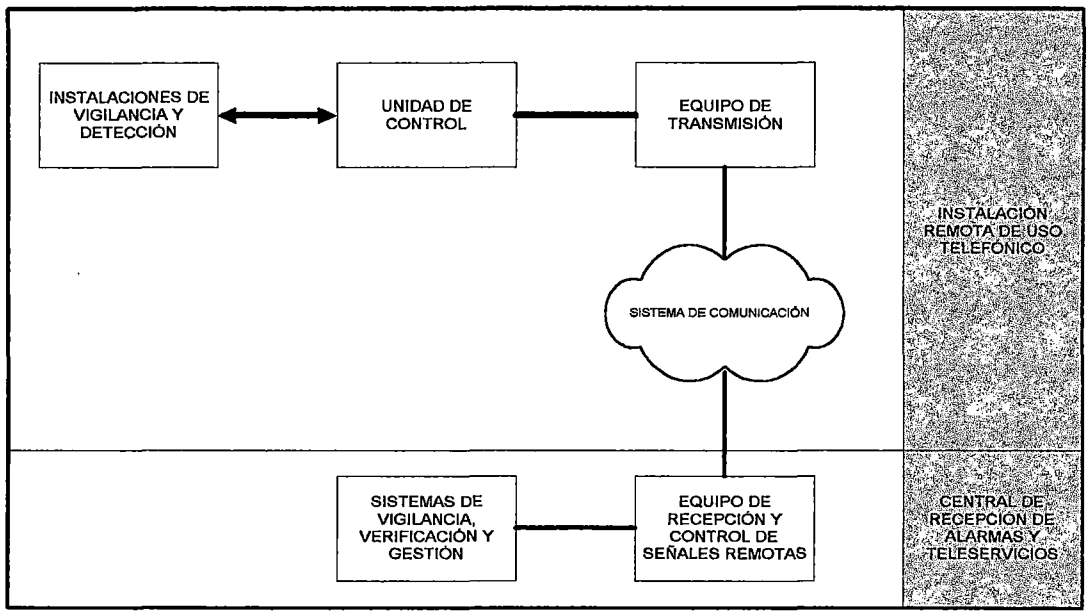
Todas las medidas de protección física que se han ido citando en el apéndice anterior, por muy eficaces que sean, el ladrón con suficiente tiempo y medio, es capaz de superarlas y es por ello imprescindible instalar otro tipo de medidas mas eficientes como por ejemplo sistemas de protección electrónica que tendrá la misión de detectar y monitorear las alarmas.

La protección electrónica según la concepción adoptada esta conformada por lo siguiente:

- Instalaciones de vigilancia, detección y control
- Unidad de control y equipo de transmisión
- Equipos de recepción y control de señales remotas
- Sistemas de vigilancia, verificación y gestión
- Sistema o medios de comunicación

En el gráfico D1 que se muestra en la siguiente página, se observa la distribución de los componentes de la seguridad electrónica, donde se puede notar si pertenecen a la CRAT o a la IRUT.

Gráfico D1. Componentes de la Seguridad Electrónica



Fuente: Elaboración Propia

D.1 INSTALACIONES DE VIGILANCIA Y DETECCIÓN

Son los dispositivos mecánicos y/o electrónicos, constituidos por los detectores, sistemas de vídeo, lectores de control de acceso, etc., capaces de comprobar las variaciones de normalidad en una instalación, mandando información hasta la Unidad de Control.

Estos dispositivos envían a la Unidad de Control un cambio de estado, como consecuencia de las variaciones de una magnitud física que ha sido interpretada como presencia de un intruso o un fuego en el área protegida, accionando de forma automática los dispositivos, detectando una anomalía: paso por lugares protegidos, apertura de puertas, rotura de vidrios, aumento anormal de la temperatura, etc.

Al margen de esta función principal de indicación de condición de alarma, realizarán otras funciones y enviarán su información a la Unidad de Control:

- Sabotaje: Puede ser por detección mecánica de manipulación o por vigilancia del propio detector (antimasking)
- Prueba (de funcionamiento)
- Memoria (de las variaciones de estado en un periodo)

D.1.1 MEDIDAS DE SEGURIDAD ELECTRÓNICA ANTE INTRUSIÓN

Estas medidas ante cualquier intrusión avisarán en forma discreta sobre los eventos anormales de robo o situaciones de alerta de la instalación a la Central de Receptora de Alarmas y Teleservicios que se comunicará con los cuerpos de seguridad privada o pública.

Hay tres tipos de detectores que controlarán la intrusión según como ésta se realice:

- **Periféricos:** Para que se produzca una señal de alarma primero se tiene que producir un daño tales como, forzamiento de una puerta, rotura de un cristal, etc. Los detectores periféricos alertarán ante este primer intento de intrusión.

- **Volumétricos:** Los detectores volumétricos, instalados en el interior, se activarán cuando la intrusión ya se haya producido.

- **Perimetrales:** Los detectores perimetrales, instalados en el exterior, protegerán la instalación antes de que se produzca el primer daño al que antes hacíamos mención.

D.1.1.1 EQUIPOS PARA LA PROTECCIÓN PERIFÉRICA

Entre los detectores tenemos:

- **Contacto Magnético**

Detecta la apertura de puertas y ventanas. Esta basado en el desequilibrio del campo magnético formado entre los dos imanes (contactos) permanentes que están situados en las partes fija y móvil de la abertura.

- **Detector sísmico**

Su función es detectar sobre los cuerpos sólidos oscilaciones que se propagan en el material en forma de ondas sísmicas. Permiten detectar todos los métodos de ataque, sobre paredes, techos, suelos y puertas de cajas fuertes, puertas blindadas, etc.

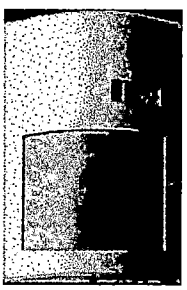
D.1.1.2 EQUIPOS PARA LA PROTECCIÓN VOLUMÉTRICA

Entre los detectores tenemos:

- **Detectores infrarrojos pasivos (PIR)**

Operan mediante la detección de un cambio de energía que ocurre cuando un cuerpo con cierta temperatura pasa por un segundo plano, con otra temperatura, dentro del alcance del detector.

Gráfico D.2 Detector Infrarrojo Pasivo



D.1.1.3 EQUIPOS PARA LA PROTECCIÓN PERIMETRAL

- **Sensor de haz fotoeléctricos**

Está compuesto por dos unidades, un transmisor de rayos infrarrojos y un receptor supervisado. Cuando un intruso interfiere su campo de acción, los pulsos que llegan al receptor tienen otro patrón. Estos pulsos serán decodificados o interpretados para determinar el nivel de alarma requerido. Por lo general el transmisor emite más de un rayo para eliminar posibles falsas alarmas (animales, objetos extraños).

D.1.1.4 CONTROL DE ACCESO

A través del Control de Acceso se administra el ingreso y/o salida de las personas previamente identificadas, logrando un control selectivo de entrada, control de frecuencia de ingreso y/o salida del personal, control estadístico del movimiento de las personas dentro del edificio.

Gráfico D.3 Control de Accesos

La identificación de personas servirá para autorizar su acceso una vez comprobado el cumplimiento de los requisitos. Además de la identificación, deberán disponerse medidas para impedir el acceso cuando resulte denegado.

Además existen otros objetivos secundarios que permiten dar utilidad al sistema y que siempre hay que definir en la fase inicial. Entre ellos podemos citar:

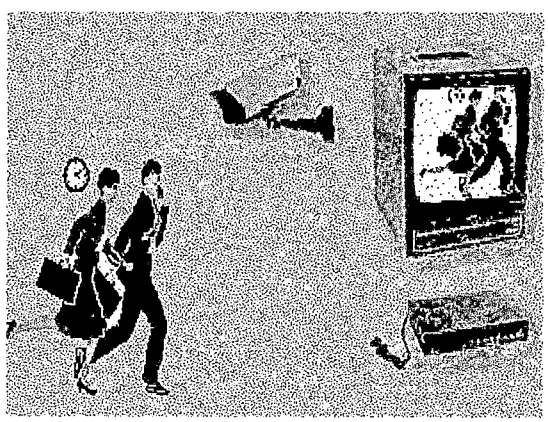
- Control de presencia
- Información de frecuencia y dirección de paso
- Conocimiento de intentos de acceso no autorizado
- Número y tipo de visitantes

D.1.1.5 TELEVIGILANCIA

Tiene como objetivo la vigilancia constante de las áreas interiores y exteriores de la instalación, permitiendo a través de la Central Receptora de Alarmas y Teleservicios, monitorear y controlar el movimiento del flujo de personas. Un sistema de televigilancia cuenta con cámaras de televisión con sus respectivos lentes.

Una cámara está compuesta por dispositivos ópticos (lentes), que recolectan la luz captada de la escena y por dispositivos electrónicos que convertirán estas señales de luz en señales eléctricas adecuadas para ser transmitidas a los monitores remotos, vídeo grabadores y/o matrices de conmutación de vídeo.

Gráfico D.4 Televigilancia



Los ordenadores (sistema de Vigilancia, verificación y gestión) recibirán las señales eléctricas de las cámaras y las presentarán en forma de luz a través de una pantalla. Los monitores estarán asociados a sistemas de audio, alarmas visuales o sonoras, de tal forma que se optimiza el trabajo de un operador y se vuelve menos tedioso. Este sistema permite la vigilancia centralizada desde un único puesto de control.

