



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

**SISTEMA DE SEGURIDAD INTEGRAL PARA GENERICA S.A**



ALVARO HERNAN POVEDA VELASCO

13.722.178

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS ADMINISTRATIVAS Y NEGOCIOS  
POSGRADO EN GESTION DE PROYECTOS**

BOGOTA

2013



UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)

## **SISTEMA DE SEGURIDAD INTEGRAL PARA GENERICA S.A**



ALVARO HERNAN POVEDA VELASCO

Tesis de grado

Director de proyecto:

Carlos Eduardo Díaz Gil

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**  
**ESCUELA DE CIENCIAS ADMINISTRATIVAS Y NEGOCIOS**  
**POSGRADO EN GESTION DE PROYECTOS**

BOGOTA

2013



## **NOTA DE ACEPTACION**

Tesis de grado titulada SISTEMA DE SEGURIDAD INTEGRAL PARA GENERICA S.A del autor Álvaro Hernán Poveda Velasco, cumple con los requisitos para optar el título de Especialización en Gerencia de Proyectos.

DOCTOR CARLOS EDUARDO DÍAZ GIL

Director de proyecto.

DOCTOR EDGAR RODRIGUEZ AFANADOR

Jurado calificador.

Bucaramanga, 5 de noviembre de 2013



## **DEDICATORIA**

A mi madre quién desde mis primeros años de vida me inculcó la importancia de la educación para superarme y hacerme una persona de bien para la sociedad.

A mi esposa quién con su amor y apoyo incondicional ha estado a mi lado, pese a los inconvenientes y problemas que se presentaron, me ayudó con su comprensión, motivación para darme coraje en mi empeño y perseverancia de seguir adelante.

A mi hijo que se ha convertido en una inspiración para mí, es mi tesoro y fuente de amor que me ha ayudado a no desfallecer ante mis objetivos.



## **AGRADECIMIENTOS**

Esta tesis no hubiera sido posible sin el interés y ánimo que me ha dado una serie de personas y amigos. En especial, al doctor Carlos Eduardo Díaz Gil, quien amablemente compartió sus puntos de vista sobre el tema y me motivo a producir un trabajo que ofreciera claridad en la doctrina. También al doctor Edgar Rodríguez Afanador el cual clarificó muchas de mis dudas y representó una fuente invaluable de información y por último pero no la menos importante a la universidad nacional abierta y a distancia por la oportunidad y su flexibilidad de alcanzar otra meta en mi vida.



## CONTENIDO

<b>ÍNDICE FIGURAS</b> .....	<b>8</b>
<b>RESUMEN</b> .....	<b>11</b>
<b>INTRODUCCIÓN</b> .....	<b>13</b>
<b>JUSTIFICACION</b> .....	<b>15</b>
<b>GENERALIDADES DEL PROYECTO</b> .....	<b>16</b>
1.1 PLANTEAMIENTO DEL PROBLEMA .....	16
1.2 FORMULACION DEL PROBLEMA.....	17
1.3 SISTEMATIZACION DEL PROBLEMA.....	17
1.4 OBJETIVO .....	18
1.4.1 Objetivo Específicos.....	18
1.4.2 Objetivo Específicos.....	18
<b>2. MARCO TEORICO</b> .....	<b>19</b>
2.1 ANTECEDENTES .....	19
2.2 CONVIVENCIA Y SEGURIDAD CIUDADANA.....	20
<b>3. ASPECTOS METOLOGICOS</b> .....	<b>23</b>
<b>4. DESARROLLO DEL PROYECTO Y RESULTADO</b> .....	<b>24</b>
4.1 ALCANCE .....	28
4.2 PRINCIPIOS DE DISEÑO.....	28
4.3 INTEGRACIÓN DE PERSONAL, EQUIPOS Y PROCEDIMIENTOS .....	32
4.4 ORGANIGRAMA.....	34
4.5 DESCRIPCION GENERAL DE LA SOLUCION .....	34
4.5.1 Subsistema de Detección Perimetral. ....	36
4.5.1.2 En las ciudadelas y Clubes. ....	41
4.5.2 Subsistema de Verificación.....	44
4.5.2.1 Zona de producción y planta.....	48
4.5.2.2 En las ciudadelas y clubes.....	50



4.5.3 Subsistema de Vigilancia Específica.....	50
4.5.3.1 Control de acceso en Zona de producción y planta. ....	51
4.5.3.2 Acceso Peatonal. ....	51
4.5.4 Subsistema de Detección Interior. ....	53
4.5.5 Subsistema de Integración. ....	54
4.5.5.1 Arquitectura del Subsistema de Integración ....	61
4.5.6 Cuarto de Control Del Sistema De Seguridad Electrónico.....	63
4.5.7 Adecuaciones Locativas. ....	64
4.5.7.1 Instalaciones Eléctricas y equipos de Energía.....	65
4.5.7.2 Instalación de equipos del SSE. ....	65
4.5.7.3 Mobiliario para operadores. ....	66
4.5.7.4 Equipos de comunicaciones. ....	66
4.6 NIVELES DE SERVICIO OFRECIDOS.....	66
4.7 LISTADO DE EQUIPOS Y PROGRAMAS (SOFTWARE) ....	66
4.8 DESCRIPCIÓN DE LA INFRAESTRUCTURA Y CANTIDADES ....	67
4.8.1 Área técnica.....	68
4.9 COMUNICACIONES.....	70
4.9.1 Transmisión Inalámbrica de Videocámaras (Térmicas, Domos, Fijas). .	70
4.10 GRABACIÓN DIGITAL DVR'S Y PLATAFORMA DE ADMINISTRACIÓN DE VIDEO.....	71
4.11 CABLE SENSOR OMNITRAX.....	73
4.12 CABLE SENSOR INTELLIFLEX.....	74
4.13 UNIDADES PROCESADORAS DE INFORMACIÓN.....	74
4.14 COMUNICACIÓN ENTRE ZONA DE PRODUCCIÓN Y CIUDADELAS.	75
<b>5. ANÁLISIS FINANCIERO.....</b>	<b>75</b>
<b>6. CONCLUSIONES Y RECOMENDACIONES .....</b>	<b>79</b>
<b>7. BIBLIOGRAFIA.....</b>	<b>82</b>

## ÍNDICE FIGURAS

<b>Figura 1.</b> Base del modelo seguridad integral. Extraído del Pliego de licitación con Genérica S.A.....	33
<b>Figura 2.</b> Organigrama. Extraído del Contrato. ....	34
<b>Figura 3.</b> Configuración en RED de equipos OmniTrax – Integración con CCTV. Extraído del Manual de instalación cable Sensor Stellar Omnitrax.....	40
<b>Figura 4.</b> Instalación física en campo del equipo IntelliFlex. Extraído de Hoja técnica Sensor Stellar IntelliFlex.....	42
<b>Figura 5.</b> Sistema de detección perimetral solución para ciudadelas y clubes. Extraído del Manual instalación Sensor Stellar IntelliFlex.....	43
<b>Figura 6.</b> Control de acceso peatonal Planta. Extraído el del catálogo Astrophysics.....	52
<b>Figura 7.</b> Arquitectura Subsistema de Integración SSE. Autor.....	61
<b>Figura 8.</b> Configuración de equipos Sala de Control. Realizada por Autor. ....	64
<b>Figura 9.</b> Organigrama área de tecnología. Realizada por Autor. ....	69
<b>Figura 10.</b> Especificaciones Técnicas Verint S1100. Extraído de Hoja técnica de las antenas Verint S1100.....	71
<b>Figura 11.</b> Sistema de Detección de Intrusión. Extraído de Hoja técnica Sensor Stellar Omnitrax. ....	73

## GLOSARIO

**Seguridad:** El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

**Integral:** total que comprende todos los aspectos o partes necesarias para estar completo.

**Cronograma:** es, en gestión de proyectos, en una lista de todos los elementos terminales de un proyecto con sus fechas previstas de comienzo y final. Hay también herramientas libres y de código abierto para la generación de cronogramas de proyecto disponibles para la mayoría de plataformas, ofreciendo oportunidades para la creación de listas de tareas, la asignación de recursos, precedencias y diagramas de Gantt. y nos ayuda a ver desde un punto diferente.

**Sistemas análogos:** Se dice que un sistema es analógico cuando las magnitudes de la señal se representan mediante variables continuas, esto es análogas a las magnitudes que dan lugar a la generación de esta señal. Un sistema analógico contiene dispositivos que manipulan cantidades físicas representadas en forma analógica. En un sistema de este tipo, las cantidades varían sobre un intervalo continuo de valores.

**Sistemas Digitales:** Es cualquier dispositivo destinado a la generación, transmisión, procesamiento o almacenamiento de señales digitales. También un sistema digital es una combinación de dispositivos diseñado para manipular cantidades físicas o información que estén representadas en forma digital; es decir, que sólo puedan tomar valores discretos.



CCTV: Circuito Cerrado de Televisión.

Perímetro: Es la suma de las longitudes de los lados de una figura geométrica.

Talanquera: Valla, pared o cualquier lugar que sirve de defensa y protección.

Winpak: Programa diseñado para la administración de los equipos de control de acceso marca Honeywell.

Wiegand :El término del interface Wiegand es una marca de la sociedad “Sensor Engineering Company” y fue diseñado para conseguir una tecnología que permitiera transmitir datos de un identificador (tarjeta) entre dos dispositivos alejados entre sí, como, por ejemplo, un lector y la central de control de accesos. El protocolo Wiegand es ampliamente utilizado por la mayor parte de los fabricantes porque permite la transmisión de información a través de un par de cobre que se acompaña de la alimentación para el dispositivo de lectura si afectar por ello a los datos.



## RESUMEN

El proyecto de seguridad integral para la empresa Genérica S.A. inicia de suplir unas necesidades de seguridad que presenta en algunas áreas de su pertenencia, tomando como referencia los estudios de seguridad realizados con anterioridad y los eventos de pérdida, deciden realizar un plan de acción, dentro este plan de acción se contempla empezar un proceso de licitación para contratar una empresa contratista que debería encargarse de la solución del problema.

En este momento la empresa Seguridad Total S.A. inicia un proceso de entender la problemática de seguridad de la empresa a través de visita técnica a campo, entrevista a los operadores y supervisores de las áreas afectadas, también como realizar una intervención evitando traumatismo a la operación.

En la parte financiera y entendiendo que el proyecto debería tener una duración de cinco (5) años empezamos a realizar proyecciones calculando de cuenta serian la perdidas promedio durante este mismo periodo en comparación al valor de nuestra solución para el tiempo total del proyecto.

Debemos hacer énfasis en los efectos adicionales que se derivarían de este proyecto, como es evitar los enfrentamientos directos del personal de seguridad con intrusos en las áreas vigiladas, el reemplazo del personal vulnerable en algunas zonas por el sistema electrónico.

También apuntamos a encasillar nuestros sistemas y materiales de instalación bajo los estándares que se encuentran estipulados en la reglamentación nacional y con los protocolos propios de la empresa Genérica S.A.



La primera etapa para la inicialización del proyecto, es la realización ingeniería de detalle en donde realizamos el diseño, del cual se deriva el presupuesto y cronograma de ejecución de la obra.

Del cronograma se definirá los recursos de personal necesario para cumplir con las fechas propuestas en el mismo.

Por último en el documento detallaremos como escogimos y realizamos la mejor solución, tratando de hondar en cada una de sus partes, como es la escogencia de los equipos y la integración de estos con la parte de seguridad física.



## INTRODUCCIÓN

Realizando un recuento de la evolución de los sistemas de seguridad electrónica, inicialmente se encuentra los sistemas análogos llamados de esta forma por su forma de señal en la transmisión de datos, los cuales se conformaban de cámaras y video grabadoras análogas. Para entender mejor definiremos que es una señal análoga es un tipo de señal generada por algún tipo de fenómeno electromagnético y que es representable por una función matemática continua en la que es variable su amplitud y periodo (representando un dato de información) en función del tiempo. Algunas magnitudes físicas comúnmente portadoras de una señal de este tipo son eléctricas como la intensidad, la tensión y la potencia, pero también pueden ser hidráulicas como la presión, térmicas como la temperatura, mecánicas, etc.

En este sistema análogo su mayor cualidad es su definición de imágenes, pero no era suficiente compensación con su defectos, como era el almacenamiento de las cintas VHS las cuales ocupaban cuartos enteros, otro problema era el procesamiento de la grabaciones, es decir que no era de fácil manipulación por ejemplo la búsqueda de un evento en una hora, día, mes y año se volvía muy tediosa en casos donde apremiaba el tiempo.

Con la evolución de la tecnología en donde vemos cada vez discos duros con mayor capacidad de grabación, aparecen los sistemas digitales que vienen a solucionar los problemas del sistema análogo, las primeras grabadoras digitales salieron a la venta como tarjetas de videos instaladas en computadores comunes los cuales contenían un programa que administraba las señales análogas capturadas por la tarjeta provenientes de cámaras análogas.

Aquí una definición sobre señal digital La señal digital es un tipo de señal generada por algún tipo de fenómeno electromagnético en que cada signo que codifica el



contenido de la misma puede ser analizado en término de algunas magnitudes que representan valores discretos, en lugar de valores dentro de un cierto rango. Por ejemplo, el interruptor de la luz sólo puede tomar dos valores o estados: abierto o cerrado, o la misma lámpara: encendida o apagada (véase circuito de conmutación). Esto no significa que la señal físicamente sea discreta ya que los campos electromagnéticos suelen ser continuos, sino que en general existe una forma de discretizarla unívocamente.

Empieza a aparecer la deficiencia más reconocida de los sistema digitales es su calidad de video que a la fecha no ha podido superar a los sistemas análogos, los fabricante empiezan a desarrollar equipos más dedicados para esta aplicación, aparecen las cámaras para los sistemas digitales llamadas cámaras IP por su asignación de dirección digital.

Al iniciar los sistemas de seguridad electrónica en el mudo digital empiezan a integrarse a todo un conjunto de equipos y sistemas, de esta fusión se derivan los sistemas de seguridad integral.

Por esta razón los sistemas de seguridad electrónica ya no solo se conforman de cámaras, videograbadores y monitores lo que conocemos como CCTV (circuito cerrado de televisión), también tenemos señales de alarmas encargadas de vigilar la instrucción en un área, sistemas de detección y extinción de incendio, señales de control de un proceso y todo lo que incluye la Domotica

Los sistemas antiguos están emigrando a sistemas digitales para iniciar un proceso de mayor integralidad.



