

UNIVERSIDAD APEC



ESCUELA DE GRADUADOS

Monografía Para Optar Por El Título De:

Especialidad En Alta Gestión Empresarial

Título:

“Redefinición de los procesos del área de tecnología de seguridad electrónica de una empresa de telecomunicaciones en el periodo-2010-2011”. Caso específico Claro Codetel

Sustentante

José Miguel Soriano Hernández

Matrícula

1999-1036

Asesor(a):

Edda Freites, MBA

*Santo Domingo, D.N
Abril, 2010*

Tabla de Contenido

Introducción

Adendum

CAPITULO I - GENERALIDADES DE LA EMPRESA.....	1
1.1 Historia	2
1.2 Misión.....	7
1.3 Principios.....	7
1.4 Valores.....	8
1.5 Estructura del Dpto. de Tecnología de Seguridad Electrónica	9
CAPITULO II - TECNOLOGIAS DE SEGURIDAD	10
2.1 Sistemas de Detección de Intrusos (SDI)	11
2.2 Sistema Detección de Intrusos de la red.....	12
2.3 Sistema de Circuito Cerrado de Televisión (CCTV)	12
2.4 Sistema de Control de Accesos (SCA).....	14
2.4.1 Continuum.....	15
2.4.2 Door kery.....	15
2.4.3 Sigar IV.....	15
2.4.4 Mul-t-lock.....	16
2.5 Sistema de Control de Incendios (SCI)	16
2.5.1 Notifier	16
CAPITULO III – PROCESOS EXISTENTES	17
3.1 Procesos manejados en los sistemas de Detección de Intrusos y Control de Acceso	18
3.2 Procesos que maneja el Sistema de Control de Acceso SIGAR IV.....	19
3.3 Procesos que maneja del sistema CCTV.....	20
CAPITULO IV – DISEÑO DE NUEVOS PROCESOS	21
4.1 Centro de Monitoreo	22
4.2. Nuevos procesos	24
Conclusión.....	25
Bibliografía	26
Anexos	27

Introducción

La tecnología juega un papel fundamental en el área de seguridad Electrónica y en los últimos años la República Dominicana ha experimentando un incremento considerable de su uso. Es por esto que el buen uso de la tecnología debe ir apoyada de procesos que mejoren la gestión y el su uso.

La implementación y la redefinición de los procesos en el área de tecnología de seguridad electrónica, es lo que va a permitir que el área de protección integral pueda ofrecer un mejor servicio con calidad y respuesta efectiva a todas las novedades e incidentes que se reportan desde todas las localidades a nivel nacional.

El fenómeno social de la delincuencia, ha traído como consecuencia que tanto las personas como las corporaciones tengan que invertir grandes cantidades de dinero para la protección de su patrimonio. La modalidad de robo de cables, robo de baterías, combustible, fraudes y demás activos de la compañía, se ha convertido en un negocio lucrativo donde intervienen múltiples entes los cuales aprovechan cualquier brecha de seguridad para cometer los delitos.

La compañía Dominicana de Teléfonos es una empresa que tiene un alto capital en activos, esto hace que invierta montos considerables en lo que es la protección de sus activos. Con la restructuración del actual Centro de Monitoreo y su futura transformación en cuanto a su infraestructura física y en el cambio e implementación de nuevas tecnologías. Nada de esto sería lo suficientemente eficaz si no existen procesos bien definidos que permitan a la empresa ser proactivos y a la vez tener la suficiente agilidad cuando se tenga que reactivo.

Este trabajo pretende presentar un desglose de los procesos implementados y por implementar en el área de tecnología de seguridad de Claro Codetel.

Adendum

El principal objetivo de este trabajo fue redefinir los procesos y crear un centro de gestión para manejar todas las solicitudes hechas al departamento de Protección Integral, ser más eficientes en el uso de la tecnología con el fin de mejorar el tiempo de respuesta a las novedades y eventos notificados a nuestro centro de monitoreo.