D.1.2 MEDIDAS DE SEGURIDAD CONTRA INCENDIOS

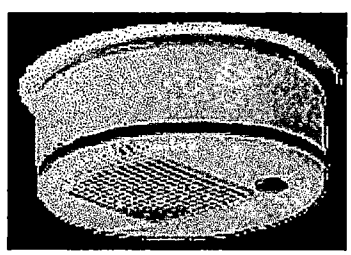
A través de este sistema se detectará y localizará un eventual incendio de manera inmediata, esto facilitará realizar una acción rápida en la aplicación del procedimiento y métodos de extinción y evacuación.

D.1.2.1 DETECTORES DE INCENDIO

- **Detectores de humo**

Son los que deberán actuar con la presencia de humo, existiendo dos tipos detectores lónicos y detector ópticos

Gráfico D.5 Sensores de Incendio



- **Detectores térmicos**

Estos dispositivos sensan temperatura, pueden ser de dos tipos termostáticos o termovelocimétricos.

- **Detectores de llama**

Los detectores de llama reaccionan ante la aparición de energía radiante visible para el ojo humano o a la energía radiante que está fuera del campo de la visión humana. Existen varios tipos de detectores de llama, entre los mas utilizados están los detectores de llama Infrarrojos y los detectores ultra violetas.

- **Estación manual de alarma**

Es un dispositivo que tiene por objeto iniciar una señal de alarma manualmente en casos que la emergencia lo amerite, cuando el sistema automático de detección no funcione o en apoyo a este último.

Gráfico D.6 Estación Manual de Alarma

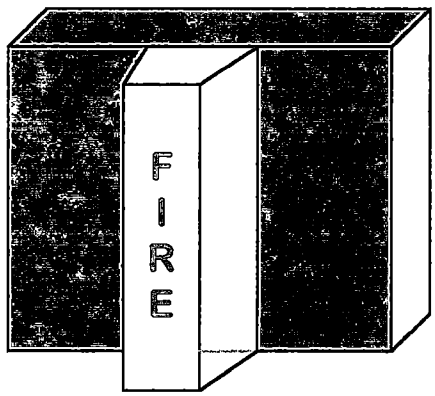
D.1.2.2 DISPOSITIVOS ANUNCIADORES

Un sistema de anunciadores de alarma y de voceo está compuesto por sirenas o bocinas, parlantes.

- **Sirena**

Son dispositivos de señalización acústica y/o óptica de alarma de incendio que son activados por los detectores de incendios o estaciones manuales.

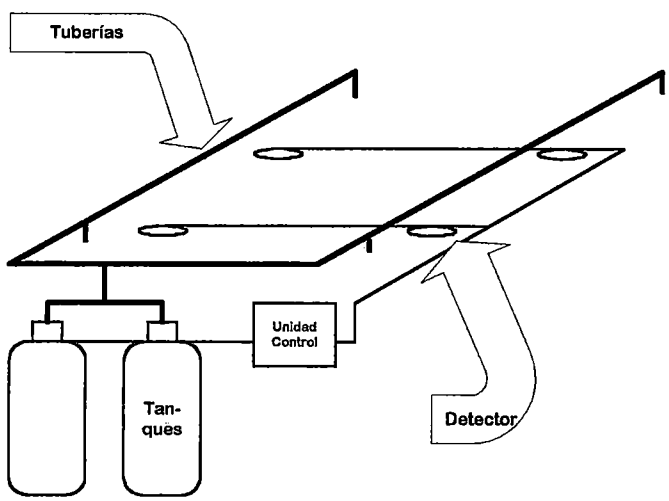
Gráfico D.7 Sirena



D.1.2.3 SISTEMA AUTOMÁTICO DE EXTINCIÓN DE INCENDIOS

Son sistemas a base de un agente extintor de fuego pudiendo ser gas o polvo contenidos en un recipiente, lo cuales están supervisados por la unidad de control, los cuales envían una señal de apertura a sus válvulas solenoides cuando los detectores de incendios dan señal de alarma.

Gráfico D.8 Sistema de Extinción Automática



D.2 UNIDAD DE CONTROL

Son equipos que controlan las señales provenientes de los dispositivos de seguridad. Por lo general estos equipos están integrados en un sistema o conjunto de dispositivos que realizan funciones afines, por ejemplo existen unidades que controlan las alarmas contra incendios, otros que controlan alarmas contra robos o intrusión, otros que controlan las lectoras, otros que controlan las cámaras de televisión, etc.

Es el elemento fundamental de la instalación en el cual se tienen que producir las reacciones necesarias ante los cambios de estado de los detectores asociados al sistema.

La unidad de control realiza las siguientes funciones:

- Recibe la señal enviada por los detectores conectados a ella a través de las bucles de detección, indicando la alarma de forma óptica o acústica y localizando la zona en que se encuentra el detector o pulsador activado. En forma optativa puede registrar total o parcialmente esta información.
- Activa los dispositivos de alarma o transmite la señal de alarma a una estación de recepción de alarmas.
- Vigila el correcto funcionamiento de la instalación e indica los defectos mediante señales ópticas o acústicas de avería (por ejemplo cortocircuito, corte de línea, fallo de alimentación).

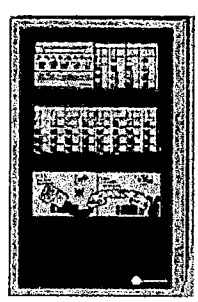


Gráfico D.9 Unidad de Control (Panel de Incendios)

D.3 EQUIPOS DE TRANSMISIÓN

Son los equipos de conectividad y envío de señales, que servirán para mantener las comunicaciones con la unidad de control, por medio de redes de comunicación. Por lo tanto facilitarán el diálogo bidireccional con la CRAT.

D.4 SISTEMA DE COMUNICACIÓN

El monitoreo de las instalaciones remotas a través de una Central Receptora de Alarmas y Teleservicios, se apoya en un Equipo de Recepción que se conectará a la Red de Comunicación para recibir las señales del Equipos de Transmisión.

Es preciso indicar que la Red Telefónica Conmutada (RTC), tiene una cobertura a nivel nacional y relativamente bajo costo de explotación. Existen otros medios de transmisión, como líneas telefónicas punto a punto pero tienen un alto costo o telefonía celular con cobertura prácticamente nacional.

D.5 CENTRAL RECEPTORA DE ALARMAS Y TELESERVICIOS

Es la Instalación donde uno o varios operadores, reciben alarmas provenientes de las instalaciones monitoreadas, se desencadenan las telegestiones multimedias y se almacena y procesa la información. Está formado por un número variable, según necesidades, de ordenadores, conectados en una red de comunicación de área local, (equipos estandarizados para asegurar su evolución), y a Equipos de Recepción y Control de Señales Remotas.

Las centrales de alarma, son centros que trabajan las 24 horas al día y 365 días al año. Su misión es la recepción, interpretación y gestión de señales de alarma a través de diversos medios de comunicación,

comunicando a los medios de neutralización propios o públicos (policías, serenazgo, bomberos, servicios médicos, etc.) sobre una determinada incidencia, luego de comprobar su veracidad.

Gráfico D.10 Central de Recepción de Alarmas

D.5.1 EQUIPOS DE RECEPCIÓN Y CONTROL DE SEÑALES REMOTAS

Constituidos por los sistemas de la CRAT encargados de recibir, interpretar y chequear las señales pocedentes de los sistemas de centralización o control local mediante los medios de comunicación establecidos.

D.5.2 SISTEMAS DE CONTROL, VERIFICACIÓN Y GESTIÓN

Se refiere fundamentalmente a los procesadores con sistemas operativos multitareas de software para la gestión general y particular de todos y cada uno de los servicios establecidos. Comprende la total parametrización de las entradas y salidas de los multiplexores, equipos de diálogo del sistema centralizado. Se incluye aquí también el UPS como sistema de emergencia en caso de caída de la energía eléctrica.

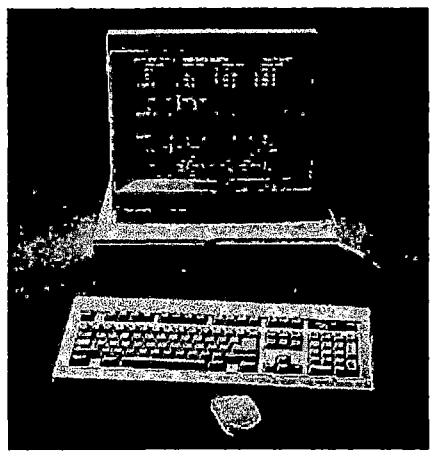


Gráfico D.11 Procesador para la Gestión de la CRAT

D.5.3 SERVICIOS DE TELEGESTIÓN MULTIMEDIA

La Central Receptora de Alarmas y Teleservicios (CRAT) puede incorporar servicios básicos especializados dentro de cinco áreas de telegestión:

- **Telealarma:** Entendiendo como tal los servicios de vigilancia, detección y control, recepción y gestión de alarmas, en forma remota, relacionadas principalmente con la seguridad de las personas y los bienes (intrusión, atraco, robo, incendio, inundaciones, explosión, etc.)

- **Televigilancia:** Comprende los servicios de control de vigilancia y gestión en forma remota, de sistemas de circuito cerrado de televisión, tratamiento y digitalización de vídeo (vigilancia, transmisión, grabación, tratamiento de imágenes, etc.).

- **Telemando:** Se denomina a los servicios de control y gestión, en forma remota, de sistemas e instalaciones con necesidades de accionamiento local (encendido o apagado, apertura o cierre, conexión o desconexión, etc.).

- **Telecontrol:** Son los servicios tendentes a controlar y gestionar, en forma remota, parámetros predeterminados de funcionamiento o mantenimiento de instalaciones técnicas (energía, averías, temperaturas, etc.).