## JUSTIFICACION

El proyecto se realizara por suplir la necesidad de seguridad de la empresa GENERICA S.A en el cual se aplicaran el manejo e implementación de redes; instalación de software especializado para las cámaras de seguridad (CCTV); el mantenimiento preventivo, predictivo y correctivo de sistemas de comunicación, el uso adecuado de materiales y equipos especializados. Para la ejecución del proyecto se pensó en una seguridad superior, en una ayuda que facilite el trabajo de los guardas y en un avance tecnológico para la empresa.

La instalación de cámaras de seguridad y de sistemas de detección y control de acceso tiene como finalidad ayudar a las personas encargadas de la vigilancia a controlar de una manera más eficaz las diferentes zonas en las cuales no hay mucha visibilidad desde la portería y por ende se presentan daños y robos a los elementos de la empresa, lo mismo que posible intrusión de personas ajenas a esta.



## **SISTEMA DE SEGURIDAD INTEGRAL PARA GENERICA S.A**

### **GENERALIDADES DEL PROYECTO**

#### **1.1 PLANTEAMIENTO DEL PROBLEMA**

A través de la historia, el hombre siempre ha deseado tener la sensación de sentirse seguro con un máximo grado de tranquilidad y confianza, de tal manera que su existencia, sus bienes, su familia y todas las actividades que realiza no se vean afectadas ante la presencia de agentes internos o externos que en un momento dado puedan poner en peligro a esa sensación de seguridad que tanto aspira lograr.

Uno de los objetivos de la creación de las primeras comunidades era poder tener una mayor cantidad de individuos para aumentar su poder militar en pro de su seguridad.

Durante mucho tiempo fue la única forma efectiva de la seguridad, al nacer la tecnología esta llegó a suplir algunas desventajas notables que tenía la parte física como el cansancio y el estado sicosocial de las personas, las cuales eran unas variantes difíciles de controlar.

Para áreas extensas se le suministraban a los guardas de vehículos para su transporte pero la desventaja es la muy baja en las rondas y eran fáciles de predecir por parte de los delincuentes, otra desventaja notoria es que al momento de la instrucción por algún sospechoso era inevitable la confrontación entre el guarda y el intruso trayendo como consecuencias fatales para los guardas o legales con el delincuente.



Con los sistemas de seguridad integral se solución estas falencia de la seguridad física, los equipos tiene un funcionamiento de 24 horas diarias sin tener la variante del cansancio, puede abarcar zonas extensas y enviar las señales en tiempo real, es integrable a los sistemas policiacos de la zona evitando a los guardas confortaciones con los delincuentes.

Son más económicos con el tiempo en comparación a los sistemas físicos, volviéndose en la actualidad uno de las mejores opciones para los clientes con déficit en su seguridad.

## **1.2 FORMULACION DEL PROBLEMA**

¿Sera mas optimo un sistema de seguridad integral comparado con el sistema de seguridad física actual?

## **1.3 SISTEMATIZACION DEL PROBLEMA**

Genérica S.A requiere de un Sistema de Seguridad Electrónica dotado de las herramientas técnicas necesarias para fortalecer los procesos de seguridad física que son la detección, demora y respuesta con personal, equipos y procedimientos; sin embargo como parte de dicho proceso en la seguridad electrónica nos basamos en los procesos de detección, confirmación y comunicación dando así apoyo al sistema integral de seguridad con una oportuna operación por parte de seguridad ante incidentes o posibles amenazas que puedan afectar la continuidad del negocio, la integridad del personal, la información el medio ambiente y los bienes.



## **1.4 OBJETIVO**

### **1.4.1 Objetivo Específicos.**

Instalar y poner en funcionamiento un sistema de seguridad integral con una solución viable desde el punto de vista técnica, económica, y administrativo que satisfaga todas las necesidades de Genérica S.A.

### **1.4.2 Objetivo Específicos.**

Recopilar información de los sitios que son vigilados electrónicamente y permite apoyar las tareas previstas por la compañía para cada caso. El análisis posterior de los incidentes se verifica con el fin de mejorar en el tiempo de respuesta y la administración de los recursos dando así un manejo de riesgos confiable.

Diseñar un sistema para las instalaciones de Genérica S.A de alerta oportuna sobre potenciales incidentes terrestres con mecanismos de verificación que facilitan la evaluación y toma de decisiones por parte del equipo de seguridad.

Evaluar los criterios necesarios (procedimentales, logísticos y técnicos) para hacerlo sostenible y eficiente a través del tiempo, esto lo confirmamos con nuestra experiencia en sistemas ya integrados e implementados en varios clientes en campo. Así mismo, le informamos que el sistema es lo suficientemente flexible para adaptarse a los cambios en las necesidades de Genérica S.A, ya sea por la parte de los procedimientos y criterios de actualización ante la aparición de mejores prácticas y tecnologías en el mercado globalizado actual.

Proveer las herramientas necesarias para obtener niveles de servicio adecuados y consistentes con las necesidades de la operación.



## 2. MARCO TEORICO

### 2.1 ANTECEDENTES

Para conceptualizar un poco el tema a desarrollar a lo largo del trabajo, comenzaremos por conocer un poco de historia sobre el desarrollo de los sistemas de seguridad electrónica industrial.

La primera aparición de los circuitos cerrados de televisión fue a mediados de los años 60`s y 70`s, época caracterizada por la violencia e inseguridad, donde la calidad de los equipos en las imágenes era deficiente y con poca nitidez, puesto que las imágenes eran a blanco y negro y las líneas de resolución eran muy bajas. Además, la grabación de éstas era limitada, una imagen a la vez, indicando que cada cámara necesitaba de un monitor para su proyección, además de la gran cantidad de cintas para la recolección de las imágenes.

Años más tarde, en los 90`s, empieza la aparición de la seguridad digital con los DVR (Digital Video Recorder), mejorando tanto la calidad como la recolección de datos o imágenes, que con la ayuda del internet, permitió una evolución remarcable de los circuitos de seguridad electrónica, permitiendo el acceso y la supervisión de las organizaciones y los bienes desde cualquier parte del mundo.

Los circuitos cerrados de televisión (CCTV), fueron usados inicialmente como dispositivos de observación, sin embargo, hoy en día, integran un sistema interactivo, entre las organizaciones, socios, entes públicos y privados, para la confianza y cooperación con la sociedad. Los CCTV pueden ser para uso en el interior o en el exterior de las organizaciones, además, pueden ser controladas manualmente o a través de un sistema electrónico que permite el envío de imágenes en tiempo real directamente a una computadora o equipo electrónico,



permitiendo la grabación de las actividades de las organizaciones en cualquier momento.

Cuando se hablan de cámaras para el interior, se hace referencia a aquellas cámaras que previenen la pérdida de activos, bienes, desperdicio de horas de trabajo, así como también, las fallas de los equipos que causen alteraciones en los procesos de la organización.

Las cámaras para el exterior, son aquellas que permiten la fácil detección de una intrusión no autorizada, mediante el monitoreo de sus alrededores, además de proveer la seguridad a los empleados y al personal no vinculado con la organización.

## **2.2 CONVIVENCIA Y SEGURIDAD CIUDADANA**

Algunos países han desarrollado estrategias para combatir la inseguridad, la violencia y la carencia de los valores sociales, entre otros temas, que día a día, se están convirtiendo en el talón de Aquiles, no sólo de las industrias, sino también en la influencia de la calidad de vida de las personas.

En el año 1994, Bogotá creó un programa de seguridad, que no solo se encargaba de combatir con la inseguridad y la violencia sino que además tenía un alto contenido preventivo, que fortaleciera las barreras sociales y culturales que de una u otra manera iban ligadas con el cuidado de la integridad ciudadana. Es así, como no solo las entidades públicas deben ser partícipes, sino también el sector privado como las empresas pertenecientes a cada región, es decir, crear interacción entre la ciudadanía para que se vincule a estos programas para obtener beneficios multilaterales que refuercen la convivencia y que permitan el desarrollo eficiente de las organizaciones.



“El Departamento Nacional de Planeación, (DNP) de Colombia y el BID, formularon la estrategia nacional de apoyo a la “Convivencia y Seguridad Ciudadana”<sup>1</sup> en la cual desarrollaran políticas saludables para el fortalecimiento institucional, la prevención, reducción de homicidios y una mayor participación de la comunidad en la seguridad, con el fin de generar acciones frente a la violencia y construir la convivencia de la ciudadanía, es así, como cada región ha venido implantando modelos de seguridad desde los años 90’s, acordes con las necesidades existentes.

Para la sociedad la seguridad física es muy importante y de gran preocupación, siendo así, que lo que era antes terreno propio para joyerías, bancos y multinacionales, hoy en día ha entrado con fuerza en la ciudadanía, viéndose como una obligación o un requisito el disponer de sistemas de seguridad electrónicos, que le permitan obtener mayor seguridad en todos los aspectos; por lo que las autoridades de la ciudad de Macondo, se han visto en la necesidad de garantizar una seguridad total y que para lograr este objetivo es necesario recurrir a la colaboración mutua y bien organizada de todos los entes públicos y privados, es decir, como lo dice Santiago Lorente Arenas en su libro “La Comunidad Digital de Vecinos”, se debe saber/tener en cuenta:

- Aspectos Humanos: Compuesto por personal específico del campo de la seguridad, como son las fuerzas de orden público, las empresas privadas de seguridad, etc.

<sup>1</sup> Arriagada, Irma y Godoy Lorena. Seguridad ciudadana y violencia en América Latina: diagnóstico y políticas en los años noventa; Santiago de Chile, Agosto de 1999.



- Aspectos Técnicos: Es el conjunto de sistemas o elementos que disuaden, previenen o detectan un acceso no previsto o un determinado evento. Se pueden clasificar en pasivos y activos. Los primeros son elementos que dificultan o impiden el acceso al interior-puertas, vallas, muros, etc.-mientras que los segundos emplean mecanismos que mantienen un funcionamiento más o menos continuo-sensores-y pueden reaccionar ante cierto evento.
- Aspectos de Gestión: Conjunto de procedimientos, legislación, normativas y organización que permite relacionar y coordinar todos los anteriores, aportando además cohesión. Se extienden desde lo general como son las leyes y normativas internacionales, nacionales y locales, hasta lo específico donde se indican procedimientos de actuación, coordinación, homologación o el propio mantenimiento de las instalaciones. Este aspecto es el más importante de los tres porque, sea cual sea el grado de sofisticación de un sistema o la eficacia de los recursos humanos, éste puede resultar inservible si no está orientado a un objetivo y no tiene un plan de actuación ante incidentes.

Así mismo, una de las principales funciones del CCTV es el monitoreo y registro de imágenes captadas por medio de cámaras convenientemente instaladas, para mantener una adecuada supervisión de áreas críticas o para ser procesadas entre la necesidad de investigación de eventos pasados, que le permiten a las organizaciones, seguridad de los bienes, seguridad de las personas y finalmente detección de incidentes u averías de las mismas.

Es importante resaltar que las organizaciones deben de tener en cuenta 3 requerimientos en sus instalaciones para la correcta funcionalidad de todos sus procesos, como son: prevención, reconocimiento y reacción ante alarmas, como se habló anteriormente, las compañías deben de cumplir ciertas misiones para el buen desempeño y una de esas está en la implementación de los sistemas de



seguridad electrónica, que no solo le determinan las potenciales fuentes de peligro, sino que también, permite validar la señal verificando su procedencia y determinar si la señal de alerta sea enviada manual o automáticamente, es decir, que sea una señal de alarma remota o telefónica, ya sea con la policía, hospitales etc, en resumen son las personas interesadas en adquirir estos sistemas quienes toman la decisión y la segunda opción que es la automática, quien actúa es el sistema de seguridad electrónica, en este caso si ocurre un incendio se activaran las alarmas e inmediatamente los sensores dejaran caer agua.

La tecnología es un factor clave en el desarrollo de la industria, como lo expresa Robbins Stephen en su libro “La administración en el mundo de hoy”, puesto que ayuda a las ciudades para que incrementen su productividad por medio de la aplicación de nuevas tecnologías

### **3. ASPECTOS METOLOGICOS**

El método de la investigación realizada en estén proyecto es de campo, es la investigación aplicada para interpretar y solucionar alguna situación, problema o necesidad en un momento determinado. Las investigaciones son trabajadas en un ambiente natural en el que están presentes las personas, grupos y organizaciones científicas las cuales cumplen el papel de ser la fuente de datos para ser analizados.

Una de las fuentes utilizadas en el proyecto son las primarias, aquellas que provee un testimonio o evidencia directa sobre el tema de investigación. Las fuentes primarias son escritas durante el tiempo que se está estudiando o por la persona directamente envuelta en el evento. La naturaleza y valor de la fuente no puede ser determinado sin referencia al tema o pregunta que se está tratando de



contestar. Las fuentes primarias ofrecen un punto de vista desde adentro del evento en particular o periodo de tiempo que se está estudiando. Algunos tipos de fuentes primarias utilizados son:

- Documentos originales
- Artefactos
- Minutas
- Entrevistas
- Apuntes de investigación
- Noticias
- Fotografías

#### **4. DESARROLLO DEL PROYECTO Y RESULTADO**

SEGURIDAD TOTAL trabaja para salvaguardar el bienestar y la prosperidad de millones de personas alrededor del mundo, ayudando a crear ambientes más seguros y mejores en los cuales la gente viva y trabaje, creemos que en cada reto de seguridad, hay una oportunidad para descubrir beneficios ocultos.

La clave está en visualizar la imagen completa. Nos apoyamos en nuestros recursos mundiales en logística, tecnología, consultoría de riesgos, gestión de proyectos y nuestra experiencia en manejar la fuerza más grande del mundo de personal de seguridad en los diversos entornos normativos de 125 países, para crear soluciones de seguridad que ofrecen más que la suma individual de sus partes.

Como resultado, nuestros clientes son capaces de proteger mejor sus activos críticos, generar ingresos adicionales, reducir los costos y ofrecer un mejor servicio a sus clientes. En tiempos de incertidumbre, hacemos la diferencia.



La organización se centra en sus clientes - interpretando las problemáticas que ellos enfrentan, los mercados en los que operan, y brindando servicios de la más alta calidad.