Para lograr con los objetivos principales de este trabajo cumplí con los siguientes puntos:

1. Analicé los procesos existentes en el área de Tecnología de Seguridad Electrónica de Claro Codetel.
2. Adecué los procesos actuales a las exigencias de los nuevos tiempos.
3. Evalué la estructura existente.
4. Evalué la tecnología existente.
5. Definí el perfil de los integrantes del departamento de seguridad electrónica.
6. Definí cual será el nuevo esquema de trabajo y cuáles serán los nuevos procesos que intervendrán.

CAPITULO I - GENERALIDADES DE LA EMPRESA

1.1 Historia

La Compañía Dominicana de Teléfonos (CODETEL), fue constituida el 11 de noviembre de 1930, como subsidiaria de la Anglo Canadian Telephone Company, iniciando sus operaciones meses más tarde, en San Pedro de Macorís, con la instalación de la primera central telefónica automática fuera de Santo Domingo. Hasta 1930, el servicio telefónico había sido administrado por el Gobierno, pero al ser virtualmente destruida por el ciclón de San Zenón todas las instalaciones, este se vio imposibilitado de seguir operándolo.

El restablecimiento del servicio implicaba una reconstrucción total, para lo cual el Gobierno carecía de los recursos necesarios, a pesar de que Santo Domingo tenía apenas unos 500 teléfonos en servicio.

CODETEL suscribió entonces contrato con el Gobierno Dominicano, que traspasó oficialmente a la compañía la totalidad del servicio telefónico interprovincial, otorgándole franquicia exclusiva para la operación del servicio de larga distancia nacional e internacional.

La compañía adquirió posteriormente las franquicias de Santiago, Puerto Plata y La Vega y comenzó la reconstrucción de la red de interconexión de esos pueblos con la capital, que también había sido destruida casi completamente por el ciclón de San Zenón.

Otro fenómeno que tocó las puertas del país, dejándolo en condiciones de emergencia nacional, lo constituyó el huracán David en septiembre de 1979. Las destrucciones ocasionadas por este fenómeno dejaron las redes inservibles casi en su totalidad, por lo cual se requirió la asistencia de nuestra casa matriz, GTE, que envió técnicos que apoyaron y reforzaron la labor del personal local. No obstante haber caído a tierra el 30% de los cables del servicio telefónico, cinco semanas después los daños habían sido corregidos casi en su totalidad, demostrando CODETEL una vez más su fortaleza y eficiencia.¹

¹ www.codetel.com.do/pdf/historia.pdf

La historia del verdadero desarrollo de CODETEL comenzó en 1968, con la instalación del cable submarino, al que siguió la estación terrena para comunicaciones por satélite de Cambita Garabito, que llegó a conducir más del 60 por ciento del tráfico internacional.

Cable submarino y estación terrena vinieron a ser etapas preparatorias de uno de los acontecimientos más importantes en la historia de CODETEL: la integración del país a la red de marcación mundial por Discado Directo a Distancia (DDD), el 21 de noviembre de 1981.

Se hicieron posible entonces desde la República Dominicana a Estados Unidos, Canadá y parte de la Cuenca del Caribe, llamadas directas, sin asistencia de operadores. En noviembre de 1986 se completó la extensión del DDD a Centro y Sudamérica, Europa, Asia, África y Oceanía, conectando así con el más remoto rincón del planeta.

Conjuntamente con la expansión del DDD para abarcar el mundo, incorporamos una nueva tecnología, la del Cero Más, para llamar a través del Cero cuando sea necesaria una comunicación de persona a persona o con cargo.