- **Telemedida**: Son los servicios de control y gestión, de forma remota, de aparatos o instalaciones con necesidad de medición periódica o permanente (lectura de contadores, controles de paso, control de equipos sanitarios, control de existencias, etc.)

- **Teleasistencia:** Entendiendo como tal la vigilancia, detección, control y gestión de alertas o alarmas, en forma remota, de carácter social o sanitario (atención social, atención sanitaria, control de vida activa, custodia de llaves, etc.).

APÉNDICE E

MEDIDAS DE SEGURIDAD HUMANAS (SERVICIO DE VIGILANCIA HUMANA)

E.1 DEFINICIÓN

Existen muchas definiciones especialmente cuando está determinado el fin que persigue. La más genérica es aquella que sostienen algunos expertos al decir que la vigilancia humana es la actitud permanente de una persona en buen sentido de la palabra, e implica reunir a todos los elementos y virtudes de las cuales ha sido dotado el ser humano: Observación, conocimiento de lo que constituye amenaza y la percepción.

Por lo tanto, la Vigilancia Humana es el servicio de seguridad realizado por seres humanos denominados agentes de vigilancia o guardianes debidamente equipados (uniforme, arma, etc.), que dependen de una empresa de vigilancia que asumirá la delicada misión de responsabilizarse del resguardo y protección de los bienes materiales.

El cuerpo de vigilancia tiene como principal objetivo, evitar, la observación y/o acciones preventivas de posibles incendios, inundaciones, derrumbamientos, robos y hurtos, así como también cualquier circunstancia anormal que pueda poner en peligro la vida de los trabajadores y/o las propiedades de la compañía cliente.

Pertenecer al servicio de vigilancia de seguridad implica someterse a una disciplina, a un reglamento y a una normas de conducta exigente.

El agente de vigilancia, para el correcto cumplimiento de sus funciones, deberá tener el siguiente comportamiento:

- Responsabilidad
- Identificación
- Conciencia
- Disciplina
- Entereza
- Honradez
- Justicia
- Lealtad
- Camaradería
- Carácter
- Gratitud
- Honor
- Respeto
- Modestia
- Obediencia
- Puntualidad
- Autoridad
- Unidad
- Dignidad
- Veracidad

E.2 IMPORTANCIA

No podrá existir una situación de seguridad, si los responsables de su ejecución no mantienen permanentemente en actitud vigilante o de

observación, para determinar los riesgos y adoptar las medidas que prevengan o respondan. Un agente de vigilancia que no vigila, es el primer riesgo para consigo mismo, para sus compañeros, para los empresarios, la empresa y sus bienes.

E.3 CARACTERÍSTICAS

El trabajo de vigilancia exige una gran actividad, una observación permanente y una prevención efectiva en todo momento, para poder garantizar la vigilancia y protección de los bienes bajo su responsabilidad, así como la diligencia, la atención, la iniciativa, la precaución y la sagacidad deben ser virtudes normales de un agente de vigilancia de seguridad.

Las características del servicio de vigilancia humana son las siguientes:

- Es permanente, se realiza de día, de noche y en forma interrumpida
- Siempre previene y no espera que algo suceda
- Observa con atención y hasta con desconfianza
- Permanentemente en alerta para la intervención en cualquier hecho sorpresivo
- Cualquier descuido suele ser perjudicial
- Inspeccionar para corregir cualquier posible descuido del empleado o trabajador que pueda favorecer la comisión del delito
- No puede omitir jamás ninguna recomendación

El cumplimiento de estas normas son indispensables en el agente de vigilancia y de su cumplimiento se deriva, primero la seguridad física del vigilante y segundo la eficiente protección de los bienes y personas de la empresa bajo su custodia.

E.4 CLASIFICACIÓN DE LOS SERVICOS DE VIGILANCIA

E.4.1 SERVICIO DE VIGILANCIA FIJA

Son los servicios de vigilancia desarrollados en una misma instalación:

- Control de accesos
- Puntos fijos
- Ronda interior
- Ronda exterior

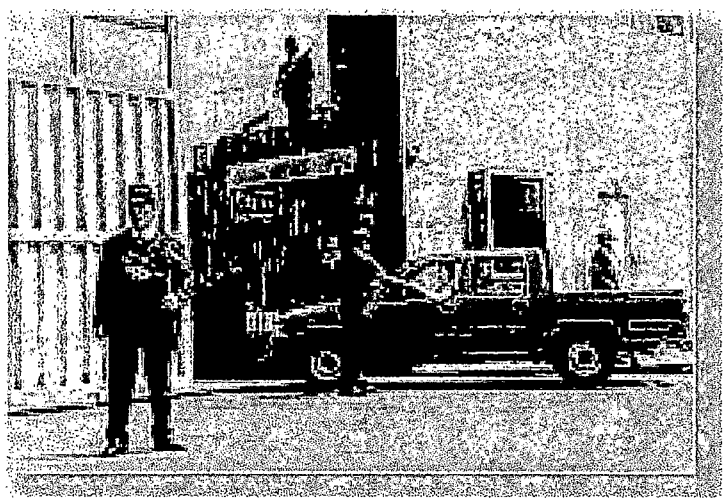


Gráfico E.1 Servicio de Vigilancia Fija

E.4.1.1 Control de accesos

Es la que tiene su mayor implantación en cualquier tipo de instalación, y dentro de estas en los periodos de actividad de la misma, aunque la función continua lógicamente fuera del período de actividad.

Dentro de los cometidos a desarrollar por el agente de vigilancia, destacados a esta función se encuentran:

- Control de entradas y salidas de personal (realizándose operaciones de: Identificación, autorización, registro y adecuación)
- Control de entradas y salidas de vehículos
- Control de entradas y salidas de mercancías
- Control de objetos portados por las personas

E.4.1.2 Puntos fijos

Consiste en la vigilancia y observación de determinadas zonas de la instalación, con la finalidad de prevenir y reaccionar ante cualquier amenaza. Dentro de este servicio podríamos citar como ejemplos la vigilancia de áreas restringidas o zonas de alto riesgo.

E.4.1.3 Ronda interior

Este servicio consiste en el control y vigilancia de las distintas áreas de una misma instalación, mediante la visita o inspección periódica de las mismas por el agente de vigilancia. Esta función se realiza normalmente fuera del período de actividad de la instalación y suele compaginar con las funciones de control de accesos y de vigilancia de puntos fijos.

E.4.1.4 Ronda exterior

De características similares a la anterior, pero ya los puntos o áreas a inspeccionar no se encuentran en las áreas interiores sino en el entorno de la instalación, pero sin salirse del perímetro que delimite la propiedad.

E.4.2 SERVICIOS DE MANEJO DE CENTROS DE CONTROL

La actividad de este servicio se basa en la recepción de las señales procedentes de los sistemas de detección de las instalaciones, para una vez

analizadas y chequeadas proceder a comunicar dicha incidencia para que se efectúe la intervención sobre dicha instalación, la respuesta o reacción podrá realizarse por personal de empresas de seguridad y/o por las fuerzas de seguridad estatales o locales.

Son este tipo de servicios los que requieren mayores habilidades de los vigilantes en los aspectos de manejo y utilización de medios electrónicos.

Gráfico E.2 Servicios de Manejos de Centro de Control

E.4.3 SERVICIO DE VIGILANCIA MÓVIL

Son aquellos que se realizan en instalaciones diversas y que si bien no se encuentran delimitadas físicamente en su conjunto, si se encuentran ubicadas en una misma zona.

La función a realizar consiste en líneas generales en la realización de visitas o inspecciones periódicas a las distintas instalaciones y/o de patrullaje continuo por las mismas, realizándose en zonas donde no hay vigilancia fija y fuera de los periodos de actividad de dichas instalaciones, siendo recomendable que este servicio sea desempeñado por dos vigilantes de seguridad, comunicados vía radio y/o teléfono con la Central de Alarmas y con un medio adecuado de transporte para sus desplazamientos dependiendo de las distancias a recorrer.

Este servicio realiza también la actividad de atención de alarmas, por la cual la patrulla de reacción actúa cuando la Central de Alarmas informa, de

que le ha llegado una señal de la instalación, y dado que en el propio vehículo de patrulla se llevan las llaves de la instalación se produce una reacción inmediata y rápida. Lo que parece obvio y eficiente es que la misma patrulla de reacción que realiza el control de las instalaciones sea la que acuda en caso de una alarma.

Gráfico E.3 Servicio de Vigilancia Móvil

E.5 LA ORGANIZACIÓN DEL SERVICIO

Consiste en ordenar, el conjunto de elementos que ya hemos determinado anteriormente y que son:

- Horas por puestos a cubrir
- Funciones a desempeñar

Se exigirá a las empresas de servicio de vigilancia que las programaciones de trabajo deban sustentarse en turnos no excesivos de 8 horas continuadas, en puestos con actividad motriz y que no comparten una constante atención de visión y concentración en espacios reducidos, tal y como sucede con los puestos de operados de centros de control de seguridad de las instalaciones donde los turnos no deberían de sobrepasar las 4 horas continuadas.

APÉNDICE F

MEDIDAS DE SEGURIDAD ECONÓMICAS

F.1 DEFINICIÓN

Luego de realizar el estudio de los riesgos a los que está expuesta la empresa se pasará por identificar, evaluar y cuantificar las pérdidas que estos eventos pueden producir en el patrimonio y finalmente intentar establecer medidas de control de los riesgos, mediante la implantación de sistemas de prevención, protección y protocolos de actuación encaminados a eliminar la causa productora del daño o al menos, reducir sus consecuencias.