Sectores en donde trabajamos:

- Gobierno
- Minería
- Energía y servicios
- Petróleo & Gas
- Transporte & Logística
- Puertos y Aeropuertos
- Recreación y Turismo
- Instituciones Financieras
- Corporaciones & Industrias
- Comercio

Antes de iniciar con la explicación del componente técnico del proyecto, describiré como se logro llegar a una propuesta financiera viable, la cual nos mostro como la opción número uno en la licitación con la empresa GENERICA S.A.

Uno de los objetivos más importante que tiene el estudio de la gestión de proyecto es buscar las soluciones óptimas y económicas supliendo el 100% de las necesidades del cliente, un claro ejemplo fue el desarrollo de este proyecto.

GENERICA S.A. venía desde hace más de 30 años manejando un contrato de seguridad solo con el componente físico, nosotros planteamos darle vuelta a este paradigma y ofrecer la parte electrónica como complemento, para así lograr un sistema de seguridad integral.



El desafío mayor era adicionar la parte de seguridad electrónica sin aumentar el presupuesto de la licitación. Esto se logra en gran parte cuantificando el costo de los equipos con su instalación, más la suma de la utilidad y dividiéndolo en 60 meses, tiempo de ejecución del proyecto, continuando por encima de la cuota fija mensual que tenía presupuestada GENERICA S.A para el contrato de seguridad.

Se realizaron visitas a las áreas supervisadas por la parte física, encontrando deficiencias las cuales las podíamos optimizar con el componente de la seguridad electrónica y podíamos después de instalado el sistema eliminar algunos puestos de guardas, de esta forma optimizaríamos recursos financieros, los cuales impactaría en la cuota fija mensual.

Esta es la relación de los puestos eliminados y cambios de turnos, los cuales iniciarían su aplicación en el sistemas de seguridad después de terminada la instalación del sistema electrónico.

Eliminación de puestos.

- Manila
- Erfurt
- Balsilla
- Porto
- Jaipur
- Tampa

Cambio de turnos.

- CE (Centro de estudio)      24 HORAS – CE 12 HORAS
- CC (Centro de capacitación) 24 HORAS – CC 12 HORAS
- RI (Residuos industriales)   24 HORAS – RI 12 HORAS



Impacto en la facturación total con mejoras \$383.736.903

DESCRIPCION	TOTAL	COMENTARIOS
VIGILANCIA	\$313.922.083	SE INCREMENTA CADA QUE VARIE EL SALARIO DEL PERSONAL
SEGURIDAD ELECTRONICA	\$ 56.356.841	TARIFA FIJA 5 AÑOS
CE,CC;IR	\$ 13.457.979	SE INCREMENTA CADA QUE VARIE EL SALARIO DEL PERSONAL
TOTAL	\$ 383.736.903	

Se realizo una proyección y a los 6 meses tiempo de instalación del proyecto y con el desmonte de algunos puestos de trabajo, no solo estaremos dentro del rango de la cuota fija mensual ofrecida por el cliente, también podríamos ofrecerle una disminución en la misma.

Por este manejo financiero y por nuestra parte tecnológica robusta que describiremos a profundidad en adelante se logra obtener el contrato con GENERICA S.A.



#### **4.1 ALCANCE**

El Sistema incluye los equipos, instalación, operación, mantenimiento, administración y actualización tecnológica a los años contratados. El desempeño se mide de acuerdo con los parámetros y la metodología establecidos con Genérica S.A dando así los niveles de servicio ofrecidos por SEGURIDAD TOTAL S.A hacia nuestro nuevo aliado comercial / cliente.

Las instalaciones objeto del presente proyecto son:

Zona de producción:

Instalaciones permanentes de gran tamaño con facilidades logísticas en las que hay una alta concentración de personal y activos donde se realizan tareas críticas para la operación.

Planta:

Instalaciones permanentes de menor tamaño ubicadas dentro de la zona de producción típicamente dedicada a labores de recolección, almacenamiento y procesamiento de producto, se realizan tareas críticas de la operación.

Ciudadelas y clubes:

Lugar de vivienda de las familias y empleados de Genérica S.A ubicada en la zona urbana del municipio de Macondo.

#### **4.2 PRINCIPIOS DE DISEÑO**

La filosofía del sistema es detectar y confirmar de manera inmediata y confiable cualquier intento de intrusión a través del perímetro de las instalaciones o en áreas críticas al interior de las mismas, para permitir que SEGURIDAD TOTAL S.A y Genérica S.A active los procedimientos de repuesta establecidos para cada caso.



Adicionalmente, el sistema efectúa tareas de vigilancia específica sobre áreas o puntos críticos en el exterior del perímetro definidos por Genérica S.A, para que se puedan detectar posibles aproximaciones al entorno que puedan generar riesgos el personal, la información y las instalaciones y / o supervisar algunas operaciones rutinarias o eventuales.

El Sistema cumple con los siguientes principios de diseño y características:

La adquisición de la información se hace a través de cuatro subsistemas, que funcionarán de manera integrada para el despliegue, gestión, administración y registro de la información:

1. Subsistema de Detección Perimetral
2. Subsistema de Confirmación
3. Subsistema de Detección Interior
4. Subsistema de Vigilancia Específica

El manejo de la información y la interacción entre los subsistemas se hace a través del Subsistema de Integración.

El Sistema permite el registro automático de las señales de alarma y vídeo asociadas con un evento, así como de las acciones o procedimientos ejecutados por los operadores o de forma automática por el sistema en respuesta al evento; también se registran las imágenes obtenidas como resultado de tareas específicas de vigilancia o supervisión que así lo requieran.

El Sistema registra además la información relacionada con la administración del sistema; la programación y ejecución del mantenimiento, los reportes generados por las fallas en equipos o programas. En general el sistema provee en forma automatizada, desatendida y confiable, la información necesaria para la gestión de los niveles de servicio.



El Sistema esta implementado de tal manera que asegura su funcionamiento permanente en todas las condiciones climáticas, topográficas y ambientales en las que se desarrolla la operación de Genérica S.A, contando con las protecciones necesarias en cantidad y calidad para operar aún en condiciones tales como: lluvia, tormentas eléctricas, vientos rigurosos, temperaturas extremas, humedad ambiental extrema, condensación, etc.

Ningún equipo causara interferencia a equipos previamente existentes en las instalaciones de Genérica S.A. El diseño garantiza la compatibilidad electromagnética para lo cual nuestros ingenieros presentaran los diseños a consideración y aprobación de Genérica S.A. Se identificaran los riesgos de pérdida o daño, a los componentes del sistema (derivados de eventos tales como acciones de terceros, semovientes, incendios, etc.) y se implementaran las medidas y acciones de mitigación que permitan garantizar el funcionamiento del sistema dentro de los niveles de servicio establecidos.

EL Sistema es suficientemente flexible para adaptarse a los cambios que surjan como resultado de las necesidades de seguridad en los diferentes tipos de instalaciones en la zona de operación de Genérica S.A sin afectar la arquitectura básica y manteniendo una proporcionalidad razonable en costo. El sistema incluye las herramientas de software y hardware necesarias para la supervisión de su operación y las tareas de mantenimiento preventivo y correctivo del sistema con todos sus componentes.

Los componentes del sistema funcionan como un todo que permite centralizar la gestión de la información correspondiente a los niveles de servicio efectivamente obtenidos, el monitoreo y control de los elementos constitutivos y su mantenimiento. La tecnología usada es vigente y adecuada a las necesidades de Genérica S.A. Los equipos usados en el sistema son de marcas reconocidas,



disponibles en el mercado colombiano y adecuadamente representadas localmente.

El Software utilizado en el sistema está disponible en el mercado, adecuadamente representado localmente y la licencia permite a Genérica S.A su uso sin restricciones durante la duración del contrato de seguridad. Las partes que conforman el software como son las bases de datos, conectores, interfaces o módulos que llegaren a ser desarrollados específicamente para este proyecto, se licenciaran de manera ilimitada no exclusiva a favor de Genérica S.A para uso únicamente en el proyecto y su código fuente y documentación técnica será puesta a disposición.

Los equipos se renovarán al cumplir el tiempo de depreciación ofrecido o eventualmente, por acuerdo entre las partes, cuando surjan alternativas más convenientes en el mercado.

Todo el manejo de información del sistema, del servicio y de la operación se encuentra enmarcado en los conceptos y recomendaciones de la norma ICONTEC-NTC-ISO-IEC-27799 para seguridad de la información.

Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".



### **4.3 INTEGRACIÓN DE PERSONAL, EQUIPOS Y PROCEDIMIENTOS**

La propuesta toma en cuenta tres variables que forman parte de la solución descrita para minimizar el nivel de riesgo del proyecto (personal, información y objetos a proteger) o en su defecto aminorar el impacto o la eventualidad de los eventos no deseados.

El personal da el control de acceso a empleados, contratistas, subcontratistas y en alguna medida el control de activos; así como también la detección de intrusión en su campo de visión.

Los equipos forman parte de la detección, confirmación y comunicación hacia el personal que realizara la respuesta.

Los procedimientos se modificarán una vez los equipos estén en línea para maximizar recursos.

SEGURIDAD TOTAL S.A toma como base el siguiente modelo:

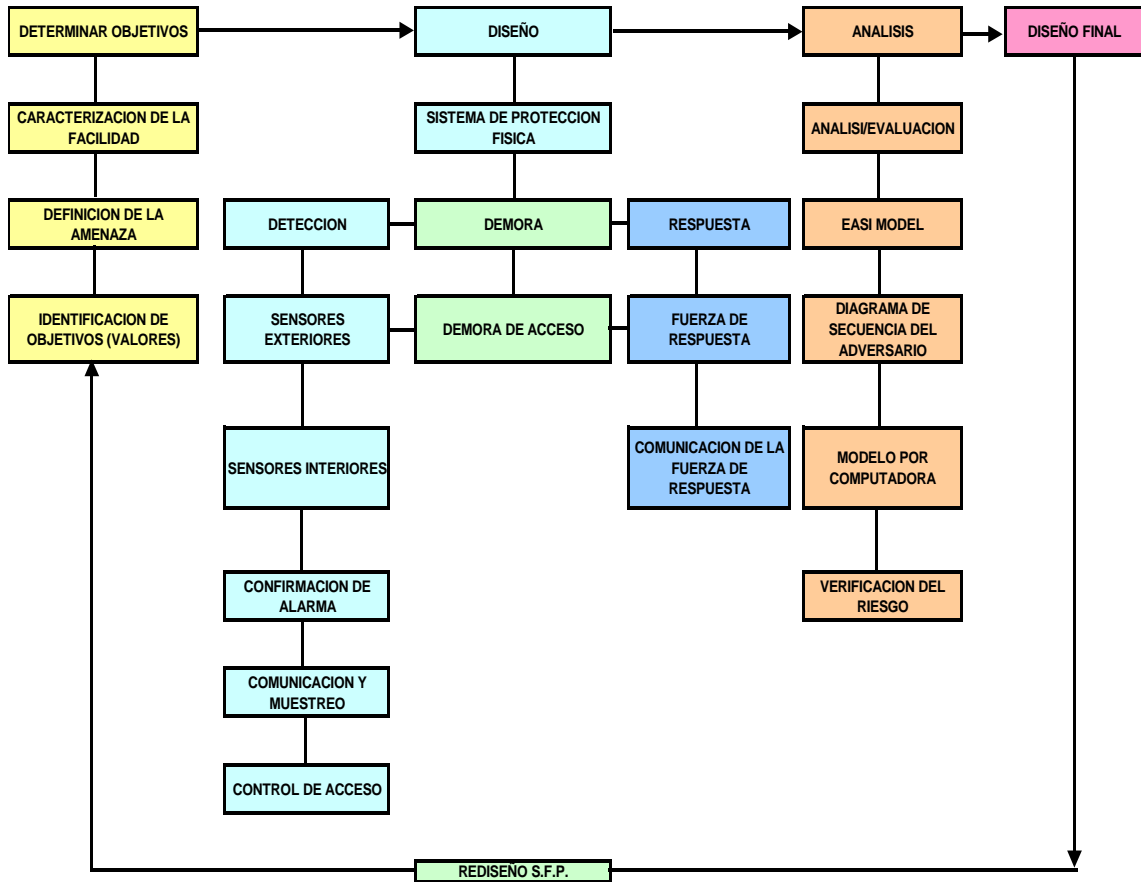


Figura 1. Base del modelo seguridad integral. Extraído del Pliego de licitación con Genérica S.A.

#### 4.4 ORGANIGRAMA

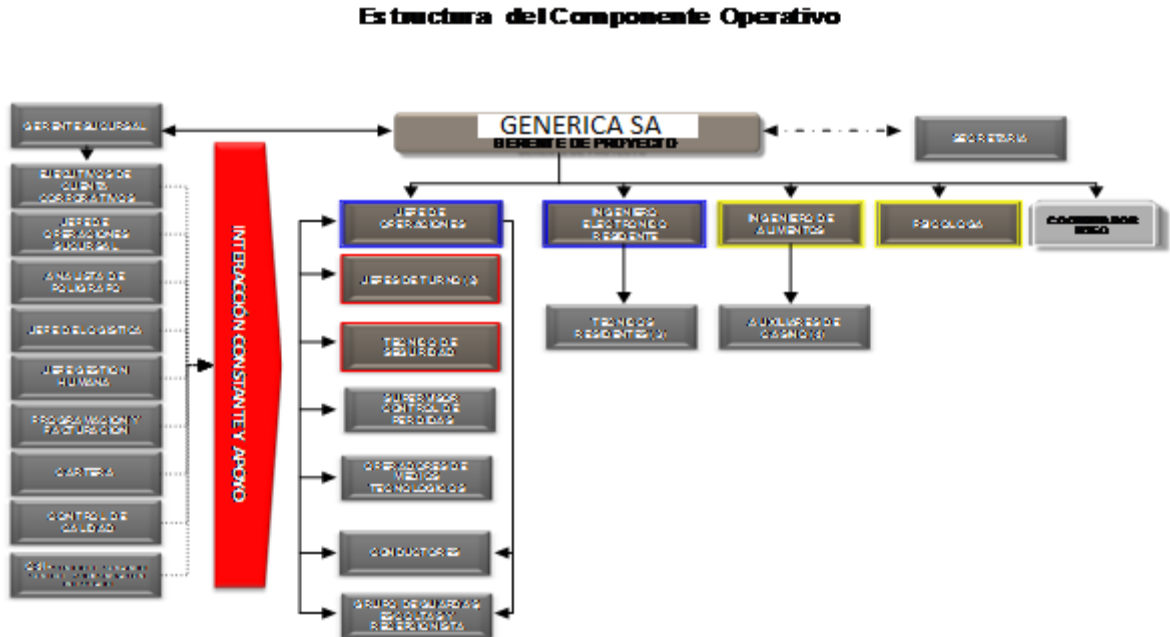


Figura 2. Organigrama. Extraído del Contrato.