Además de Estados Unidos, tenemos circuitos directos con Venezuela, Colombia, Curazao, Islas Vírgenes, San Martín, España, Italia, Holanda, Francia, Suiza, Antigua, Argentina, Aruba, Brasil, Canadá, Chile, Corea, Costa Rica, Cuba, Guadalupe, Haití, Hawái, Honduras, Japón, México, Nicaragua, Panamá, Perú, Puerto Rico y Tórtola.²

Tres sistemas sirven de soporte al servicio internacional: Estaciones terrenas para comunicación por satélite, cable submarino y microondas. La estación Júpiter ubicada en la urbanización Alameda, de Santo Domingo, está destinada especialmente al transporte de datos, lo que la hizo la primera de su tipo en Latinoamérica, y en el sector Altos de Virella, de Santiago, funciona la primera estación terrena digital para comunicaciones por satélite para transmisión de voz.

² www.codetel.com.do/pdf/historia.pdf

El cable submarino nos conecta con el mundo a través de Saint Thomas, Islas Vírgenes.³

El 14 de junio de 1990 entró en operación el cable transcaribeño de fibra óptica V Centenario que amplió los canales de comunicación de la República Dominicana con todo el mundo, especialmente con el Caribe, Sudamérica y Estados Unidos.

Este cable de fibra óptica permite el transporte de voz, data y señales de video a alta y baja velocidad, con una altísima calidad en las comunicaciones internacionales.

El sistema de microondas es una extensión de la red nacional, que nos conecta por el Oeste con Haití.

El 1986 marcó el año en que entramos de lleno en el campo de las innovaciones, al instalarse un anillo digital de fibra óptica para interconectar los principales centros alámbricos de Santo Domingo.

Fibra óptica es lo más moderno en materia de sistemas de transmisión de voz y datos.

Se trata de un finísimo tubo de vidrio, tan fino como una hebra de cabello humano, a través de la cual proyectamos un haz de luz que nos permite transmitir miles de conversaciones o miles de documentos al mismo tiempo.

El primer cable de fibra óptica que instaló CODETEL, para unir las centrales Duarte, Sánchez y 30 de Marzo, operaba con una capacidad de 45 Megabitios/segundo. Esto significa que la luz proyectada a través del hilo de vidrio podía encenderse y apagarse 45 millones de veces cada segundo, lo que permitía una capacidad de transmisión de alrededor de 760 conversaciones o su equivalente en datos, por cada par de fibra.

Antes de completar el primer año de funcionamiento la fibra óptica había pasado de 45 a 135 Megabitios/segundo. Esto hacía crecer nuestra capacidad de transmisión hasta 2,000 canales de voz o datos por cada par de fibra.

³www.codetel.com.do/pdf/historia.pdf

Al finalizar el año 1987, nuestras necesidades habían crecido a tal punto que nos obligaban a aumentar la capacidad de interconexión. Comenzamos entonces a utilizar los más avanzados sistemas disponibles hasta ese momento, 560 Megabitios/segundo, con lo cual alcanzamos una capacidad de ocho mil canales de voz o datos por cada par de fibra.

El 22 de septiembre de 1998 la infraestructura de nuestra empresa volvió a sufrir severos daños provocados por la furia del huracán Georges. Volvimos a poner a prueba nuestro alto sentido de responsabilidad, una vocación incesante de servicio y la efectividad del amplio engranaje organizacional que posee CODETEL en situaciones de emergencia.

A pesar de las dimensiones del fenómeno, logramos mantener la comunicación telefónica en un 85% durante el paso del huracán tanto en las localidades del interior del país como en el Distrito Nacional, aunque el nivel de daños provocados por los vientos incluyó caídas de torres de antenas y la destrucción de postes de las redes externas. Para la reconstrucción fue necesaria una inversión extraordinaria de más de 700 millones de pesos.

CODETEL fue por muchos años una subsidiaria de la corporación GTE, pero desde junio del año 2000, al fusionarse GTE con Bell Atlantic, seleccionaron a Verizon como el nuevo nombre bajo el cual la compañía combinada identifica sus servicios, y por tanto, Verizon es desde entonces nuestra casa matriz.⁴

El miércoles 31 de enero de 2007 fue un gran día para nuestra organización. Dimos un paso agigantado en nuestra exitosa trayectoria como líderes del mercado de telecomunicaciones en República Dominicana. A partir de ese día informamos con orgullo que las nuevas marcas para continuar comunicando a los clientes de Verizon son: Claro para la comunicación móvil, y Codetel para las comunicaciones fijas y de datos.