Sin embargo este análisis puede llevar a situaciones frustrantes ya que pueden existir ocasiones en las que resulte imposible eliminar o controlar las causas que origine un siniestro. Pensemos en los efectos destructivos que pueden ocasionar fenómenos de la naturaleza como los terremotos o inundaciones que ocurren en forma imprevisible y cuyas consecuencias son catastróficas. Se pueden citar como ejemplos recientes los incendios que han destruido grandes empresas o medianas y pequeños negocios.

Ante esta perspectiva cabe plantearse varias soluciones. El establecimiento de una provisión de fondos en base a dotaciones periódicas con las que hacer frente a graves pérdidas o bien la obtención de líneas de financiación externa cuyo costo será con cargo a la cuenta de resultados, es decir, al beneficio de la empresa. En muchos casos estas soluciones

presentan ciertas limitaciones ya que la cuantía de los daños susceptibles de sufrirse en el patrimonio a causa de siniestros no puede ser prevista con certeza en los presupuestos anuales y otras ocasiones estos fondos invierten en otras cuestiones tales como la adquisición de nuevas líneas productivas o ampliaciones de negocios. Incluso si el impacto de un posible siniestro pudiera cuantificarse, la pérdida podría resultar tan elevada que la retención del riesgo bajo la formula de la provisión o constitución de fondos propios resultaría ineficaz para la financiación de las pérdidas, por lo que resultará más apropiado acudir a la transferencia del riesgo, por ejemplo, con la contratación de un seguro. A ello hay que añadir que la creación de ciertos fondos de autoseguro puede resultar poco atractiva desde el punto de vista fiscal. De esta forma puede optarse por transferir las pérdidas esperadas a otras entidades las cuales soporten el coste de los daños ocurridos como contraprestación al pago de determinadas cantidades. Fundamentalmente estamos hablando de empresas de seguros.

Este pago aporta una ventaja sobre los anteriores métodos de financiación, su periodicidad permite establecer previsiones en los costes fijos y presupuestales de la empresa y su acuantía es reducida en relación con la posible pérdida a la que se tiene que hacer frente.

Se llega a la conclusión, por tanto, que la mayor parte de las empresas, sea cual fuera el sector en el que se ubiquen, necesitan proteger su patrimonio y una de las fórmulas básicas de protección es la contratación de una póliza de seguro para sus bienes.

F.2 POLIZAS DE SEGUROS DE DAÑOS PATRIMONIALES

Estos conceptos de retención y transferencia del riesgo, tratado individualmente pueden operar conjuntamente en un contrato de seguro, por otra parte fórmula habitual utilizada en el ámbito empresarial.

Los mecanismos que generalmente se arbitran son los **deducibles** así como la **indemnización**. Por ello, las pérdidas sufridas en un siniestro son repartidas entre el asegurado y el asegurador.

Si se aplica un deducible al pago de un siniestro, el asegurado se hace cargo de todas las pérdidas siempre y cuando éstas no sobrepase la cantidad establecida como deducible. En caso contrario si el valor del siniestro sobrepasa la cantidad deducible el asegurado afronta el pago esta cantidad y el resto de la indemnización a cargo de la entidad aseguradora hasta completar el valor total de los daños.

La técnica transferencia debe ser cuidadosamente manejada y aplicada en la gerencia de los riesgos de la empresa. Una mala gestión en la identificación de los riesgos y el cálculo de las posibles pérdidas puede llevar a una incorrecta aplicación de las medidas económicas de protección adoptadas y poner en peligro la subsistencia del negocio en el caso de un grave siniestro baja que produzcan daños alta cuantía pero de frecuencia baja.

F.3 CONDICIONES DE UNA POLIZA DE SEGUROS

Las redacción de una póliza recoge en sus condiciones generales el objeto y la extensión del seguro definiendo los riesgos cubiertos (garantías) y excluidos, cuáles son los bienes asegurados, el pago de primas, deducibles en caso de siniestro, y las indemnizaciones.

En las condiciones particulares se fija la duración del contrato, las coberturas y se fija el valor de los bienes asegurados.

El mercado de seguros es exigente y los productos que se ofertan deben responder a las necesidades que demandan las empresas. De esta

forma, y respetando las directrices anteriormente expuestas, se han definido básicamente dos tipos de seguros que responden a la denominación de pólizas de riesgos nominados y pólizas todo riesgo.

F.4 PRINCIPIOS BÁSICOS

Bajo estas premisas hay que tener presente los principios básicos aseguradores y legales que rigen los contratos de seguro y que esencialmente son:

- Para tener derecho a percibir una indemnización debe de producirse un daño en el interés asegurado.
- El pago de un siniestro no debe ser objeto de lucro por parte del asegurado
- Deben de especificarse claramente cuales son los eventos causantes de daños y objeto de cobertura.
- Estas causas deben ser siempre súbitas, accidentales y no requeridas

De ahí la importancia vital que tiene establecer las causas del siniestro, la cuantía de los daños producidos y la correcta valoración de los capitales que deben de figurar la póliza.

En innumerables ocasiones un siniestro de baja cuantía en daños a los bienes conlleva a una parada de producción que se dilata en el tiempo y que acarrea la inevitable pérdida de ventas de los productos fabricados. Este acontecimiento puede hacer peligrar la subsistencia de la Empresa al verse afectada muy seriamente su cuenta de pérdidas y ganancias. También el seguro tiene propuesta para ello. Siempre que el siniestro cubierto por la póliza de daños materiales provoque una disminución del volumen del negocio o bien se incurran en gastos para evitar esta caída (por ejemplo aumentar un turno más de trabajo una vez reanudada la producción o

comprar productos similares a terceros para atender los pedidos de los clientes y evitar pérdidas de ventas) puede indemnizarse el margen bruto o los gastos permanentes en la medida en que han sido afectados, así como los extra costos en que haya que incurrir para evitar la pérdida de ventas.

Sin embargo hay que tener en cuenta que, aunque el seguro resarza económicamente a la empresa, resultaría difícil recuperar los clientes perdidos que hayan tenido que recurrir a la competencia para abastecerse de productos, ni tampoco recuperar la cuota de mercado que tenía antes del siniestro ni el posible deterioro o pérdida de imagen frente al público al no estar presentes sus productos en el mercado.

Finalmente no se puede obviar un aspecto muy importante en la contratación de un seguro: la valoración de los bienes. La incomoda aplicación de la regla proporcional en el pago de un siniestro es consecuencia de una infravaloración del interés asegurado, de ahí la importancia de fijar criterios de dicha valoración y en consecuencia obtener los valores correctos de los bienes cubiertos.

El Seguro utiliza el concepto de valor de reposición a nuevo. Se valora la cantidad necesaria para la adquisición de un bien nuevo de las mismas características o similares. El capital fijado en póliza incluye también los gastos de transporte, montaje y derechos de aduana si lo hubiere.

El concepto moderno de seguro no se limita sólo al pago de las cantidades correspondientes al valor de los bienes dañados en un siniestro, sino que amplía sus prestaciones acercándose más a la prevención y los servicios añadidos a la reposición de las pérdidas sufridas en un evento, apoyando al empresario con coberturas hasta hace poco no consideradas como aseguradoras.

El más conocido siniestro de incendio eleva las pérdidas no exclusivamente a los bienes afectados directamente por el fuego o el humo sino también a los gastos incurridos en el pago de los servicios de bomberos, el descombro, las medidas adoptadas por le asegurado para salvar los bienes no afectados por el siniestro como son el transporte y alquiler de otros equipos durante las reparaciones, el coste que supone el llenado con nuevo agente extintor de los sistemas de protección contra incendio, etc. Todos estos importes a los que el asegurado debe de hacer frente son cubiertos por el seguro, como valor añadido.

La fuerte competencia en el mercado libre amplía la oferta de servicios que una aseguradora pone en manos de los clientes y va más allá de la mera indemnización de los daños y gastos parejos de un siniestro. Así podemos encontrar departamentos técnicos especializados en temas de seguridad en los cuales se trabaja paralelamente con la empresa en la identificación, evaluación y control de los riesgos, siendo asesorado el cliente por técnicos especializados en la materia. Estos mismos departamentos realizan auditorias de los sistemas de protección, diseñan o aconsejan sobre sistemas de seguridad a adoptar en el caso de ampliaciones en el negocio o confeccionan planes de emergencia y forman al personal de la empresa en el uso y manejo de los sistemas de protección. Abordar las últimas tecnologías es otra tarea llevada a cabo en el mundo del seguro.

Así mismo la combinación del seguro y el valor de la prima se pueden ver favorablemente afectados cuando existe una conexión permanente de sensores de intrusión, incendio, inundación, etc. con una Central Receptora de Alarmas.

ANEXO 01

VALOR DE ACTIVOS E INGRESOS DE UNA INSTALACIÓN REMOTA DE USO TELEFÓNICO

A1.1 VALOR DEL BIEN (US $)

AMBIENTES	EQUIPOS	VALOR
Ambiente A	Baterías	20.000,00
	Rectificador	30.000,00
	Repartidor Principal	10.000,00
Ambiente B	Conmutador	80.000,00
	Transmisor	100.000,00
	Aire Acondicionado	5.000,00
Sala Grupo Electrógeno	Grupo Electrógeno	200.000,00
	Tablero General	2.500,00
Sala Subestación Eléctrica	Sub Estación Eléctrica	50.000,00
Patio	Tanque de Combustible	2.500,00
TOTAL INVERSIÓN FIJA		**500.000,00**

A1.2 INGRESOS POR EL SERVICIO TELEFÓNICO (US $)

Ingreso Mensual por Línea	50,00
Número de Líneas por IRUT	2.000
Ingreso Mensual por IRUT	100.000,00

ANEXO 02

ANÁLISIS DE RIESGOS EN INSTALACIONES REMOTAS DE USO TELEFÓNICO

Tabla A2.1 Análisis de Riesgo de Incendio en el Ambiente A

AMBIENTE A		
RIESGO INCENDIO		
CRITERIO	**VALOR**	**JUSTIFICACIÓN**
Función (F)	3	Este ambiente es parte del proceso.
Sustitución (S)	3	Está conformado por equipos de tecnología importada y de elevada inversión.
Profundidad (P)	3	Existiría un clima hostil de los clientes hacia la empresa, que podría ser usado por la competencia
Extensión (E)	2	Afecta únicamente a los abonados de dicha central (2,000 aprox.)
Agresión (A)	2	Los equipos están mantenidos periódicamente, sin embargo trabajan con energía eléctrica.
Vulnerabilidad (V)	2	El proceso de combustión de los materiales es lento y se cuenta con respuesta de los bomberos rápida.