#### 4.5 DESCRIPCION GENERAL DE LA SOLUCION

En el presente capítulo se da una descripción general del alcance de los elementos constitutivos del sistema de seguridad electrónica. La solución propuesta es la de un Servicio de Vigilancia y Seguridad Privada con Medios Tecnológicos para las instalaciones de Genérica S.A y su valor incluye:

- Suministro de equipos (compra, prueba, transporte internacional, nacionalización)
- Instalación
- Puesta en servicio
- Capacitación
- Operación



- Mantenimiento
- Administración
- Actualización tecnológica.

Para cada una de las actividades anteriormente mencionadas, una vez adjudicado el proyecto, se incluirá la documentación técnica de instalación y mantenimiento de los equipos pertenecientes al sistema.

El servicio de Vigilancia y Seguridad Privada con Medios Tecnológicos se realizará en las siguientes instalaciones de Genérica S.A: Zona de producción, Planta, ciudadelas y clubes, por medio de los siguientes subsistemas:

- Subsistema de detección perimetral.
- Subsistema de verificación.
- Subsistema de detección interior.
- Subsistema de vigilancia específica .
- Subsistema de integración.

El diseño del sistema está basado en el uso de tecnologías y equipos vigentes, flexibles, modulares y adaptables a las diferentes condiciones geográficas, climáticas y logísticas de las instalaciones de Genérica S.A, obteniendo un sistema con tecnologías homogéneas e integrables entre sí

Dichas tecnologías y equipos, serán empleadas en cada subsistema de la siguiente manera:



#### **4.5.1 Subsistema de Detección Perimetral.**

De acuerdo con las exigencias de diseño se propone el uso de un sistema continuo de detección a lo largo del perímetro que posee la capacidad de discriminación de zonas de producción suficiente para maximizar la posibilidad de detección y mantener un rango mínimo de falsas alarmas, según el tipo de localización a cubrir se utilizarán los siguientes equipos:

El perímetro de todas las instalaciones está cubierto por una línea continua de detección que cuenta con la capacidad de discriminación de zonas de producción suficiente para maximizar la probabilidad de detección y mantener el rango de falsas alarmas de acuerdo con los niveles de servicio. La línea de detección se extiende aún en los puntos de acceso del cerramiento, ya sea utilizando el mismo equipo o combinando tecnologías.

El subsistema reporta los eventos detectados, identificando la zona de detección para permitir la automatización de los mecanismos de respuesta. Las tecnologías aplicables en este subsistema pueden incluir sensores en la malla, cables o fibras ópticas enterrados.

Las características para el diseño y la selección de la tecnología o tecnologías para este subsistema que se tuvieron en cuenta son las siguientes:

- Bajo nivel de falsas alarmas
- Posibilidad de discriminación para minimizar el número de Alarmas Inválidas.
- Flexibilidad de configuración (número y tamaño de zonas configurables, etc.)
- Bajo costo de mantenimiento.
- Estabilidad (que sus características no se degraden en el tiempo).



- Facilidad de instalación y versatilidad para aplicaciones en instalaciones temporales.
- Facilidad de integración con otros subsistemas.
- Baja vulnerabilidad (dificultad de ser engañada o neutralizada).
- Muy baja sensibilidad a los cambios atmosféricos y climáticos.
- Baja interferencia ante la presencia de campos electromagnéticos.
- Capacidad de monitoreo remoto de estado.

Una tecnología o una combinación de tecnologías, dependiendo de las condiciones particulares de aplicación en cada instalación, serán utilizadas para la implementación de este subsistema teniendo en cuenta, las siguientes variables:

- Topografía.
- Tipo de suelo.
- Presencia o cercanía de corrientes de agua.
- Presencia o cercanía de tuberías.
- Presencia o cercanía de equipos de la operación.
- La existencia de campos electromagnéticos.
- Temperatura ambiente y sus variaciones.
- Tipos de vegetación.
- Servidumbres o tránsito de personas.
- Presencia rutinaria de ganado o animales.
- Dificultad de mantenimiento de la malla.
- Existencia de doble malla y/o corredores de seguridad.
- Calidad del cerramiento.
- Longitud del perímetro.
- Cantidad de accesos (peatonales y vehiculares).



**4.5.1.1 Zona de producción y planta.** En instalaciones como lo son la zona de producción y las Planta se ha determinado la instalación del sistema de cable sensor enterrado en el suelo denominado OmniTrax de la fábrica Senstar Stellar.

El sistema opera creando un campo electromagnético alrededor de los cables enterrados. La intrusión se detecta cuando ese campo es perturbado por cuerpos o elementos basados en su conductividad, peso y movimiento; la probabilidad de detección es del 99% cuando el cuerpo del intruso es de 35 kilogramos o más, moviéndose a través de la zona de detección con una velocidad de 8 metros por segundo. Cuerpos o elementos con tamaños o masas menores de 10Kg son ignorados con una confianza del 95%, reduciendo de esta manera la detección de pequeños animales y efectos molestos causados por vegetación, vientos, lluvia, nieve, arena, etc.

El campo de detección volumétrico creado es típicamente de un (1) metro de alto por dos (2) metros de ancho, sin embargo el tamaño de este campo de detección depende de la profundidad a la que se entierre el cable, del tipo de terreno y de la sensibilidad ajustada. La profundidad recomendada por el fabricante para suelo blando (zona verde) es de 25 a 30 centímetros, en piso duro como lo son pisos con asfalto o en concreto la profundidad recomendada es de 8 centímetros que se puede lograr fácilmente con un disco de corte. El cable tiene construcción robusta para ser enterrado directamente sin necesitar ningún tipo de canalización.

La tecnología de detección desarrollada por Senstar Stellar se denomina iRange y permite que la intrusión sea detectada con una precisión de un metro, además permite identificar múltiples intrusiones simultáneamente.

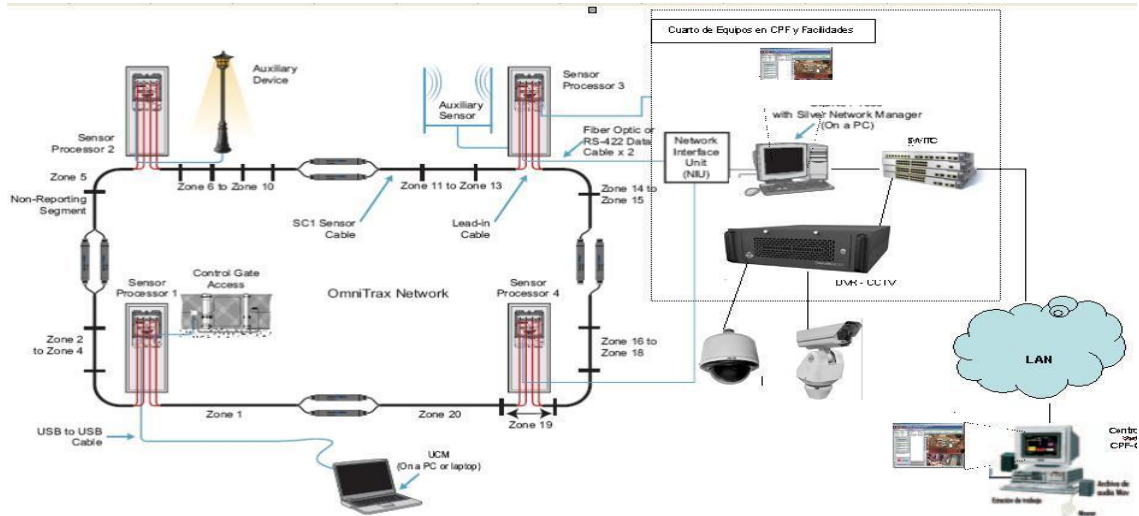
Cada unidad del equipo OmniTrax atiende hasta dos segmentos de cable sensor enterrado de 400 metros cada una. Para este proyecto se utilizará el cable SC1 permitiendo hasta un cubrimiento de 800 metros por cada unidad OmniTrax. Cada



unidad permite crear mediante su software de parametrización hasta 50 zonas de detección cambiando la sensibilidad de detección del cable metro a metro, incluso pudiendo dejar zonas inactivas para pasos vehiculares, pasos de agua, etc., si se requiere. Este cable se instalará alrededor de la zona demarcada en los planos de requisitos de Genérica S.A previendo que se quiere realizar una detección perimetral temprana.

El cable sensor además de las funciones de detección de intrusos también permite la interconexión entre varias unidades procesadoras, permitiendo así la distribución de energía eléctrica a cada uno de ellos desde una fuente de energía hasta ocho equipos conectados en red uno a continuación de otro como se muestra en la Figura 1. De igual manera por el cable sensor una vez interconectado viajan las señales de detección y de estado de cada procesador hasta llegar al módulo de interface de red (NIU) que realiza el envío de todos los datos en RS422-4W hacia el software de visualización y gestión StartNet 1000. El número de unidades de procesamiento OmniTrax interconectadas de esta manera es ilimitado, la restricción únicamente aplica para el suministro y transmisión de energía eléctrica. Esta propiedad permite que el sistema sea redundante al permitir por lo menos dos caminos para transmitir las señales de alarma y estado de cada procesador hacia el centro de control.

El despliegue y visualización de las alarmas generadas por el sistema de detección perimetral se realizará de manera local y de manera remota según lo mostrado en el documento de alcance y especificaciones técnicas del servicio mediante la utilización del software de integración Integrator desarrollado por SEGURIDAD TOTAL S.A.



**Figura 3.** Configuración en RED de equipos OmniTrax – Integración con CCTV.  
Extraído del Manual de instalación cable Sensor Stellar Omnitrix.

El operador podrá apreciar mensajes audibles de acontecimientos específicos; los procesamientos automatizados de eventos y gráficos de alta resolución específicos del lugar serán mostrados automáticamente al operador indicando sobre ellos la localización exacta del evento. El operador puede modificar con facilidad las acciones para usar los procedimientos previamente establecidos. También el operador puede acceder a los módulos de supervisión y mantenimiento que le permite obtener diagnósticos, informes y configuración del sistema.

Se tienen las siguientes cantidades de equipo para el Subsistema de Detección Perimetral:

Equipos Subsistema de Detección Perimetral	ZONA DE PRODUCCIÓN CUBRIMIENTO PERIMETRAL SOLICITADO POR GENÉRICA S.A
Unidades Procesadoras OmniTrax	6
Cable sensor SC1 [metros]	2100
Computador + software StarNet 1000	1

#### 4.5.1.2 En las ciudadelas y Clubes.

En locaciones como ciudadelas y clubes se ha determinado la instalación del sistema IntelliFlex de la fábrica Senstar Stellar.

Se escogió el uso de este equipo a pesar de ser localizaciones con perímetros relativamente pequeños, el sistema IntelliFlex permite la creación de zonas de detección de hasta 300 metros, pero se tendrán zonas de 100m para garantizar una mejor ubicación del generador del evento.

El sistema IntelliFlex es un sensor microfónico como medio de detección de intrusión en exteriores, los cuales pueden ser montados en cercas, pisos, paredes u otros medios físicos que detecta un intruso que este cortando, trepando o levantando el material.

Una unidad protege un perímetro de hasta 300m (por diseño). Se pueden unir múltiples unidades para cubrir distancias más largas.



**Figura 4.** Instalación física en campo del equipo IntelliFlex. Extraído de Hoja técnica Sensor Stellar IntelliFlex.

Una vez se ha dado la detección de un intruso la unidad procesadora realiza la activación de un relevo de alarma. Debido a que en este tipo de solución no se contempla la construcción de una red alamburada de comunicaciones, la transmisión de esa señal de alarma se realizará utilizando un Kit de transmisión inalámbrica INNOVONICS FA464DR de 16 canales con salida por relevos que mediante el módulo de alarmas del DVR se incorpora las señales de alarma al software de Integración.





El operador podrá apreciar mensajes audibles de acontecimientos específicos, procesamientos automatizados de acontecimientos y gráficos de alta resolución del lugar donde se ha generado la alarma procesada, la resolución de cada zona de detección será de máximo 300 metros.

Al igual que en la operación de los sistemas de detección perimetral de los zona de producción, también el operador puede acceder a los módulos de supervisión y mantenimiento que le permite obtener diagnósticos, informes y configuración del sistema.

Para mayor documentación a cerca de las características del equipo ofrecido por favor revisar el catalogo de este producto en la sección anexo de catálogos y brochures de nuestra oferta.

Se tienen las siguientes cantidades de equipo para el Subsistema de Detección Perimetral:

Equipos Subsistema de Detección Perimetral	CIUDADELAS CLUBES
Unidades Procesadoras IntelliFlex	4
Kit inalámbrico Innovonics de 16 canales	1
Computador + software	1

#### **4.5.2 Subsistema de Verificación.**

De acuerdo con el documento alcance y especificaciones técnicas del servicio se describe a continuación las configuraciones de los subsistemas de verificación (CCTV) propuestos para cada una de las locaciones.



El sistema provee de manera automática e inmediata la información necesaria para la verificación visual a través de un sistema de CCTV (Circuito Cerrado de Televisión), de los eventos generados en la línea de detección perimetral. Los operadores disponen de las imágenes y planos necesarios de las áreas relacionadas con el evento de detección, las cuales son enfocadas y desplegadas de manera automática.

Para la verificación se garantiza que el sistema de CCTV cubre todo el perímetro de detección con la sensibilidad, contraste y resolución necesarios para identificar adecuadamente el origen de la amenaza en cualquier condición de iluminación de producción.

Las tecnologías aplicadas en este subsistema incluyen cámaras de CCTV móviles tipo domo y cámaras fijas y cámaras térmicas para observar el perímetro en horas de la noche donde no hay iluminación en zona de producción por medio de diferenciación de calor.