Claro es una marca de comunicaciones móviles que opera en Brasil, Perú, Chile,

⁴ www.codetel.com.do/pdf/historia.pdf

Honduras, El Salvador, Nicaragua, Guatemala y ahora República Dominicana. Es parte de América Móvil, el grupo de telecomunicaciones más grande en América⁵ Latina que cuenta con una red de más de 115 millones de clientes y la seguridad y solidez de estar en 15 países de Latinoamérica y EUA.

Como reconocimiento a más de siete décadas en el país, invirtiendo en el progreso y desarrollo del país, apoyando la cultura y siendo un ciudadano responsable, retomamos nuestra tradicional marca Codetel, que estará manejando todo lo relativo a comunicaciones fijas (alámbricas y de datos).

Entramos a un nuevo mundo de servicios y oportunidades. Dimos la bienvenida a un mundo mejor

El 15 de mayo se lanza a nivel nacional la cobertura de la nueva red GSM que incluye la red de datos GPRS.

El primero de octubre se lanza la red de datos UMTS/HSDPA que permite el acceso de bandas anchas con velocidades de hasta 2 megabits por segundo, a los clientes de las principales ciudades de la República Dominicana.

⁵ www.codetel.com.do/pdf/historia.pdf

1.2 Misión

Ser una organización líder en el mercado nacional de las comunicaciones, anticipándonos a las necesidades de nuestros clientes y superando sus expectativas con soluciones integrales de calidad mundial; excediendo los objetivos financieros para contribuir con el crecimiento de nuestros accionistas, generando bienestar y desarrollo para los empleados y la comunidad.⁶

1.3 Principios

Nuestro trabajo contribuirá al cumplimiento de la misión, siempre que se rija por los siguientes principios:

- Buscar la excelencia operacional enfocándonos en resultados y no en volumen de actividades.
- Desarrollar sistemas de trabajo orientados al cumplimiento de la misión, haciendo fácil nuestro servicio y la atención al cliente.
- Ser innovadores y creativos para proveer un servicio de máxima calidad, siendo flexibles para satisfacer las necesidades de nuestros clientes.
- Respetar, apoyar y estimular al personal, proporcionándole capacitación, autoridad y responsabilidad que le permita mejorar su desempeño y desarrollo profesional.
- Mantener nuestro servicio a la vanguardia tecnológica.
- Trabajar en conjunto con nuestros distribuidores autorizados para crear una relación de socios basada en el respeto, la confianza y profesionalismo.
- Aprovechar nuestras fortalezas y presencia a nivel nacional para proveer un servicio de excelencia a nuestros clientes.⁷

⁶ Código de Ética Compañía Dominicana de Teléfonos

⁷

1.4 Valores

Honestidad

Nuestra conducta es coherente con los más altos estándares éticos, cumpliendo con los compromisos establecidos y asumiendo siempre nuestra responsabilidad individual y colectiva.

Trabajo

Como actividad humana logra cubrir necesidades y al mismo tiempo, servir a los demás. Creemos en el trabajo esforzado y en equipo; actuamos lo mejor de nosotros para lograr transformar y mejorar de manera creativa el ambiente en que vivimos, fortaleciendo las relaciones interpersonales.

Austeridad

Ser austero significa cuidar y utilizar eficientemente lo que tenemos, optimizar el uso de los recursos y evitar desperdicios, implica gastar en lo necesario y prescindir de lo inútil o lo superfluo.