Tabla A2.2 Análisis de Riesgo de Sabotaje en el Ambiente A

AMBIENTE A RIESGO SABOTAJE		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	3	Este ambiente es parte del proceso.
Sustitución (S)	3	Está conformado por equipos de tecnología importada y de elevada inversión.
Profundidad (P)	3	Existiría un clima hostil de los clientes hacia la empresa, que podría ser usado por la competencia
Extensión (E)	2	Afecta únicamente a los abonados de dicha central (2,000 aprox.)
Agresión (A)	2	Existe un alto índice de delincuencia, una relación empleado - empleador no muy buena y falta de control a las contratistas.
Vulnerabilidad (V)	2	El local está situado a distancias cortas de la estaciones policiales. Está cercado, tiene portones metálicos. Sin embargo el acceso a personal autorizado no determina que éste pueda sabotear fácilmente el proceso.

Tabla A2.3 Análisis de Riesgo de Fraude en el Ambiente A

AMBIENTE A RIESGO FRAUDE		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	1	Al intervenir la línea de un cliente, sólo se disminuye la capacidad libre del ancho de banda en ese instante en la línea troncal. Es decir el daño no es permanente, ni afecta el servicio a los otros clientes.
Sustitución (S)	1	En este caso el bien a sustituir sería el costo de la llamada fraudulenta. Por lo tanto este costo y el tiempo de cubrirlo es mínimo comparándolo con los ingresos netos de esta instalación remota.
Profundidad (P)	2	Los reclamos constantes de los clientes pueden generar condiciones favorables a la competencia.
Extensión (E)	1	Afecta a un número mínimo de clientes.
Agresión (A)	1	Los fraudes son mucho más fáciles de cometer en las líneas aéreas (planta externa) y menos fáciles de rastrear. Las empresas de telecomunicación cuentan con sistemas que detectan la ocurrencia de un posible fraude.
Vulnerabilidad (V)	2	Se produciría daño, pues la empresa dejaría de percibir ingresos y debería cubrir los gastos de las llamadas efectivamente comprobadas como fraudulentas, con lo cual la empresa tendría doble perjuicio.

Tabla A2.4 Análisis de Riesgo de Incendio en el Ambiente B

AMBIENTE B RIESGO INCENDIO		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	3	Este ambiente es parte secuencial del proceso.
Sustitución (S)	3	Está conformado por equipos de tecnología importada y de elevada inversión.
Profundidad (P)	3	Existiría un clima hostil de los clientes hacia la empresa, que podría ser usado por la competencia
Extensión (E)	2	Afecta únicamente a los abonados de dicha central (2,000 aprox.)
Agresión (A)	1	Los equipos operan con niveles bajos de voltaje, con mínimo riesgo de incendio.
Vulnerabilidad (V)	2	El proceso de combustión de los materiales es lento y se cuenta con respuesta de los bomberos rápida.

Tabla A2.5 Análisis de Riesgo de Sabotaje en el Ambiente B

AMBIENTE B RIESGO SABOTAJE		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	3	Este ambiente es parte secuencial del proceso.
Sustitución (S)	3	Está conformado por equipos de tecnología importada y de elevada inversión.
Profundidad (P)	3	Existiría un clima hostil de los clientes hacia la empresa, que podría ser usado por la competencia
Extensión (E)	2	Afecta únicamente a los abonados de dicha central (2,000´aprox.)
Agresión (A)	2	Existe un alto índice de delincuencia, una relación empleado-empleador no muy buena y falta de control a las contratistas reconocidas o de prestigio.
Vulnerabilidad (V)	2	El local está situado a distancias cortas de la estaciones policiales. Está cercado, tiene portones metálicos. Sin embargo el acceso a personal autorizado no determina que éste pueda sabotear fácilmente el proceso.

Tabla A2.6 Análisis de Riesgo de Incendio en la Sala Grupo Electrógeno

AMBIENTE SALA DE GRUPO ELECTRÓGENO RIESGO INCENDIO		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	2	Este ambiente es parte secundaria del proceso, pues se usa sólo en caso de caída de energía eléctrica del exterior, y sólo por un determinado tiempo.
Sustitución (S)	2	Se alquilaría un equipo móvil electrógeno para un determinado tiempo, dependiendo del daño causado.
Profundidad (P)	2	Puede ser utilizado por el sindicato o agrupación de trabajadores descontentos con la seguridad de vida de los trabajadores.
Extensión (E)	2	Podría afectar a los locales circundantes a la instalación remota
Agresión (A)	3	Dentro de este ambiente se encuentra material altamente combustible, como el petróleo y los equipos trabajan con altas cargas de energía.
Vulnerabilidad (V)	3	El fuego, debido al líquido combustible, se extendería rápidamente.

Tabla A2.7 Análisis de Riesgo de Robo en la Sala Grupo Electrógeno

AMBIENTE SALA DE GRUPO ELECTRÓGENO RIESGO ROBO		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	2	Este ambiente es parte secundaria del proceso, pues se usa sólo en caso de caída de energía eléctrica del exterior, y sólo por un determinado tiempo.
Sustitución (S)	1	El reemplazo de los equipos que conforman esta sala es inmediato, fácil y a un costo bajo.
Profundidad (P)	2	En caso de alguna emergencia podría afectar a los clientes por no encontrarse operativo el servicio.
Extensión (E)	2	En caso de alguna emergencia podría afectar a los clientes por no encontrarse operativo el servicio.
Agresión (A)	2	Son piezas de fácil comercialización y de fácil movilización en una zona de alta delincuencia.
Vulnerabilidad (V)	2	El equipo puede quedar fácilmente inoperativo por el robo de algunas piezas.

Tabla A2.8 Análisis de Riesgo de Sabotaje en la Sala Grupo Electrógeno

AMBIENTE SALA GRUPO ELECTRÓGENO RIESGO SABOTAJE		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	2	Este ambiente es parte secundaria del proceso, pues se usa sólo en caso de caída de energía eléctrica del exterior, y sólo por un determinado tiempo.
Sustitución (S)	1	La reparación y/o la adquisición de repuestos para los equipos que conforman esta sala es inmediato, fácil y a un costo bajo.
Profundidad (P)	2	En caso de alguna emergencia podría afectar a los clientes por no encontrarse operativo el servicio.
Extensión (E)	2	En caso de alguna emergencia podría afectar a los clientes por no encontrarse operativo el servicio.
Agresión (A)	2	Son equipos sin protecciones especiales
Vulnerabilidad (V)	2	El equipo puede quedar fácilmente inoperativo por el sabotaje de algunas piezas.

Tabla A2.9 Análisis de Riesgo de Incendio en la Sala Sub Estación Eléctrica

AMBIENTE SALA DE SUB-ESTACIÓN ELÉCTRICA RIESGO INCENDIO		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	2	Si bien el incendio de la sala de sub-estación detendría el proceso, la existencia del grupo electrógeno reduciría el efecto negativo sobre la normalidad del proceso.
Sustitución (S)	3	La reposición de los equipos componentes de esta sala es costosa y demanda un tiempo prudencial.
Profundidad (P)	2	Puede dejar sin comunicación a los clientes por el lapso que duren los reemplazos de los medios secundarios de energía, causando una imagen de mal servicio al cliente.
Extensión (E)	2	La cantidad de clientes afectados podría ser : todos, aunque a intervalos.
Agresión (A)	3	La existencia de altos voltajes y el refrigerante combustible pueden generar incendios de grandes proporciones.
Vulnerabilidad (V)	3	Las llamas afectarían totalmente al equipo, eliminando el medio primario de energía. Además, las llamas podrían propagarse y generar explosiones.

Tabla A2.10 Análisis de Riesgo de Sabotaje en la Sala Sub Estación Eléctrica

AMBIENTE SALA DE SUB-ESTACIÓN ELÉCTRICA RIESGO SABOTAJE		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	2	Si bien el incendio de la sala de sub-estación detendría el proceso, la existencia del grupo electrógeno reduciría el efecto negativo sobre la normalidad del proceso.
Sustitución (S)	3	La reposición y/o reparación de los equipos componentes de esta sala es costosa y demanda un tiempo prudencial.
Profundidad (P)	2	Puede dejar sin comunicación a los clientes por el lapso que duren los reemplazos de los medios secundarios de energía, causando una imagen de mal servicio al cliente.
Extensión (E)	2	La cantidad de clientes afectados podría ser : todos, aunque a intervalos.
Agresión (A)	1	El sabotaje de este tipo de equipos es muy riesgos y se encuentra dentro de una ambiente cerrado en el interior de la instalación remota
Vulnerabilidad (V)	2	EL daño podría ser aminorado por el uso de medios de energía secundario.