Cámaras móviles:

Estas cámaras están en capacidad de distinguir una figura humana en cualquier parte del perímetro con claridad y definición, utilizando para ello únicamente el acercamiento óptico (zoom). Las imágenes que llegan al Centro de control estarán libres de imágenes distorsionadas (pixelación), oscilación y ruido.

Las cámaras móviles son de tipo día/noche y están ensambladas en un solo paquete que incluye:

- “Housing” o enclaustramiento para intemperie con mecanismo para evitar la condensación y donde se requiera, “housing” para zonas clasificadas (Explosion-Proof).
- Mecanismo interno de “PAN/TILT”



- Sistema óptico automático y mecánico de auto enfoque.
- Brazo o soporte resistente a la intemperie y a prueba de vibración, apropiado para las condiciones de la operación.
- Estabilización de movimiento en donde sea necesario.
- Posee un sistema de pre-posicionamiento (mínimo 32 preposiciones), mas conocidos como tours.
- El enfoque automático deberá tener la opción de enfoque manual.
- Movimiento horizontal continuo de 360°.
- Velocidad de posicionamiento de mínimo 180 grados/segundo en modo automático.
- Ajuste de compensación para luces de fondo "BACKLIGHT COMPENSATION" automático.
- Ajuste de blancos "WHITE BALANCE" automático.
- Control automático de ganancia, (AGC) de alta velocidad.
- Alta sensibilidad de la cámara para condiciones de luz mínimas incluyendo horarios nocturnos (uso continuo 24 horas) sin depender de la iluminación de producción especial.
- Zonas de blanqueo de vídeo programables.
- Inserción en el vídeo de la identificación de cada cámara.
- Bajo consumo de energía.

#### Cámaras fijas:

Estas son de alta resolución y las imágenes que llegan al centro de control están libres de pixelación, oscilación y ruido, con características adecuadas para la aplicación específica.

Las cámaras fijas son día/noche y están ensambladas en un solo paquete que incluye:



- “Housing” o enclaustramiento para exteriores e intemperie con mecanismo para evitar la condensación y donde se requiera “housing” para zonas clasificadas (Explosion-Proof).
- Sistema óptico automático / mecánico de auto enfoque si es necesario para la aplicación.
- Brazo o soporte resistente a la intemperie y a prueba de vibración mecánica.
- Estabilización de movimiento en donde sea necesario.
- Ajuste de "BACKLIGHT" automático.
- Ajuste de blancos "WHITE BALANCE" automático.
- Control automático de ganancia, (AGC) de alta velocidad.
- Sensibilidad adecuada para la aplicación particular que debe incluir horarios nocturnos (uso continuo 24 horas).
- Inserción en el vídeo de la identificación de cada cámara.
- Bajo consumo de energía.

Cámaras térmicas para observar áreas donde no hay iluminación de producción y observa diferencial de calor:

Estas cuentan con las siguientes características:

- Sensible en el rango de longitudes de onda de 7-14 micrones.
- “Housing” o enclaustramiento para exteriores e intemperie con mecanismo para evitar la condensación y donde se requiera “housing” para zonas clasificadas (Explosion-Proof).
- Mecanismo de “PAN/TILT”.
- Sistema óptico mecánico de auto enfoque.
- Brazo o soporte resistente a la intemperie y a prueba de vibración mecánica.
- Estabilización de movimiento donde sea necesario.
- Sistema de pre-posicionamiento (mínimo 32 preposiciones).



- Enfoque automático con opción a cambio manual.
- Ajuste de "BACKLIGHT" automático.
- Inserción en el vídeo de la identificación de cada cámara.

#### **4.5.2.1 Zona de producción y planta.**

Con la finalidad de poder realizar la verificación visual de los eventos generados por el subsistema de detección perimetral, se ha dispuesto ubicar dos tipos de cámaras móviles en la parte exterior e interior del perímetro de la zona de producción y la planta con la finalidad de lograr el cubrimiento del perímetro y de los puntos críticos exteriores.

Se ha diseñado un tipo de sistema móvil para la verificación en el área de almacenamiento material de escoria, en estos lugares podrá trasladarse el sistema al sitio requerido, de acuerdo con las necesidades de la verificación y la operación de Genérica S.A.

También se busca con esto hacer más efectiva la verificación automática de las alarmas de detección temprana del subsistema de detección perimetral al evitar los obstáculos visuales que se generan al interior de la planta.

Sistema de verificación tipo fijo día /noche

- Una Cámara Domo Spectra IV – Pelco
- Una Cámara térmica ES30TI – Pelco
- Un poste de 18 metros en concreto
- Sistema de tierras y pararrayos.
- Conjunto de Radios para transmisión de video S1100 – Verint

Se utilizan cámaras de dos tecnologías: domos color / B & N (Spectra IV) y cámaras térmicas (ES3050TI-2N) para poder garantizar obtención de imágenes de video independientemente de las condiciones de iluminación de la zona de



producción durante todas las horas del día sin depender de mecanismos de iluminación de producción especial.

Cada kit de generación solar está compuesto por 6 paneles de 130W, baterías estacionarias, regulador de carga e inversor. Se incluye el cálculo utilizado para el dimensionamiento de esta solución, la cual pretende dar respaldo de energía durante las 24 horas del día los 365 días del año.

Por estrategia de optimización del suministro de energía y de disponibilidad de transmisión de señal de video se tendrá en funcionamiento una sola cámara a la vez, la escogencia de cual estará en funcionamiento se podrá realizar de manera automática o manual desde el Centro de Control.

Cada sistema de verificación posee pararrayos, sistema de puesta a tierra con valor de impedancia final de 5 ohmios, se incluyen protecciones contra sobre tensiones Ditek.

La transmisión de las señales de video, datos de control y señales de alarma de intrusión se realiza a través de radio enlaces punto a punto marca Verint S1100. Cada radio enlaces posee un canal de video de entrada análoga IRE, un canal bidireccional para datos de control en formatos RS232/RS422/RS485, dos entradas de contacto seco para transmisión de señales de alarma y una salida de relevo para activación remota de dispositivos. Estos radio enlaces operan en bandas no licenciadas de 2,4 y 5 GHz y manejan un rango máximo de transmisión de 5 a 15 kilómetros dependiendo de las condiciones geográficas, atmosféricas y de las frecuencias de operación. Dentro del diseño propuesto bajo ninguna condición de operación se superan estos valores máximos.

Las señales de video, datos de control y señales de alarma provenientes de los radio receptores se conectan a un equipo DVR MARCH-4316 de 16 entradas de video, el cual estará en función de grabación permanente a una velocidad baja de



imágenes por segundo y que cambiará de manera automática a una velocidad mayor y ordenará a una cámara o a un conjunto de ellas la realización de preset automáticos cuando el software de visualización y gestión Integrator le indique que lo haga debido a la generación de una alarma de detección perimetral, específica o de detección interior.

#### **4.5.2.2 En las ciudadelas y clubes.**

Para el control y la verificación del perímetro se instalarán 16 domos color/BW (Spectra IV) de acuerdo a la siguiente distribución

Sistema de verificación móvil día /noche ciudadelas

- Una Cámara Domo Spectra IV – Pelco
- Un poste de 18 metros en concreto
- Sistema de tierras y pararrayos.
- Conjunto de Radios para transmisión de video S1100 – Verint

#### **4.5.3 Subsistema de Vigilancia Específica.**

Este subsistema facilita la detección de actividad en puntos críticos ubicados en los accesos y hará interfase con los sistemas de control de acceso en las porterías.

Igualmente el sistema provee la capacidad de vigilancia mediante CCTV donde sea posible, de los puntos críticos definidos por Genérica S.A, localizados fuera del perímetro tales como posibles vías de aproximación, etc. Esta vigilancia se hará de manera previa y durante el desarrollo de algunas actividades críticas con el fin de detectar posibles acercamientos que puedan terminar en un intento de intrusión o un ataque.



Las tecnologías aplicables en este subsistema incluyen; CCTV y sistemas de control de acceso más cualquier aplicación que desee el cliente complementar para este tipo de aplicaciones. En este caso podemos mencionar una de ellas como es la apertura de puertas para la evacuación en caso de conato de incendio, si este da al sistema la posibilidad de informar el evento.

Para este sistema se han diseñado el uso de sistemas de control de, que permitirán el registro y acceso de personal autorizado a todas las áreas, ya sea de tipo vehicular o peatonal.

Al igual como se maneja la portería principal en la zona de producción se implementaran en la ciudadela, todas contarán con un sistema de control de visitantes, en el cual se registrarán los datos esenciales del visitante y se reseñara al visitado, se incluirá un registro fotográfico y se asignará una tarjeta de visitante que le permitirá pasar a través del sistema de control de acceso.

Una sola base de datos en planta controlará el registro de visitantes permitiendo usar listas negras, entre otras funciones.

#### **4.5.3.1 Control de acceso en Zona de producción y planta.**

Usando la infraestructura actual de talanqueras, controladoras y molinetes, se integrará todo el sistema al Integrator.

#### **4.5.3.2 Acceso Peatonal.**

Dentro del diseño para el control de acceso de las porterías a fin de mejorar el ingreso y seguridad del personal y las instalaciones, se implementara el uso de detectores de metales Garret de cuerpo completo y máquina de rayos x de paquetes. Para los detectores de metales se activarán y repararán si son necesarios los que actualmente tiene Genérica S.A, para colocarlos en servicio.

En cuanto a la máquina de rayos x, se usará la ASTROPHYSICS INC 5335.



**Figura 6.** Control de acceso peatonal Planta. Extraído el del catálogo Astrophysics.

Esta configuración permite mejorar la seguridad de ingreso y salida de trabajadores, visitantes, así como de las instalaciones y los activos que se encuentren

Equipos Subsistema de Vigilancia Especifica	ZONA DE PRODUCCIÓN PEATONAL
Arcos Detectores de Metales	1
Máquina de rayos X 5335	1

**4.5.3.3 Acceso peatonal polvorines y planta de emulsión.** Se implementaran sistemas de control de acceso compatibles con el sistema actual y se colocaran a reportar al sistema de control de acceso actual Winpak .



Las lectoras se comunicaran a controladoras por Wiegand y esta a su vez vía TCP/IP al software de gestión del sistema de control de acceso y al Integrator

Equipos Subsistema de Vigilancia Especifica	ZONA DE PRODUCCIÓN
Unidades controladoras IRC 2000	1
Lectoras HID	1

#### 4.5.4 Subsistema de Detección Interior.

Este subsistema proporciona las herramientas necesarias para la detección y verificación de un evento de intrusión en áreas críticas ubicadas al interior de una instalación.

Las tecnologías aplicables en este subsistema incluyen cámaras de CCTV con detección digital de movimiento o combinaciones de cámaras y sensores.

Para la detección, la tecnología o tecnologías seleccionadas contarán con las siguientes características:

- Bajo nivel de falsas alarmas
- Posibilidad de discriminación de la zona de producción para minimizar el número de falsas alarmas.
- Bajo costo de mantenimiento.
- Estabilidad (sus características no se degraden en el tiempo).
- Facilidad de instalación y versatilidad para aplicaciones en instalaciones temporales.
- Facilidad de integración con otros subsistemas del SISSE.



- Baja vulnerabilidad (dificultad de ser engañada o neutralizada).
- Muy baja sensibilidad a los cambios atmosféricos y climáticos.
- Baja interferencia ante la presencia de campos electromagnéticos.
- Capacidad de monitoreo remoto de estado.

La elección de una o de una combinación de tecnologías dependerá de las condiciones particulares del área a proteger. Para la verificación se garantizará que los equipos seleccionados cubran el área de detección con la sensibilidad, contraste y resolución necesarios para identificar adecuadamente el origen de la intrusión en cualquier condición de iluminación de producción.

Se implementa con equipos que permiten la detección y verificación de un evento de intrusión en áreas críticas ubicadas al interior de la instalación. Este subsistema se presenta para futuras ampliaciones de sitios críticos dentro de las instalaciones de Genérica S.A que podrían ser integradas al sistema. Pero no hacen parte del alcance de esta propuesta.

#### **4.5.5 Subsistema de Integración.**

El subsistema de integración permitirá la integración de todos los componentes y subsistemas del Sistema para que respondan en forma unificada, incluyendo el procesamiento, despliegue, gestión y registro de la información operativa, alarmas, eventos de detección, señales de video, acciones de los operadores y demás actividades que contribuyan a la gestión y control del mantenimiento del sistema.

El subsistema de integración gestiona también la información relativa al mantenimiento, especialmente el plan de mantenimiento, control de ejecución del mantenimiento preventivo y correctivo. Este subsistema permite también la medición y el cálculo de los indicadores para la administración de los Niveles de Servicio: TBF, TTR, TBSI, Tiempos de Respuesta, Eventos no Gestionados, FAR, NAR, Disponibilidad, etc. (Indicados en el numeral 10 de este documento)



Las características de este subsistema permiten filtrar, clasificar y jerarquizar las señales generadas por los componentes del sistema, las cuales serán enviadas al centro de control, y tienen la capacidad necesaria para gestionar múltiples eventos concurrentes. Los eventos se anuncian a través de medios auditivos y visuales, proporcionando al operador la ubicación del evento y toda la información necesaria para su verificación y evaluación.

El sistema permite monitorear y controlar todos los subsistemas desde una estación de trabajo, integrando el manejo de alarmas de intrusión, CCTV, relevos de salida, manejo de mapas gráficos, transmisión en red, señales de audio, entre otros y permite automatizar varios procesos, de tal manera que cuando un evento de intrusión es detectado, una respuesta programada activa varias acciones y minimiza la posibilidad de error del operador.

La integración de los subsistemas se apoya en un software que efectúa el procesamiento, normalización y estandarización de las señales provenientes de los componentes y subsistemas, permitiendo su despliegue y gestión conjunta y armónica de tal manera que se optimiza la respuesta ante cada evento, e incluye la capacidad de realizar automáticamente funciones tales como:

- Asociar la señal proveniente de la línea de detección perimetral con la señal de la cámara correspondiente, que responde repuntándose hacia la zona de ubicación del evento, facilitando la verificación.
- Relacionar gráficamente mediante una interface gráfica de usuario (GUI) avanzada, los eventos con su ubicación en el mapa, facilitando la evaluación por el operador y la iniciación del procedimiento adecuado de respuesta en cada caso que es sugerido por el sistema (los mapas y gráficos que usa el sistema son suministrados y mantenidos por



SEGURIDAD TOTAL S.A, no obstante lo anterior Genérica S.A pondrá a disposición la base cartográfica disponible).