Manos en la Operación

Nuestros líderes, conocedores de las estrategias del negocio, de los empleados a su cargo y de las necesidades de los clientes, dirigen de manera cercana a su personal, involucrándose todos en la operación para lograr una gestión eficiente, que permita exceder las expectativas de nuestros clientes.⁸

⁸ Código de Ética Compañía Dominicana de Teléfonos

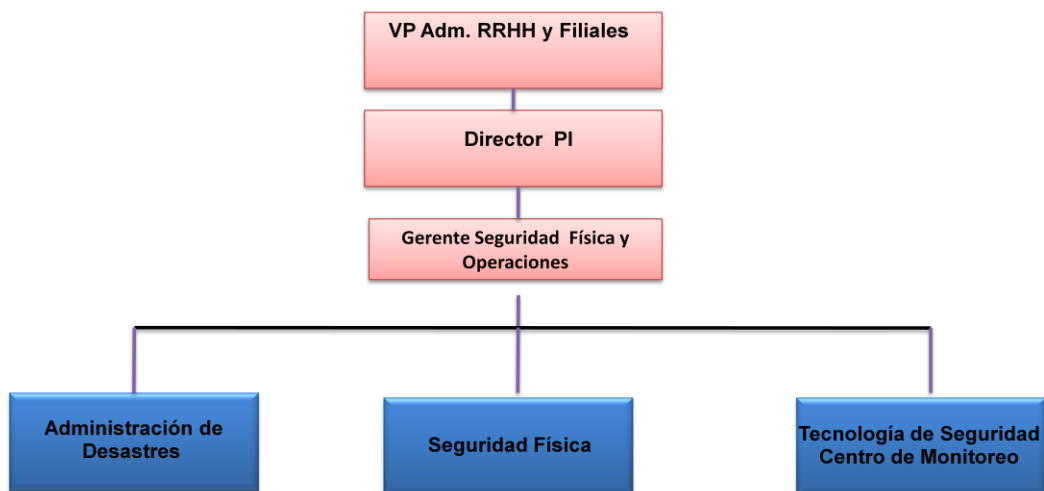
1.5 Estructura del Dpto. de Tecnología de Seguridad Electrónica

La sección de tecnología de seguridad electrónica reporta directamente al Gerente de Seguridad Física y Operaciones.

Esta sección está liderada por un Ingeniero en Sistemas con diez operadores que trabajan en el Centro de Monitoreo de Protección Integral (CMPI). El Centro de monitoreo es el centro de Operaciones del departamento de Tecnología de Seguridad, aquí es donde concentra la tecnología de seguridad y se manejan todos los sistema de seguridad de la empresa.

El organigrama del departamento es el siguiente:

Estructura de la Sección Seguridad Física y Operaciones



CAPITULO II - TECNOLOGIAS DE SEGURIDAD

2.1 Sistemas de Detección de Intrusos (SDI)

Son sistemas que cuentan de equipos o programas especializados cuya función principal es detectar los accesos no autorizados a localidades, computadores o a la red de personal no autorizado por la institución.

Entre los sistemas de Detección de Intrusos que existen el mercado en la empresa contamos con los siguientes:

2.1.1 Ademco Central Station

Recibidora de Señales de alarmas de detección de intrusos, botones de pánico y puertas abiertas en las localidades.

2.1.2 Netcool

Sistema vía web utilizado para recibir las señales de las alarmas de intrusos en localidades remotas, puertas abiertas, cabinas de baterías y accesos no autorizados.

2.1.3 Sistema Antirrobo de Combustibles y Baterías

Sistema desarrollado para el monitoreo de los tanques de combustibles y las baterías de las cabinas GSM, CDMA ubicadas en las localidades remotas. Este sistema emite una alarma audible a través de la red celular al centro de monitoreo.

2.1.4 Sistema Antirrobo de Cables

Sistema desarrollado para el monitoreo de los cables telefónicos y las baterías de las cabinas GSM, CDMA ubicadas en las localidades remotas. Este sistema emite una alarma audible a través de la red celular al centro de monitoreo.