Tabla A2.11 Análisis de Riesgo de Incendio en el Patio

AMBIENTE PATIO RIESGO INCENDIO		
CRITERIO DE	**VALOR**	**JUSTIFICACIÓN**
Función (F)	1	El patio no forma parte del proceso secuencial de funcionamiento de una instalación remota
Sustitución (S)	1	El bien que se incendiaría sería el combustible del tanque; el cual es fácil de reponer y a un costo relativamente bajo.
Profundidad (P)	2	Los gases calientes podrían ingresar a las salas de equipos y dañar progresivamente el servicio a los clientes.
Extensión (E)	1	Sólo podría afectar a las casas habitadas a su alrededor, ya que no cuenta con techo.
Agresión (A)	2	Existe material combustible, pero está protegido por una tanque normado.
Vulnerabilidad (V)	1	Ardería el material combustible hasta agotarse, sin posibilidad de expandirse. El incendio estaría focalizado.

Tabla A2.12 Análisis de Riesgo de Robo en el Patio

AMBIENTE PATIO RIESGO ROBO		
CRITERIO	**VALOR**	**JUSTIFICACIÓN**
Función (F)	1	El patio no forma parte del proceso secuencial de funcionamiento de una instalación remota
Sustitución (S)	1	El bien sujeto a robo sería el combustible del tanque; el cual es fácil de reponer y a un costo relativamente bajo.
Profundidad (P)	1	La ocurrencia del robo no sería percatado por los clientes.
Extensión (E)	1	No afectaría a ningún cliente.
Agresión (A)	2	Existe alto índice de delincuencia y el bien (combustible D-2) es de fácil comercialización y movilización sistemática.
Vulnerabilidad (V)	1	Afectaría mínimamente a los ingresos de la empresa por su bajo valor en comparación a los ingresos.

ANEXO 03

DISTORCIÓN DE FACTORES HUMANOS QUE DISMINUYEN LA EFICIENCIA DEL SERVICIO DE VIGILANCIA FIJA

El hombre, como factor básico del sistema de seguridad, es un complejo elemento en sí mismo. En él inciden características antropológicas, psicológicas y sociológicas, y situaciones de tipo económico y de idiosincrasias de grupo.

No es el caso del presente estudio, realizar una investigación profunda sobre el particular, tareas que pertenecen al campo del psicólogo y del sociólogo; por lo tanto se limitará a dar una semblanza de aquellos factores que intervienen de modo importante sobre el elemento individuo, a fin de analizar la protección de las instalaciones contra las deficiencias por los factores humanas que influyan negativamente en la generación de riesgos o situaciones de conflicto.

La biología humana que estudia la anatomía, como la fisiología y la sicología, da pautas de posible comportamiento del individuo, frente a la actividad que desarrolla. Y es en este campo, que al relacionarse con otros elementos surgen las variaciones de disfuncionamiento y crean la situación de riesgo.

A3.1 FACTORES FISIÓLOGICOS

El hombre tiene la necesidad de cierta energía que su organismo consume al momento de realizar cualquier actividad. Un aumento sensible de esfuerzo, incide en la elevación de la frecuencia cardiaca, y del sistema nervioso. El cuerpo humano reacciona en forma análoga ante situaciones conflictivas tanto de factores externos tipo físicos, o de origen psíquico. Por otra parte, el organismo humano pasa por una serie de etapas, y condicionamientos, lo que determina que la capacidad de trabajo varíe según la talla, la edad, el sexo, la alimentación, condiciones físicas, aptitudes y motivaciones, detallamos cada una de ellas:

- **La alimentación,** juega un papel esencial en el comportamiento físico de la persona; según ergonomistas, existen técnicas que permiten medir el esfuerzo físico y el gasto de energía en kilocalorías por hora, independientemente de la forma de actividad ejercida. Un agente de vigilancia mal alimentado son causa de bajo rendimiento.

- **Las dimensiones antropométricas,** juegan un papel preponderante en el aspecto dimensional de los puestos de trabajo, a fin de conseguir una mejor adaptación y maniobrabilidad en los mismos. Para que el trabajo del agente de vigilancia sea eficaz, es necesario que controle las diferentes situaciones mediante los sentidos del oído, la vista y el tacto.

- **Los sonidos,** que escapan de los límites admisibles, bien no pueden ser detectados, causa indirecta del bajo rendimiento.

- **La vista**, con la edad disminuye la adaptación a la oscuridad, y se necesita mayor claridad para el trabajo, pero generalmente los delincuentes prefieren acceder a las instalaciones por ambientes oscuros, lo cual es causa de bajo rendimiento.

- **Respecto a la capacidad física,** está comprobado que la fuerza muscular, la capacidad sensorio motora, la capacidad de retención disminuye a medida que pasan los años, todos estos fenómenos acarrean consecuencias graves en el desempeño de la tareas, es así como un vigilante de avanzada edad tratará de mantener su misma eficacia, pero cometerá mayores errores; de lo contrario, disminuirá éstos, y por ende su rendimiento.

- **La fatiga física,** presenta variaciones considerables en relación con los cambios de las condiciones exteriores, particularmente con el aspecto de la moral; y va acompañada de otros síntomas subjetivos, como la irritabilidad, el egocentrismo, la disconformidad, falta de motivación, y otros. Estos efectos constituyen un primer factor de predisposición en la consecuencia de los conflictos, aún más si se tiene en consideración que la exposición a los riesgos es extremadamente variable.

A3.1.1 POSIBLES CAUSAS DE CONFLICTOS DEBIDOS AL FACTOR FISIOLÓGICO

- Pérdida de eficiencia física, por deficiente régimen alimenticio
- Fatiga física
- Características antropométricas fuera de lo común, no de acuerdo con el puesto de trabajo, para hacer frente a los delincuentes
- Edad, que incide en general sobre cualquier actividad
- Disminución general de los sentidos principales

A3.2 FACTORES PSICOLÓGICOS

Desde la perspectiva del factor humano, la empresa viene hacer un conglomerado de diferentes grupos, con motivaciones, pautas de conducta,

status y formación cultural diferentes; no obstante todos convergen hacia un objetivo final, desde el punto de vista económico, para subsistir.

Si se considera que la experiencia de un individuo es el resultado de su preparación, educación familiar, de la influencia del medio y de la imitación del comportamiento de otros, más de una vez su comportamiento puede ser equivocado con respecto a determinada situación.

Desde el punto de vista de la seguridad los vigilantes no ven de manera igual una misma situación; o sobrestiman o subestiman los hechos. Los vigilantes antiguos y experimentados; se aferra a sus propios métodos y procedimientos y se dejan llevar por la llamada fuerza de la costumbre. Detallamos los factores psicológicos:

- **El carácter,** es la expresión externa de los factores potenciales, pensamiento, sentimiento y movimiento, en forma de reacción ante las situaciones tanto internas del propio yo como de las externas al individuo y que se presentan como estímulos mediatos e inmediatos, y actúan sobre el yo integrado.

- **Conducta,** no es otra cosa que la reacción en el individuo para satisfacer sus necesidades, y puede o no producir sensaciones y experiencias agradables y positivas, o experiencias negativas generando en ambos casos hábitos o condicionamiento que le convierten en una norma o regla de conducta. Son formas específicas adoptadas, ya sean innatas o adquiridas y que el individuo emplea de un modo habitual, las cuales utiliza el individuo para desarrollar su comportamiento, eligiendo aquella combinación que considera más adecuada en cada momento de acuerdo con sus necesidades y motivaciones en general. Al no alcanzar los objetivos deseados pueden dar lugar a una serie de tipos de conducta de tipo racional o de tipo perjudicial. La conducta ante la frustración, es la

que se produce cuando aparece algún problema que afecte negativamente a la imagen del yo.

- **Motivación,** No es otra cosa que la incentivación, la conducta del hombre es causada, dirigida a objetivos. El hombre espera que su trabajo además de la satisfacción de sus necesidades básicas otras de tipo personal y social como por ejemplo, posibilidad de ejercer su iniciativa, necesidad de relacionarse con otras personas, sentirse copartícipe de la utilidad del trabajo, trabajar en condiciones de seguridad e higiene, etc.

- Si el trabajador no llega a un resultado favorable en su trabajo, tratará de encontrarlo. Este resultado improductivo podría llegar a ser, inclusive contra productivo (apatías, indiferencia y falta de desenvolvimiento).

A3.2.1 POSIBLES CAUSAS DE CONFLICTOS DEBIDO AL FACTOR PSICOLÓGICO

- Exceso incontrolado de dinamismo
- Fuerza de la costumbre
- Insatisfacción en las necesidades básicas
- Inseguridad en el medio de trabajo
- Falta de autorrealización
- Apatía por falta de desenvolvimiento
- Inestabilidad en el trabajo
- Remuneración injusta
- Indiferencia al no sentirse importante y responsable
- Irritación por el exceso de control
- Resentimiento por su falta de participación
- Desmoralización por su no valoración humana

A3.3 FACTOR SOCIOLÓGICO

El factor sociológico puede ser visto desde dos ángulos diferentes:

- Desde el ángulo interno, o sea del medio de trabajo, en el cual el individuo es influenciado por la reacción del grupo, y su entorno.
- Desde el ángulo externo, o fuera de su trabajo en el cual el individuo sufre la influencia del medio en que se desarrolla, los problemas familiares, las costumbres del status al que pertenece, grado de cultura y sus creencias religiosas.

Los problemas de tipo social, influyen por tanto en la comunicación de los individuos, en sus responsabilidades.

El aspecto económico se añade como elemento disociador en el factor sociológico, y es causa muchas veces de malos hábitos y de vicios adquiridos.