- Registrar los eventos debidamente identificados y fechados con las imágenes correspondientes y la descripción de las acciones tomadas en respuesta por parte del operador del sistema, manteniendo un registro automático y unificado de dichos eventos que permiten su revisión y análisis con el fin de alimentar los procesos de toma de decisiones.
- Mantener un registro unificado de los reportes de fallas, las acciones tomadas y en general las tareas de mantenimiento realizadas sobre el sistema y el historial de cada componente o equipo.
- Todas las señales generadas en los subsistemas por eventos, programación o mando del operador son registradas y almacenadas digitalmente durante 90 días, permitiendo su consulta de acuerdo con perfiles de usuario y características de seguridad asignadas previamente. Para los eventos, el registro de CCTV incluye un lapso previo al evento de 10 segundos, el momento mismo y un lapso posterior, así como las acciones tomadas por el operador en cada caso.
- El sistema provee las herramientas necesarias para buscar, consultar, respaldar o realizar copias de los registros de los eventos o rutinas. Para la búsqueda se dispone de filtros por los diferentes criterios que pueden ser asociados a cada uno de dichos eventos o rutinas. Los formatos y configuraciones utilizados para reportes especiales son salvados para su uso rutinario. La capacidad de consulta y reporte está relacionada con el perfil del usuario y los reportes generados por cada usuario son adecuadamente registrados.



- Para su administración el sistema permite la configuración y parametrización remota; estas tareas sólo podrán ser ejecutadas por usuarios con el nivel de autorización apropiado. Las labores de administración del sistema están registradas de manera que hay trazabilidad por fechas, administrador, subsistema o equipo intervenido.
- El sistema lleva un registro de todos los eventos inherentes a su funcionamiento así como de todos los cambios de configuración u otras tareas de administración del sistema y los intentos de acceso permitido o fallido.
- El sistema permite la identificación y localización automática o asistida de fallas. Cada módulo o dispositivo efectúa un autotest y reportar el estado de funcionamiento, en caso de falla se reporta en el centro de control, donde se direcciona la información a mantenimiento para tomar las acciones correctivas necesarias, dentro de los parámetros de servicio.
- El sistema cuenta con una base de datos de conocimiento para apoyar la labor de mantenimiento donde se informa al técnico las posibles alternativas de solución.
- El sistema mantiene un registro de las labores de mantenimiento programadas o eventuales con el fin de permitir su trazabilidad y evaluar sus resultados.

En nuestra propuesta, el subsistema de integración está soportado en tres plataformas, en la plataforma StarNet 1000 desarrollada por Senstar Stellar, que permite la gestión de los eventos de los subsistemas de Detección perimetral, el software Winpak que controla el sistema de control de acceso y también se tendrá



la plataforma “R5” de March Networks que optimiza los procesos de administración y manejo del video y capacidad de grabación de los DVR, haciendo uso de las variables de resolución, velocidad de grabación (FPS) y calidad, al igual que optimiza los recursos de red disponible para permitir la mejor transmisión de señales de video en este caso a través de la red LAN de seguridad. Todo lo anterior se automatizara con el desarrollo del Integrator.

El Sistema Integrador estará en capacidad de realizar respaldos de información a medios magnéticos tales como DVD o CD, estos respaldos pueden ser programados de forma automática por capacidad del sistema o por cronograma.

A continuación se mostrarán las características y prestaciones del Integrator, en adelante DI.

El DI soporta por completo las características de mantenimiento y diagnóstico remoto de todos los dispositivos que permiten esta funcionalidad, tales como: procesadores OmniTrax, IntelliFlex, DVR, Cámaras, PC, Radios de Comunicación. Todo esto a través de diferentes métodos de diagnostico según el caso.

El módulo de mantenimiento del DI permite programar todas las actividades de mantenimiento del sistema y equipos, de manera automática registra y crea un archivo histórico de todas las fallas de los equipos mencionados anteriormente. De manera adicional permite la creación de fallas de equipos que no poseen esta funcionalidad, tales como pantallas, Sensores, baterías, paneles solares, entre otros. El módulo de mantenimiento también permite la creación de reportes de acciones de mantenimiento, cálculo y reportes de niveles de servicio, base de datos de personal de servicio técnico.



Este desarrollo personalizado generara la base de datos de conocimiento, la cual servirá para solucionar futuros casos de fallas en equipos de una manera más ágil y oportuna.

DI puede automatizar las respuestas de seguridad y brindar al operador un punto de control único para las tareas en las cuales el tiempo es crítico durante respuestas a alarmas de emergencia para así incrementar en gran medida la eficiencia de cualquier sistema de seguridad.

Las pantallas del DI establecen niveles de exigencia con pantallas despejadas de respuesta a emergencias que libran al operador de obstrucciones innecesarias y aun así brindan información crítica y acceso inmediato para la asistencia adaptable al contexto y otras opciones de control más sofisticadas.

DI permite emitir mensajes audibles de acontecimientos específicos, procesamientos automatizado de acontecimientos y gráficos de alta resolución específicos del lugar, características que el personal de mantenimiento del usuario final puede modificar con facilidad para satisfacer requisitos y preferencias locales.

Es necesario que el operador teclee los datos para sólo unas pocas funciones administrativas y el resto de la interacción será por medio de un mouse intuitivo, una lista de comandos y/o interface, lo cual aumenta en gran medida la velocidad y precisión de las respuestas del operador a situaciones de emergencia y reduce los costos de capacitación.

El DI además del diseño de interface GUI se extiende también a los módulos de supervisión y mantenimiento que son poderosas herramientas para mantenimiento de contraseñas, diagnósticos, configuración de sistema, informes. Los informes generados por el sistema, de forma automática o manual permiten



tener una estadística de los eventos de los diferentes elementos del Sistema, de hardware o software, con lo cual se realizara la gestión de los niveles de servicio.

Los procesos se pueden personalizar por completo:

- Biblioteca de anuncio de audio con archivos "WAV" predeterminados que se pueden asociar con alarmas y acontecimientos de operación. Se puede importar o crear archivos WAV adicionales por medio de programas estándar de grabación de audio y un micrófono
- Módulos de operación, supervisión y mantenimiento protegidos con contraseña

El DI es suficientemente flexible para adaptarse y recibir cualquier cantidad de sitios.

El sistema permite monitorear y controlar todos los subsistemas desde una estación de trabajo, integrando el manejo de alarmas de intrusión, CCTV, relés de salida, manejo de mapas gráficos, transmisión en red, señales de audio y permitiendo automatizar varios procesos, de tal manera que cuando un evento de intrusión sea detectado se dará una respuesta programada, que dará inicio a la ejecución de un proceso de respuesta automatizado, previamente evaluado entre los asesores de Seguridad, que guiará al operador hacia el procedimiento más adecuado minimizando la posibilidad de error.

Los equipos de detección perimetral OmniTrax e IntelliFlex se integran mediante la interface NIU que convierte la información de estado y alarmas de las unidades procesadoras más la información ya integrada de los equipos del subsistema de vigilancia específica a datos seriales RS232.

#### 4.5.5.1 Arquitectura del Subsistema de Integración

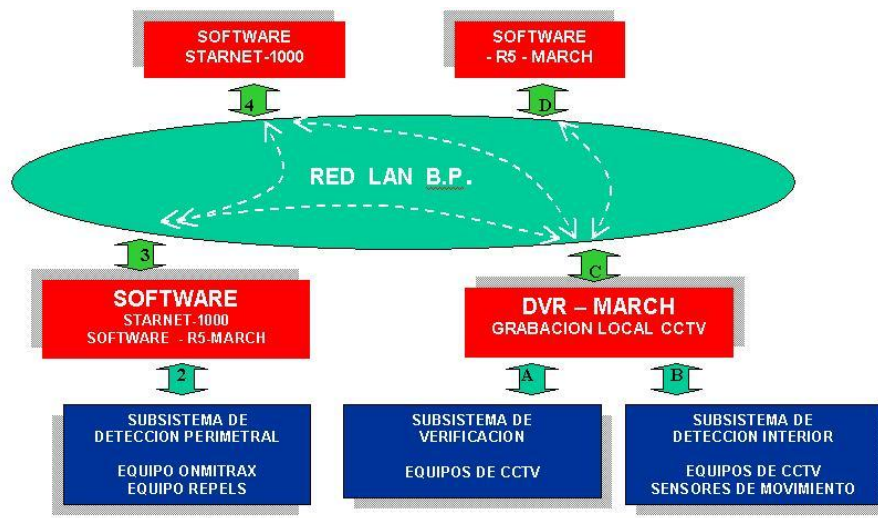


Figura 7. Arquitectura Subsistema de Integración SSE. Autor.

Los equipos en donde reside el software StarNet 1000 de Senstar Stellar y el software R5 de March Networks, permiten tener una base local de datos y registros de todas las alarmas y acciones que se han tomado sobre el sistema, asociados a todos los subsistemas , para un periodo de 90 días.

Si se desea se puede consultar de manera local la base de datos de información de alarmas y también se puede realizar la consulta y revisión del equipo DVR que de manera local guarda las grabaciones de video de vigilancia y verificación.

Todo el subsistema de integración dispone de medios de seguridad y control de acceso lógicos con más de cuatro niveles funcionales de operación así:



- Nivel de monitoreo:

En el nivel de monitoreo se recibirán, para su gestión y registro en el sistema, los eventos generados por los equipos de detección y la imagen de las cámaras dedicadas a tareas de vigilancia y verificación.

En este nivel también se proveerá acceso a los registros recientes de los sensores e imágenes de vídeo de la instalación, así como a la información relacionada con la programación diaria de mantenimiento. Esta función es permanente y puede ser local o remota.

- Nivel de supervisión:

En el nivel de supervisión estarán disponibles tanto las imágenes de las cámaras, los registros históricos del sistema, relacionados con eventos y las acciones tomadas en cada caso, así como los registros de mantenimiento. La función de supervisión se ejecutará de manera rutinaria y/o periódica y podrá hacerse de manera local en la instalación (donde haya centro de monitoreo) o remota. El nivel de supervisión estará habilitado para la extracción y cálculo de los índices para medición de los niveles de servicio.

- Nivel de consulta gerencial:

En el nivel de consulta gerencial se tendrá acceso a toda información y a los registros históricos del sistema, relacionados con eventos, acciones tomadas, imágenes de las cámaras, labores de mantenimiento y lo referente a la administración del sistema. Esta función se ejecutará remotamente y de manera eventual.

- Nivel de administración:

En el nivel de administración parametrizará todo el sistema, en particular lo referente a características de registro, asociaciones entre sensores y



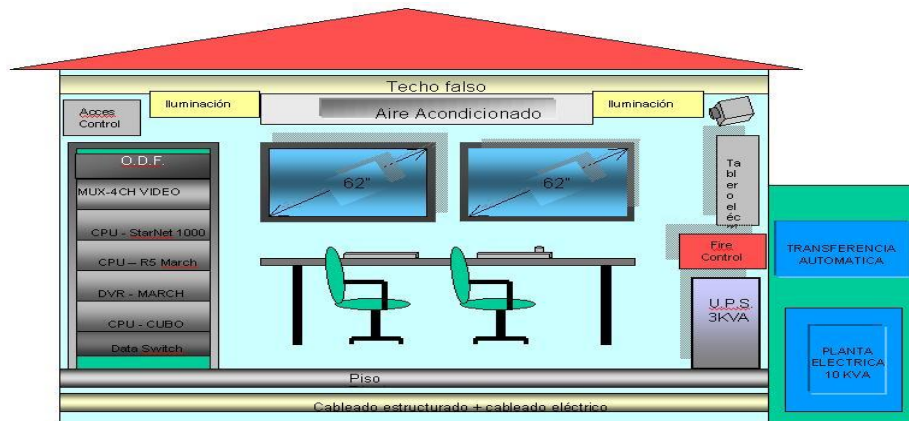
cámaras, zonificación de sensores, formatos de búsqueda de información, perfiles de usuarios, etc.

#### **4.5.6 Cuarto de Control Del Sistema De Seguridad Electrónico.**

El Cuarto de Control del Sistema de Seguridad Electrónico será implementado en la zona de producción. En él se podrá obtener toda la información integrada de todos los componentes y subsistemas para que respondan en forma unificada, incluyendo el procesamiento, despliegue, gestión y registro de la información operativa, alarmas, eventos de detección, señales de video, acciones de los operadores y demás actividades que contribuyan a la gestión y control del sistema, para cumplir los niveles de servicio ofrecidos en esta oferta.

Será el único sitio de operación local permanente del sistema, para ello estarán siempre personal en turno, los 365 días del año. En él se encuentran todos los equipos que harán posible la integración de todas las señales de avisos de alarma proveniente de las demás locaciones involucradas en el proyecto de seguridad.

Para su diseño y adecuación se han tenido en cuenta todas las normas técnicas en cuanto a: ergonomía, salud ocupacional, HSE, adecuaciones locativas, instalación técnica de equipos, protecciones, seguridad eléctrica, suministro con respaldo de energía, cableados eléctrica, cableada de datos y de seguridad física.



**Figura 8.** Configuración de equipos Sala de Control. Realizada por Autor.

En la Figura 8 se pretende hacer un resumen gráfico de los componentes de la sala de control del Sistema, se procederá a hacer una descripción de los elementos y equipos constitutivos.

#### **4.5.7 Adecuaciones Locativas.**

Genérica S.A deberá proveer un sitio adecuado para la instalación del centro de control de mínimo 5 x 5 metros.

Este sitio deberá proveer como mínimo los siguientes requisitos.

- Instalación de piso falso antiestático en recubrimiento de micarta, en paneles de 60cmx60cm, con soportes metálicos que permiten un espacio libre de hasta 30cm.
- Instalación de luz zona de producción rias fluorescentes de encendido rápido en unidades de 2X40w con control de encendido independiente inalámbrico.
- Instalación de equipo de aire acondicionado centralizado.
- Resane, pintura de muros, mantenimiento de ventanas, puertas y mantenimiento de instalaciones sanitarias (Si las hay).



- Polarización de vidrios
- Instalación de cortinas o persianas
- Construcción de sistema de puesta a tierra para equipos del cuarto de control

#### **4.5.7.1 Instalaciones Eléctricas y equipos de Energía.**

SEGURIDAD TOTAL S.A implementará las siguientes instalaciones:

- Instalación de tablero de distribución para energía eléctrica regulada y no regulada, en cofre metálico de sobre poner, con totalizador, breaker para 10 circuitos y alojamiento para protecciones eléctricas tipo TVSS.
- Instalación de canaletas metálicas de 20cmx10cm con división central para poder alojar cableado de fuerza y de baja señal
- Instalación de tomas de energía tipo hospitalario de tierra aislada y tomas de puntos lógicos de voz y de datos.
- Instalación de ductos y cableados de sistemas de detección de incendios y control de accesos.
- Instalación de UPS con tablero de bypass para labores de mantenimiento.

#### **4.5.7.2 Instalación de equipos del SSE.**

SEGURIDAD TOTAL S.A implementara las siguientes instalaciones:

- Instalación de Rack de 19" - 2 pies de altura, con multi-tomas y organizadores para cableados internos.
- Instalación de equipos del Sistema al interior del Rack de 19"
  - Servidores
  - CPU sistema de visualización
  - Switch de datos



- Sistema de Audio

- Instalación de pantallas de visualización tipo de 32 pulgadas con soportes.

#### **4.5.7.3 Mobiliario para operadores.**

SEGURIDAD TOTAL S.A implementara las siguientes instalaciones:

- Instalación de puestos de trabajo para operadores
- Instalación de sillas ergonómicas de cinco apoyos para operadores
- Instalación de mueble archivador
- Dispensador de agua

#### **4.5.7.4 Equipos de comunicaciones.**

- Instalación de línea telefónica y aparato telefónico
- Instalación de equipo radio base

### **4.6 NIVELES DE SERVICIO OFRECIDOS**

El nivel de servicio permitirá evaluar la calidad de servicio y respuesta de los elementos para el sistema electrónico de seguridad, a través del manejo estadístico de los datos ingresados a la plataforma de administración del sistema.

### **4.7 LISTADO DE EQUIPOS Y PROGRAMAS (SOFTWARE)**

Según nuestras investigaciones las frecuencias que utilizan los equipos listados en la siguiente tabla, son de uso libre. Por lo tanto no es necesario la adquisición y/o pago de licencias.



Se hizo la correspondiente consulta ante el Ministerio de Comunicaciones y ellos suministraron las resoluciones que lo reglamentan, las adjuntamos a este documento para que sean plenamente revisadas.

Sin embargo esperamos la respuesta del ministerio al respecto por escrito donde se verifique esta información, consulta ya hecha por nosotros formalmente.

EQUIPO	FRECUENCIA	POTENCIA
OmniTrax	27 – 37MHz	Regulable. Máx. 100mW
IntelliFlex	N / A	NA
INNOVONICS	902 - 928MHz	-20 dBm (min), +5 dBm (typ)
VERINT	2.412 - 2.472 GHz 5.470 - 5.725 GHz	11dBm 3 - 17dBm

En caso de necesitar una licencia para uso de frecuencias por cambio de reglamentación, o por cualquier motivo, durante el contrato, para los equipos propuestos, SEGURIDAD TOTAL S.A asumirá los costos que se generen, sin cambio en los precios ni en los niveles de servicio.

#### **4.8 DESCRIPCIÓN DE LA INFRAESTRUCTURA Y CANTIDADES**

El proyecto tendrá la infraestructura técnico-administrativa necesaria para el cumplimiento de los niveles de servicio ofrecido y el diseño en general.

Para dar cumplimiento estricto al contrato SEGURIDAD TOTAL S.A cuenta con un equipo interdisciplinario de apoyo disponible que en cualquier momento del contrato estarán a disposición del proyecto.



Adicionalmente el proyecto cuenta con equipo permanente de profesionales dedicados de manera exclusiva al proyecto.

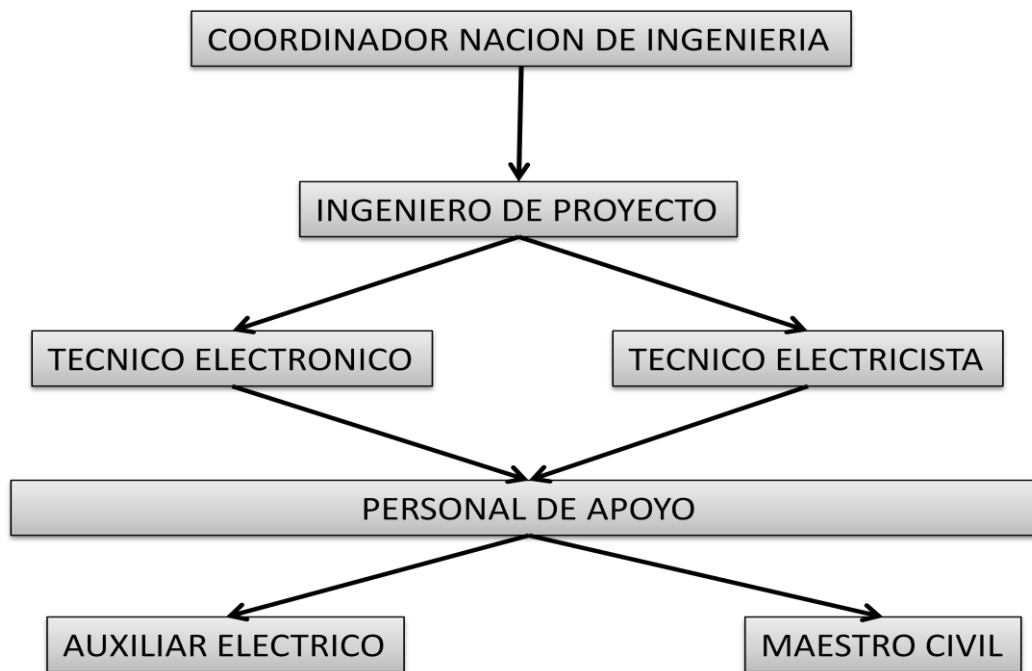
A lo anterior se suma la tecnología de punta y sistemas automatizados de administración y gestión para el sistema, que dará como resultado un óptimo funcionamiento del esquema de seguridad planteado.

El número de elementos de seguridad, control y gestión ha sido cuidadosamente seleccionado así como el número de personal necesario para operar y mantener los niveles de servicio esperado.

SEGURIDAD TOTAL S.A basa su selección de cantidades teniendo en cuenta los siguientes aspectos

- Experiencia específica (Proyecto seguridad electrónica BP)
- Requerimientos de seguridad física
- Requerimientos de seguridad Industrial (HSE)
- Limitaciones físicas, ambientales, económicas, operación y movilidad

#### **4.8.1 Área técnica**



**Figura 9.** Organigrama área de tecnología. Realizada por Autor.

Para cumplir los indicadores de servicio para los sistemas y servicios ofrecidos por SEGURIDAD TOTAL S.A, se contempla la siguiente estructura con la cual se dará cumplimiento a los tiempos máximos y porcentajes de disponibilidad.

**Coordinación Técnica:** El coordinador técnico se encargará de dirigir las operaciones técnicas relacionadas con el soporte especializado al Grupo Técnico del proyecto en campo desde Bogotá asegurando la continuidad y disponibilidad del servicio. El coordinador será responsable de dar solución a cualquier inquietud y/o necesidad adicional del cliente.

**Supervisor Técnico:** Encargado de los procesos de instalación, mantenimiento preventivo, mantenimiento correctivo, soporte técnico, todo lo relacionado con la instalación y puesta en funcionamiento del sistema electrónico de seguridad para las instalaciones del Proyecto de Seguridad Electrónica.



Para tal fin SEGURIDAD TOTAL S.A designará un ingeniero electrónico especializado que trabajara en horario administrativo en las instalaciones de Genérica S.A y tendrá disponibilidad de las 24 horas del día.

Grupo Técnico: Este equipo está compuesto por 1 técnico especializado que tendrán bajo su responsabilidad el mantenimiento preventivo y correctivo del sistema.

#### **4.9 COMUNICACIONES**

La topología del sistema electrónico de seguridad para las instalaciones de Genérica S.A, plantea la integración de diversos elementos, cuya información es transmitida por los diferentes medios de comunicación inalámbricos y cableados.

Se describen a continuación los subsistemas con los diferentes medios de comunicación a emplear.

Todo el tráfico de datos que viajara a través de las redes del sistema estará encriptada por seguridad de 128 bits y no podrá interferirse en ningún punto de la comunicación.

##### **4.9.1 Transmisión Inalámbrica de Videocámaras (Térmicas, Domos, Fijas).**

- Se instalará una solución inalámbrica punto-a-punto (Verint S1100), la cual consiste de dos unidades; transmisor y receptor.
- El transmisor digitaliza el video proveniente de cámaras análogas y lo transmite a través de bandas libres de operación (2.4 / 5.3-5.8 Ghz).

- La salida del receptor se enlaza al sistema de CCTV y se visualiza a través de sus respectivos monitores, posee un puerto serial (RS-232) para el manejo y control de Cámaras Domo con funciones PTZ.
- La encriptación AES con rotación de llave de 128-bits permite tener un alto nivel de seguridad durante la transmisión inalámbrica de video.

NETWORK	Nextiva SDCF
RF Interface	802.11a/802.11g PHY with proprietary MAC protocol
Frequency	2.40-2.4835 GHz (ISM) 5.250-5.350 GHz (U-NII 2) 5.470-5.725 GHz (DFS) 5.725-5.825 GHz (U-NII-3/ISM)
Modulation	OFDM
Output Power	2.4 GHz 19 dBm 5.x GHz 18 dBm
System Gain	2.40-2.4835 GHz with 8.5 dBi gain antenna: 126 dB 2.40-2.4835 GHz with 16 dBi gain antenna: 141 dB 5.250-5.350 GHz with 13 dBi gain antenna: 131 dB 5.250-5.350 GHz with 18 dBi gain antenna: 136 dB 5.725-5.825 GHz with 13 dBi gain antenna: 132 dB 5.725-5.825 GHz with 18 dBi gain antenna: 142 dB
Range (RF Line of Sight)	2.40-2.4835 GHz (8.5 dBi): up to 3.9 miles (6.3 km) 2.40-2.4835 GHz (16 dBi): up to 11.4 miles (18.3 km) 5.250-5.350 GHz (13 dBi): up to 3.2 miles (5.2 km) 5.250-5.350 GHz (18 dBi): up to 5.3 miles (8.5 km) 5.725-5.825 GHz (13 dBi): up to 3.3 miles (5.3 km) 5.725-5.825 GHz (18 dBi): up to 6.2 miles (10 km)
Data Rate (Max Burst Rate)	6, 9, 12, 18, 24, 36, 48 and 54 Mbps
Channel	2.4 GHz: 11, 3 non-interfering 5.3 GHz: 4, non-interfering 5.4 GHz: 11, non-interfering (DFS) 5.8 GHz: 5, non-interfering
Encryption Protocols	128-bit AES with auto key rotation RTP/IP, UDP/IP, TCP/IP

**Figura 10.** Especificaciones Técnicas Verint S1100. Extraído de Hoja técnica de las antenas Verint S1100.

#### 4.10 GRABACIÓN DIGITAL DVR'S Y PLATAFORMA DE ADMINISTRACIÓN DE VIDEO

La plataforma de administración ESM (Enterprise Service Manager) para el sistema de video grabación DVR (March Networks), proporciona al usuario autorizado un conjunto de funciones para configurar y controlar eficazmente toda una red de sistemas de DVR's extensos a través de una red de área local (LAN) o corporativa. Asimismo, ayuda a los integradores a conseguir una rápida

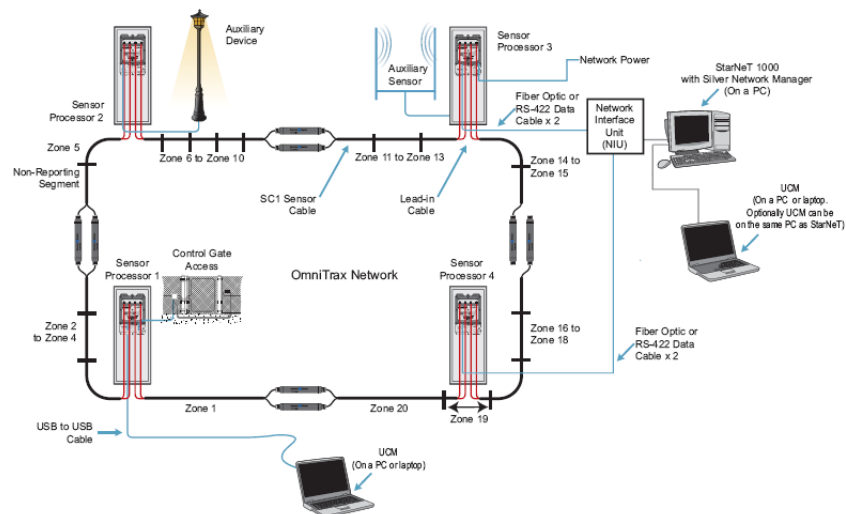


implementación y verificación de nuevas instalaciones de sistemas. El software contribuye a incrementar la eficacia del departamento de seguridad y a disminuir los costos de operación gracias a su arquitectura de administración centralizada de todas las DVR's. La posibilidad de funcionamiento multiusuario, local o remoto proporciona un acceso inmediato a vídeo en directo o grabado. La seguridad por contraseña garantiza que únicamente los usuarios autorizados puedan recuperar y revisar vídeo.

El software de administración para las DVR puede administrar cualquier número de DVR locales o remotas y reconocer automáticamente unidades nuevas agregadas a la red IP. El software controla la configuración y las características de todas las entradas de vídeo, audio, alarmas y dispositivos periféricos conectados a la DVR.

Cada DVR posee un puerto de conexión principal RJ-45 10/100 BaseT, conexión a PSTN vía adaptador opcional USB para módem o terzona de producción, DHCP habilitado, configuración opcional SNMP, y sincronización de hora NTP. La velocidad de bit o cuadro es limitada por el ancho de banda, lo cual puede configurarse a nivel global o por cámara específica, también posee cualidades de adaptación para redes de ancho de banda reducido.