A3.3.1 POSIBLES CAUSAS DE CONFLICTOS DEBIDAS AL FACTOR SOCIOLÓGICO

- Disminución de la moral
- Malos hábitos
- Problemas familiares
- Irresponsabilidad, como resultado de falta de cultura
- Sentimientos negativos incontrolados por causa del medio en que se desarrolla el individuo
- Prejuicios, debidos a falsas supersticiones
- Negligencia, por falta de una seguridad ocupacional
- Inseguridad en el trabajo, por falta de medidas de seguridad e higiene
- Corrientes filosóficas o políticas con aspectos de descontento y rebeldía.

A3.4 FACTOR ORGANIZACIÓN

Existen una serie de definiciones sobre organización; considerada por algunos como el conjunto de relaciones formales y/o informales dentro y fuera de la empresa y que tienen relación con el comportamiento de los individuos; otros consideran la organización como un sistema estructural; de todos modos las técnicas de análisis de una organización, determinan ciertos factores inherentes a la misma, como: estructuración de actividades, control, autoridad, servicios, etc.

A3.4.1 POSIBLES CAUSAS DE CONFLICTOS DEBIDAS AL FACTOR ORGANIZACIÓN

- Incertidumbre por falta de limitación de autoridad
- Desconocimiento de normas y procedimientos por falta de comunicación
- Mala interpretación de datos por errores en las comunicación.
- Confusión debido a una mala delimitación de la autoridad
- Subordinación múltiple
- Falta de responsabilidad, debida a una inadecuada distribución de funciones
- Incomprensión entre directivos y subordinados
- Despersonalización, debido al exceso de automatismo

ANEXO 04

ANÁLISIS ECONÓMICO DEL SISTEMA DE SEGURIDAD TRADICIONAL

El Sistema de Seguridad Tradicional es implantado por muchas empresas sin realizar ningún análisis y evaluación de riesgos, para la protección de sus edificios, éste sistema de protección cuenta en sus instalaciones únicamente con el servicio de vigilancia fija comúnmente conocidos como agentes de vigilancia o guardianes, quienes se encargaran de cumplir con los requisitos de las 4 D's de la Seguridad que son la Demorar, Disuadir, Detener y Detectar; en otras palabras, la seguridad de está únicamente a cargo de seres humanos, apoyado en su propia intuición, capacitación, en barreras físicas simples y extintores manuales.

Para poder controlar el trabajo de los agentes de vigilancia en instalaciones remotas se debe contar con inspectores de seguridad, quienes se encargarán de visitar los locales en forma periódica, para verificar si se están cumpliendo con las consignas y obligaciones. Por la cantidad de locales que están en estudio de esta tesis (aproximadamente 200) y porque cada inspector contará con un número grande de locales (mayor a 50) a su cargo necesitará para trasladarse camionetas.

Ante cualquier evento o siniestro el agente de vigilancia deberá comunicar las novedades a una Central de Control por teléfono (teléfono asignado en su garita de vigilancia), de tal manera que la persona que cumple la función de operador de la Central de Control realice las

coordinaciones correspondientes con las unidades de apoyo externo (bomberos, policías, etc.) o internos con el fin de coadyuvar en las funciones del vigilante.

En el presente estudio, por la dimensión del área y el número de plantas de la Instalación Remota de Uso Telefónico, se ha asumido para su protección ante cualquier siniestro y para el control de accesos de un agente de vigilancia.

La Central de Control contará con dos teléfonos para poder recibir la información de los agentes de vigilancia y así mismo para poder realizar las coordinaciones, además deberá contar con una computadora e impresora para poder realizar los informes y las autorizaciones respectivas, así mismo para mantener información de los locales.

Los montos de inversión y gastos que aquí se presentan corresponden al sistema de seguridad tradicional para que luego dicha información se registre en la evaluación económica mostrada en la tabla 7.2 del capítulo VII. Es muy importante destacar que estas determinaciones de costos se hicieron en los meses finales de 1,999.

Tabla A4.1 Costo del Puesto de Operador de la Central de Control

Cantidad de Puestos	1	Puesto
Costo del Servicio	1,40	Dólares /Hora
Horas / Puesto	24	Horas/Día
Días / Semana	7	Días
Semanas / Año	52	Semanas

Fuente : Empresa de Vigilancia SEGUROC S.A.

Tabla A4.2 Costo del puesto de Inspección

Cantidad de Puestos	2	Puestos
Costo del Servicio	1.200	Dólares/ Mes
Horas / Puesto	8	Horas/Día
Días / Semana	5	Días
Meses / Año	12	Meses

Fuente : Empresa de Vigilancia SEGUROC S.A.

Tabla A4.3: Costo del Puesto de Vigilancia Fija

Cantidad de Puestos	1	Puesto / Instalación
Costo del Servicio	1,2	Dólares / Hora
Horas / Puesto	24	Horas / Día
Días / Semana	7	Días
Semanas / Año	52	Semanas

Fuente : Empresa de Vigilancia SEGUROC S.A.

Tabla A4.4 Resumen Gasto Anual Servicio Vigilancia Humana US $)

PUESTO	MONTO
Operador	12.230,40
Inspectores	28.800,00
Vigilancia Fija	10.483,20

Fuente : Empresa de Vigilancia SEGUROC S.A.

Tabla A4.5 Costo del Acondicionamiento de la Central de Control

(US $)

Servicio	Concepto	Cantidad	Costo Unitario Equipo	Costo Total Equipo	Costo Unitario Instalación	Costo Total Instalación
Iluminación	Luminarias	2	20	40	10	20
Decoración	Alfombras	1	300	300	50	50
	Pintado	1	0	0	100	100
Mobiliario	Mesa	1	150	150	20	20
	Silla	1	50	50		0
	Estante	1	200	200		0
Fontanería		1	500	500	200	200
Instalación Eléctrica		1			1.000	1.000
Total				1.240		1.390

Fuente : Elaboración Propia

Tabla A4.6 Costo del Sistema de Comunicación de la Central de Control

(US $)

Concepto	Descripción	Cantidad	Precio Unitario	Costo Total
Línea Telefónica	RTC	2	200	400
Total				**400**

Fuente : Telefónica del Perú S.A.A.

Tabla A4.7: Costo de Instalaciones Especificas Central Control

(US $)

Concepto	Descripción	Cantidad	Precio Unitario	Costo Total
Sistema Informático	Impresora	1	200	200
	Computadora	1	800	800
Total				1.000

Fuente : Datacont S.A., representante de Canon

Tabla A4.8 Costo del Sistema de Comunicaciones en las IRUT

(US $)

Concepto	Descripción	Cantidad	Costo Unitario Instalación	Costo Total Instalación
Comunicaciones	Teléfono	1	200	200
Total				**200**

Fuente :Telefónica del Perú S.A.A.

Tabla A4.9 Costo de Instalación Especifica Física en las IRUT

(US $)

Concepto	Equipo	Cant.	Costo Unitario Equipos	Costo Total Equipos	Costo Unitario Instalación	Costo Total Instalación
Protección Contra Intrusión/ Sabotaje	Puertas	5	100	500	50	250
Protección Contra Incendio	Extintores	4	200	800	20	800
Garita de Vigilancia		1	1000	1000	500	500
Total				2300		1550

Fuente : Elaboración Propia

Tabla A4.10 Otras Inversiones

(US $)

Concepto	Descripción	Cantidad	Costo Unitario	Costo Total
Movilidad para Inspección	Camionetas	2	10.000	20.000

Fuente : Toyota Hernes

Tabla A4.11 Costo de Mantenimiento para la Central de Control

(US $)

Concepto	Valor Inicial	Porcentaje Mantenimiento	Costo De Mantenimiento
Acondicionamiento	1.240	3%	37,20
Instalaciones Especificas de la Central de Control	1.000	3%	30,00
Comunicación	400	10%	40,00
Total			**107,20**

Fuente : Elaboración Propia en base a información del proveedor

Tabla A4.12 Costo de Mantenimiento para la IRUT

(US $)

Concepto	Valor Inicial	Porcentaje Mantenimiento	Costo de Mantenimiento
Protección Física	3850	3%	115,5
Comunicación	200	10%	20
Total			135,5

Fuente : Elaboración Propia en base a información del proveedor

Tabla A4.13 Costo del Mantenimiento de Otras Inversiones

(US $)

Concepto	Valor Inicial	Porcentaje Mantenimiento	Costo de Mantenimiento
Camioneta	20.000	5%	1.000
Total			**1.000**

Fuente : Elaboración Propia en base a información del proveedor

Tabla A4.14 Depreciación en la Central de Control

(US $)

Concepto	Inversión Inicial	Tasa %	Periodos Anuales					Valor Residual
			1	2	3	4	5	
Acondicionamiento	1240	10%	124	124	124	124	124	620
Total			**124**	**124**	**124**	**124**	**124**	**620**

Fuente : Elaboración Propia

Tabla A4.15 Depreciación en las IRUT

(US $)

Concepto	Inversión Inicial	Tasa %	Periodos Anuales					Valor Residual
			1	2	3	4	5	
Protección Contra Intrusión/Sabotaje	500	10%	50	50	50	50	50	250
Protección Contra Incendio	800	10%	80	80	80	80	80	400
Garita de Vigilancia	1000	3%	30	30	30	30	30	850
Total			**160**	**160**	**160**	**160**	**160**	**1.500**

Fuente : Elaboración Propia

Tabla A4.16: Depreciación de Otras Inversiones

(US $)

Concepto	Inversión Inicial	Tasa %	Periodos Anuales					Valor Residual
			1	2	3	4	5	
Camioneta	20.000	10%	2.000	2.000	2.000	2.000	2.000	10.000
Total			**2.000**	**2.000**	**2.000**	**2.000**	**2.000**	**10.000**