## Sistema de Detección de Intrusión.



**Figura 11.** Sistema de Detección de Intrusión. Extraído de Hoja técnica Sensor Stellar Omnitrax.

### 4.11 CABLE SENSOR OMNITRAX

El sistema de protección perimetral, está compuesto por un cable sensor (Omnitrax) distribuido longitudinalmente por la periferia del lugar a proteger, procesadores de información, interfaz de comunicación entre procesadores y el software de administración (StarNet 1000). Este cable permite calibrar su sensibilidad metro a metro y de esta manera compensar las variaciones del terreno con el fin de adaptarse a las condiciones topográficas.

Adicional a la detección de intrusión, el cable sensor Omnitrax puede usarse para transmitir la potencia de una única fuente a cada uno de los procesadores de información que lo componen, como también, recolectar la información de alarmas



y datos de cada uno de los procesadores en la red, con el fin de proporcionar el control y despliegue de la información en el software de administración (StarNet 1000).

El cable OmniTrax es único para facilitar la detección, distribución de potencia y recolección de datos sobre un único cable de detección distribuido.

#### **4.12 CABLE SENSOR INTELLIFLEX**

Las unidades independientes de detección tales como; sensores infrarrojos independientes, como los sistemas de detección perimetral IntelliFlex, comunicaran sus estados de alarma a través de kit de transmisión inalámbrica INNOVONICS FA464DR (Frecuencia 900Mhz) de 16 canales cuyas salidas se incorporan a módulos de 16 entradas del DVR.

#### **4.13 UNIDADES PROCESADORAS DE INFORMACIÓN**

La red del sistema de detección de intrusión consiste de un software de administración SNM (Silver Network Manager), el cual controla las comunicaciones y transporta el estado y las ubicaciones de las alarmas a un sistema de observación como el StarNet 1000.

El Network Interface Unit (NIU) es una interface entre el software SNM y el procesador para el cable sensor. La comunicación entre procesadores se realiza a través del cable sensor, y la comunicación entre los procesadores y la interfaz NIU se realiza vía RS-422 o también cable de datos cuatro pares o por par de fibras multi-nodo.

La señal de datos es regenerada completamente en cada procesador con el fin de evitar la degeneración de datos.



Adicionalmente, el procesador cuenta con módulos de entrada y salida para el control de elementos externos, tales como; sensores auxiliares, actuadores (Lámparas), etc.

Posee ocho (8) salidas de relevos y ocho (8) entradas supervisadas.

#### **4.14 COMUNICACIÓN ENTRE ZONA DE PRODUCCIÓN Y CIUDADELAS**

Para la comunicación entre la zona de producción y las ciudadelas se instalara un sistema inalámbrico de red para 10 kilómetros, este equipo permitirá manejar un ancho de banda de hasta 10 MB, que se usaran exclusivamente para el sistema de seguridad electrónica. Las antenas se instalaran en las mismas torres de comunicaciones de Genérica S.A.

### **5. ANÁLISIS FINANCIERO**

Según información suministrada por el cliente GENERICA S.A. dieron como pauta el presupuesto aproximado que tenían asignado para los 60 meses de duración del contrato este valor oscilaba entre cuatro ciento millones de pesos (\$400.000.000).

Se presenta una propuesta ajustada a las necesidades de seguridad y financieras solicitadas por el cliente, en los siguientes cuadros mostraremos como llevamos a cabo este ajuste financiero a nuestra propuesta, y también mostraremos la adición del componente de seguridad electrónica como un plus para ganar la licitación.



Cuadro 1: Porcentajes aplicados a la propuesta.

DTF Proyectado 5 años	5,57%
Spread autorizado por tesorería	15%
Tasa mes vencido	1,78%
Plazo del contrato	60
Residual de los equipos	0%
Valor administración del Contrato	
Seguridad electrónica	8%
Tasa seguros corriente débil 1.67 por mil	0,00167

En este cuadro 1 observamos que se muestra los porcentajes que se aplicara a la propuesta, estos valores son estándares que maneja la compañía y depende principalmente de la duración del contrato y del costo que tendrá el mismo.

Cuadro 2: Valor equipos de seguridad electrónica.

<b>Costo de los equipos</b>	
COSTO EQUIPOS TOTAL	\$ 1.374.680.347
<b>Total Costo de Equipos</b>	<b>\$ 1.374.680.347</b>
<b>IVA</b>	\$ 219.948.855
<b>EQUIPOS CON IVA</b>	<b>\$ 1.594.629.202</b>
<b>Total Instalación de Equipos</b>	<b>\$ 1.594.629.202</b>
<b>Precio Total equipos de seguridad electrónica</b>	<b>\$ 1.594.629.202</b>

El cuadro 2 es el resultado de un cuadro en donde se enumeran todos los equipos a instalar con sus respectivos costos.

Cuadro 3: Valor del mantenimiento a los equipos.



<b>TARIFA MANTENIMIENTO CORRECTIVO Y PREVENTIVO MENSUAL</b>	<b>\$ 11.326.963</b>
<b>Costo del mantenimiento preventivo y correctivo anual</b>	<b>\$ 135.923.561</b>

Una de las figuras principales en este proyecto es que los equipos durante todo el tiempo del contrato serán del contratista y está obligado a mantener todos los equipos al cien por ciento de su funcionamiento durante los 60 meses, entonces se deberá destinar una cuota mensual para el mantenimiento correctivo y preventivo de los equipos.

Cuadro 4: Valor de la cuota mensual propuesta por Seguridad Total.

<b>Calculo de la cuota mensual Servicios de Seguridad</b>	
<b>Pago mensual servicio de vigilancia humana</b>	<b>\$ 325.731.000</b>
<b>Equipos de seguridad electrónica</b>	<b>\$ 43.417.693</b>
<b>Seguros</b>	<b>\$ 221.919</b>
<b>Mantenimiento</b>	<b>\$ 11.326.963</b>
<b>Reposición de equipos</b>	<b>\$ 3.720.801</b>
<b>Administración</b>	<b>\$ 3.473.415</b>
<b>Cuota mensual servicios de seguridad Electronica</b>	<b>\$ 62.160.793</b>
<b>Cuota mensual servicios de seguridad</b>	<b>\$ 387.891.793</b>

En el cuadro 4 vemos el resumen discriminado de todos los valores que irán a componer la cuota mensual que pagara el cliente por todo el servicio de seguridad física y electrónica, de esta forma nos ajustamos al presupuesto destinado por el cliente para este servicio.

## PRESUPUESTO DE CAJA

<b>CONCEPTO</b>	<b>Inicial</b>	<b>Mes 1</b>	<b>Año 1</b>	<b>Año 2</b>	<b>Año 3</b>	<b>Año 4</b>	<b>Año 5</b>
<b>INGRESOS</b>							
Cuota Seguridad Física		\$387.891.793	\$4.654.701.516	\$4.654.701.516	\$4.654.701.516	\$4.654.701.516	\$4.654.701.516
Cuota Seguridad Electrónica		\$62.160.793	\$745.929.516	\$745.929.516	\$745.929.516	\$745.929.516	\$745.929.516
<b>TOTAL INGRESOS</b>	\$0	\$450.052.586	\$5.400.631.032	\$5.400.631.032	\$5.400.631.032	\$5.400.631.032	\$5.400.631.032
<b>EGRESOS</b>							
Costo Vigilancia	\$185.731.000	\$185.731.000	\$2.228.772.000	\$2.340.210.600	\$2.457.221.130	\$2.580.082.187	\$2.709.086.296
Costo Ingeniería y mantenimiento	\$20.330.576	\$20.330.576	\$243.966.907	\$256.165.252	\$268.973.515	\$282.422.190	\$296.543.300
Compra de Equipos	\$1.594.629.202	\$15.946.292	\$191.355.504	\$191.355.504	\$191.355.504	\$191.355.504	\$191.355.504
Reembolsables	\$140.000.000	\$140.000.000	\$1.680.000.000	\$1.680.000.000	\$1.680.000.000	\$1.680.000.000	\$1.680.000.000
<b>TOTAL EGRESOS</b>	\$1.940.690.778	\$362.007.868	\$2.664.094.411	\$2.787.731.356	\$2.917.550.149	\$3.053.859.881	\$3.196.985.100
Flujo Neto Anual	\$1.940.690.778	\$88.044.718	\$2.736.536.621	\$2.612.899.676	\$2.483.080.883	\$2.346.771.151	\$2.203.645.932
Mas: Saldo Inicial de Caja	\$0	-\$1.940.690.778	\$0	\$2.736.536.621	\$5.349.436.297	\$7.832.517.180	\$10.179.288.331
<b>SALDO FINAL DE CAJA</b>	\$1.940.690.778	-\$1.852.646.059	\$2.736.536.621	\$5.349.436.297	\$7.832.517.180	\$10.179.288.331	\$12.382.934.263

## 6. CONCLUSIONES Y RECOMENDACIONES

Como conclusión se puede decir que para lograr un cambio exitoso, los 4 factores (visión, consistencia, participación, adaptabilidad) de la cultura organizacional deben de estar muy fuertes, las estrategias para el cambio que se propongan deberán de orientarse a lograr el mejor balance entre estas 4 dimensiones.

Además se recomienda tomar en cuenta que la resistencia al cambio no se da por capricho necesariamente, sino como un proceso natural de reacción ante lo que se percibe como una amenaza de probable pérdida o desajuste, de tal forma que se debe de lograr un exitoso proceso del cambio orientado hacia la efectividad y salud organizacional deseada

Conocer a profundidad los procesos y necesidades del cliente para acerca nuestras propuestas económicas a la realidad de los requerimientos del cliente.

Tener en cuenta los estándares técnicos manejados por la compañía a la cual vamos a licitar, nos ayudara a dimensionar de mejor forma el presupuesto de la instalación.

Reconocer los entornos cambiantes en donde vamos a intervenir, para diseñar en áreas específicas sistemas flexibles, que permitan realizarles modificaciones dependiendo de las variaciones que surjan en el tiempo.

Como conclusión se puede decir que para lograr un cambio exitoso, los 4 factores (visión, consistencia, participación, adaptabilidad) de la cultura organizacional deben de estar muy fuertes, las estrategias para el cambio que se propongan deberán de orientarse a lograr el mejor balance entre estas 4 dimensiones.



Además se recomienda tomar en cuenta que la resistencia al cambio no se da por capricho necesariamente, sino como un proceso natural de reacción ante lo que se percibe como una amenaza de probable pérdida o desajuste, de tal forma que se debe de lograr un exitoso proceso del cambio orientado hacia la efectividad y salud organizacional deseada

Al ajustar nuestros costos y ganancia a una cuota mensual por debajo de los costos destinados por el cliente para este contrato nos llevo aumentar nuestras posibilidades de ganar la licitación.

También la forma de pago en forma de leasing es un punto valioso a nuestro favor ya que el cliente podría pagar el valor del contrato de una forma mas cómoda y ajustada a sus necesidades.

La implementación de los sistemas de seguridad electrónicos industriales, deben ser manejados con la responsabilidad adecuada, es decir, que su utilización le permita a las organizaciones satisfacer las necesidades y que al mismo tiempo generen mayor producción y mejor rentabilidad.

Recordar que un sistema de seguridad no evita que pasen las cosas, solo las puede disuadir y proporcionar evidencia a posteriori de lo que haya pasado.

Al ofrecer un contrato tipo leasing, lo hace mas atractivo para el cliente el cual no deberá realizar una inversión muy fuerte al inicio del contrato sino que pagara una cuota durante un tiempo determinado, permitiéndole dirigir estos recursos que se debería tener en un principio a otras necesidades propias de su negocio.

Para que una compañía pueda ofrecer contratos del tipo leasing deberá tener en cuenta el tiempo de duración del contrato para encontrar un punto de equilibrio y de esta forma recuperar su inversión y en adelante recibir utilidad.



Una de nuestras estrategias como empresa es que poseemos diversas unidades especializadas en diferentes áreas de la seguridad, lo cual nos permite ofrecer a nuestros clientes paquetes integrales y que se acomoden a sus necesidades.



## 7. BIBLIOGRAFIA.

Grob Bernard, TELEVISIÓN PRACTICA Y SISTEMAS DE VÍDEO, Marcombo, 18/04/1990 – 453 páginas.

Kruegle Herman, CCTV SURVEILLANCE, Second edition, Video Practices and technology, BH, 2007 – 643 páginas.

Rashid Muhammad H., ELECTRONICA DE POTENCIA, Circuitos, dispositivos y aplicaciones, tercera edición, Pearson Prentice Hall, 2004 – 873 páginas.

Guerra Sotillo Alexei, Cambios, Organización y Entorno, Apuntes para su estudio.

UNAD, Modulo Administración y Gestión de proyectos, Modulo de la materia 210111.

Rubio Salvo Víctor, Estrategias para el cambio, De una “cultura productiva” a la cultura de “producir con seguridad”.

Página web de la empresa Innotegia –Cadena de valor de la innovación [http://www.innotegia.com/index.php?option=com\\_content&view=article&id=8&Itemid=11](http://www.innotegia.com/index.php?option=com_content&view=article&id=8&Itemid=11) extraído el 04 de Diciembre de 2011

Emprendedores.es –La siete fuentes de la innovación. [http://www.emprendedores.es/empresa/noticias/las\\_siete\\_fuentes\\_de\\_la\\_innovacion](http://www.emprendedores.es/empresa/noticias/las_siete_fuentes_de_la_innovacion) Extraído el 04 de Diciembre de 2011

Mendoza, Oliva (2010). Modulo: Iniciativa y Desarrollo Empresarial. UNAD. Disponible en: <http://66.165.175.253/moodle/mod/resource/view.php?id=1625> Recuperado el 4 de Septiembre de 2011.



Facultad de ciencias empresariales: Curso 2007 (3ra. Edición). Disponible en:  
<http://www.ucu.edu.uy/Facultades/CienciasEmpresariales/pcer/curso.htm>

Recuperado el 4 de Septiembre de 2011.

Pagina web <http://www.alarmasseguridad.com/vigilancia/camaras-vigilancia.html>

Extraído del 04 de Marzo del 2013.

Arriagada, Irma y Godoy Lorena. (1999). Seguridad ciudadana y violencia en América Latina: diagnóstico y políticas en los años noventa. Santiago de Chile.

Stephen, Robbins. (1998). La administración en el mundo de hoy. Prentice Hall. México. 608 p.

Romero Morales, Cristóbal, Vásquez Serrano, Francisco y Lozano Carlos de Castro. (2007). Domótica e Inmótica: Viviendas y edificios inteligentes. Alfa omega Grupo editor S.A de C.V. México.416 p.