Fuente : Elaboración Propia

Tabla A4.17 Parámetros Consumo de Energía Sistemas Informáticos en la Central de Control

Cantidad de Equipos	1	Computadora
Consumo / Hora	175	Watts
Horas / Día	24	Horas
Días / Semana	7	Días
Semanas / Año	52	Semanas
Costo Kw/Hora	0,11	Dólares

Fuente : Osinerg

Tabla A4.18 Parámetros Consumo de Energía por Iluminación Central de Control

Cantidad de Equipos	2	Luminarias
Consumo / Hora	100	Watts
Horas / Día	12	Horas
Días A La Semana	7	Días
Semanas / Año	52	Semanas
Costo Kw - Hora	0,11	Dólares

Fuente : Osinerg

Tabla A4.19 Resumen del Costo Anual por Energía de la Central de Control

(US $)

Concepto	Monto
Sistema Informáticos	168,17
Iluminación	96,10
Total	**264,26**

Fuente : Osinerg

Tabla A4.20: Gasto Anual por Consumo de Comunicaciones Telefónicas

(US $)

Reporte de Novedades	3 Veces por día
Establecimiento de Llamadas	0,14
Consumo de Llamada	0,14
Dias por Año	365
Total por instalación remota	**306,60**

Fuente : Telefónica del Perú S.A.A

Tabla A4.21: Otros Costos Anuales de la Central de Control

(US $)

Concepto	Cantidad	Unidades	Costo Unitario	Costo Total
Disquetes	24	Cajas	5	120
Cintas de Impresora	2	Unidades	10	20
Utiles de Oficina	2	Unidades	10	20
Gastos de Oficina	1		100	100
Total				**260**

Fuente : Elaboración Propia

Tabla A4.22: Costo de Combustible para la Inspección de las IRUT (US $)

Concepto	Cantidad	Costo Unitario	Costo Total
Combustible	2	3.600	7.200
Total			**7.200**

Fuente : Elaboración Propia

Tabla A.23 Determinación de la Prima de Seguro por Sabotaje en la Subestación Eléctrica (US $)

Estimado de las Pérdidas Potenciales por Instalación	Costo de Reemplazo Permanente (Inversión Fija: Valor del Bien)	50.000,00
	Costo de Reemplazo (Inversión Intangible: Instalación)	5.000,00
	Costo de Sustitución Temporal	0,00
	Costo de Perdidas Relacionadas: Pagos Por Servicios	1.100,00
	Costo de Pérdidas en Inversiones que Generan Ingresos (Lucro Cesante)	50.000,00
	Total pérdidas	55.000,00
Reconocido		55.000,00
Deducible	33%	18.150,00
Indemnización		36.850,00
Prima de Seguro	0.67%	**368.50**

Fuente : Elaboración propia

GLOSARIO

- **AGENTE VIGILANTE**.- Persona que se encarga de custodiar o proteger un bien.
- **ALARMA**.- Estado de activación de un dispositivo de seguridad.
- **AMENAZA**.- Se define como la habilidad o intento de una acción o evento para afectar adversamente un activo, o un amplio rango de fuerzas que pueden producir un resultado adverso.
- **ASEGURADOR**.- Es la entidad o persona jurídica llamada compañía de seguros que emite la póliza y se compromete a cubrir el riesgo o asume el peso del riesgo en su capacidad de suscriptor con el objeto de indemnizar o reparar el daño o la pérdida cuando estos ocurran.
- **BIEN**.- Un elemento que tenga valor económico.
- **CIRCUITO CERRADO DE TELEVISIÓN (C.C.T.V.)**.- Sistema de transmisión y distribución de señales de T.V.
- **COBERTURA**.- Es sinónimo de garantía. Compromiso aceptado por el asegurador para hacerse cargo de las consecuencias económicas derivadas de un suceso desfavorable. Es el amparo de un daño o pérdida.
- **C.R.A.T.**.- Centro de Recepción de Alarmas y Teleservicios.
- **DEDUCIBLE**.- Es una cantidad parcial fija o porcentaje de la suma asegurada o del importe total de siniestro que corre a cargo del asegurado en cada reclamo de éste.
- **INDEMNIZACIÓN**.- Importe que esta obligado a pagar el asegurador en caso de producirse un siniestro

- **INTRUSIÓN**.- Evento que describe el acceso de una persona, no deseado o no comunicado.
- **MEDIDAS DE SEGURIDAD**.- O contramedidas, son el conjunto de elementos de seguridad Físicas, Electrónicas, Humanas y Económicas que tiene como misión disminuir la vulnerabilidad del sistema de seguridad.
- **MEDIDAS DE SEGURIDAD TECNICAS**.- Es un conjunto de elementos técnicos físicos o electrónicos destinados a demorar o advertir localmente y/o a distancia de cualquier incidencia que pueda representar un riesgo para las vidas, bienes o continuidad de actividades.
- **PÉRDIDAS**.- Las pérdidas se crean mediante la activación exitosa de una de las amenazas, es decir, la amenaza a creado una pérdida debido a nuestra vulnerabilidad hacia ella. Las pérdidas se clasifican en dos categorías. A la primera se le llama Pérdida inmediata o Directa (el daño al bien afectado) y la asegunda es la pérdida consecuente o indirecta (el daño a las operaciones conexas y/o usos del bien).
- **POLIZA**.- Contrato del seguro mediante el cual una de las partes (compañía de seguros o asegurador) conviene en proteger un bien, una propiedad, la vida, etc.
- **PREVENCIÓN DE RIESGOS**.- Es la serie de actos encaminados a impedir que el hecho temido se produzca, y en caso de ocurrir, lograr que sus consecuencias sean lo menos dañosas posible.
- **PRIMA DE SEGURO**.- Es la contraprestación pecuniaria que el asegurado o contratante paga al asegurador en retribución de la cobertura a cargo del último. Por lo general se paga para una cobertura anual.
- **R.T.C.**.- (Red Telefónica Conmutada). Es un canal de comunicación cuya forma de interconexión entre dos puntos, no es permanente o dedicada.
- **RIESGO**.- Se define como un evento futuro, y por lo tanto incierto, que podría tener un efecto adverso en operaciones beneficiosas. Es una medida probabilística, es decir responde a la pregunta ¿qué tan probable es que una amenaza se convierta en daño?.

- **SABOTAJE**.- Estado de avería de un dispositivo o de los cables que conectan a este con la fuente o nodo de control.
- **SEGURIDAD**.- puede ser comprendida como un estado ideal o de perfecto equilibrio con el medio ambiente; equilibrio que para ser mantenido requiere de la implantación de medidas autoregulatorias continuas de protección que respondan con aciones correctivas inmediatas a las amenazas.
- **SEGURIDAD TRADICIONAL**.- Es el sistema de seguridad basado únicamente en empleo de agentes vigilantes o guardianes para la protección del bien.
- **SIIS**.- Sistema Integral Inteligente de Seguridad. Sistema de seguridad que reúne las diversas medidas de seguridad (físicas, electrónicas, humanas, económicas)
- **SINIESTRO**.- Acontecimiento, suceso o materialización del riesgo.
- **VULNERABILIDAD**.- Es una medición del estado de la seguridad frente a la ocurrencia de una amenaza, es decir, nos permite responder a la pregunta ¿qué pasa si determinada amenaza se presenta ahora?

BIBLIOGRAFÍA

Libro : Evaluación de Proyectos
Autor : Gabriel Baca Urbina
Edición : Tercera - Perú 1997
Editorial : Mcgraw Hill

Libro : Seguridad Industrial "Normas, Técnicas y Procedimientos Administrativos
Autor : Mario Ibañez Machicao
Edición : Primera - Perú 1996
Editorial : Concytec

Libro : Programa de Alta Dirección de Seguridad
Autor : Varios
Edición : Primera - España 1999
Editorial : Universidad Pontificia Comillas Madrid

Libro : I Jornada Internacional de Seguridad
Autor : Bureau Internacional de Información y Negocios
Edición : Primera - España 1998
Editorial : Bureau Internacional de Información y Negocios

Libro : Bases Técnicas de la Vigilancia Privada
Autor : Empresa Service Company Seguridad
Edición : Primera - Perú 1999

Libro : Seminario "Prevención Protección en Operadoras Telefónicas"
Autor : Allianz Casiopea Re
Edición : Primera - Perú 1997
Editorial : Allianz Casiopea Re - España

Libro : Norma Técnica Construcción de Edificios de Uso Telefónico
Autor : Telefónica del Perú
Edición : Primera - Perú 1997
Editorial : Sub Gerencia de Tecnología

Libro : Introducción a la Metodología de La Investigación
Autor : Roberto Avila Acosta
Edición : Primera - Perú 1997
Editorial : Estudios y Ediciones Perú

Libro : Modulo de Impartición Técnica
Autor : Telefónica del Perú Red de Clientes
Edición : Primera - Perú 1998
Editorial : Gerencia de Operación y Mantenimiento

Libro : Seguridad Industrial un Enfoque Integral
Autor : Cesar Ramírez Cavassa
Edición : Segunda - Perú 1996
Editorial : Limusa - Noriega

Libro : Risk Analysis And The Security Survey
Autor : James F. Broder
Edición : Primera - EE. UU 1984
Editorial : Butterworth - Heinemann

Libro : II Conferencia Tecnología Avanzada en Seguridad Electrónica
Autor : Empresa Seguridad Optima S.C.
Edición : Primera - Perú 95
Editorial : Empresa Seguridad Optima S.C.

Libro : Manual de Evaluación y Administración de Riesgos
Autor : Rao Kolluru
Edición : Primera - E.E.U.U 1998
Editorial : Mc Graw Hill