2.2 Sistema Detección de Intrusos de la red

El Sistema de detección de intrusiones hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.

El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

2.3 Sistema de Circuito Cerrado de Televisión (CCTV)

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las

imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros. Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

Dentro de la gama de equipos y software que existen en el mercado para las CCTV, en la empresa utilizamos los siguientes:

2.3.1 Integral

A través de los equipos de la Marca Integral Technologies monitoreamos nuestros principales edificios y localidades a nivel nacional. Nuestro sistema primario de CCTV está compuesto por cámaras de alta resolución de la marca Pelco, equipos de transmisión y recepción a través de fibra óptica y monitores Pelco en nuestro centro de monitoreo para la visualización de las imágenes.

2.3.2 Eclipse Nubix

A través de los equipos de la Marca Eclipse específicamente el modelo Nubix, monitoreamos todos los Centros de Atención al Cliente a nivel Nacional. Esta tecnología nos permite monitorear dichos centros a través de nuestra red LAN.

2.3.3 Ip CCTV

Sistema de CCTV basado en tecnología IP.

A través de las cámaras basadas en IP tenemos monitoreados algunas localidades remotas. Esta tecnología nos permite tener una o varias cámaras conectadas solo con un cable de red, sin necesidad de algún otro equipo adicional. La misma nos permite conectarnos a la cámara a través de un browser o del un celular en cualquier parte del mundo a través del internet.

2.4 Sistema de Control de Accesos (SCA)

El Sistema de Control de Acceso es un sistema flexible y confiable para el control y monitoreo de accesos y control de tráfico y movimientos en sus instalaciones, este permite la captura de datos del empleado o visitante, creando un expediente electrónico del mismo que incluye datos, fotografía y huellas dactilares.

El sistema de control de acceso permite la verificación de datos electrónicos, huellas dactilares, fotografía y firma.

Podrá realizar consultas sobre el registro del visitante, la verificación de derechos de acceso así como la verificación de las huellas del visitante o empleado de la institución permitiendo altas, bajas o modificaciones a los derechos de acceso de acuerdo a los días de visita u horarios de trabajo.

El sistema puede manejar diferentes tipos de lectoras o dispositivos de entrada/salida como son las de contacto (banda magnética o chip), de

proximidad (Chip o Antena), lectora de huellas dactilares así como la combinación de ellas autenticando los datos o huellas con el gárate, dispositivo utilizado o con la base de datos local o de red de acuerdo a los derechos de acceso, permitiendo o rechazando el paso al empleado o visitante.

El Sistema puede mantener interrelación con sistemas de alarmas y alertas tales como circuito cerrado de televisión (CCTV), alarmas sonoras, alarmas visuales.

2.4.1 Continuum

El sistema de Control de Acceso que utilizamos es el Continuum de la empresa TAC (Tour Andover Controls).

Este sistema controla todos los accesos de los empleados, contratistas y visitantes de las principales localidades a nivel nacional.

2.4.2 Door kery

Sistema de control de acceso secundario. El mismo es utilizado para controlar todos los accesos de los empleados a las localidades remotas a nivel nacional. Este sistema cuenta con un teclado numérico en cada localidad donde está instalado que permite o no el acceso a los empleados o al personal autorizado a la puerta de la central. Para esto es necesario un PIN de 4 dígitos.

2.4.3 Sigar IV

Sistema desarrollado por la empresa Colombiana Insitel. El mismo controla las aperturas de las cabinas de planta externa que están ubicadas en las calles de las principales ciudades de las regiones Metro, Norte, Sur y Este. Este sistema permite tener el control de los técnicos que accedan a las cabinas telefónicas ya que para su apertura es necesario de una llave especial otorgada a cada personal autorizado y registrado en nuestra base de datos.

2.4.4 Mul-t-lock

Sistema de Candados, Cerraduras y Llaves utilizados para proteger las localidades de la empresa a nivel nacional. Este sistema cuenta con llaves exclusivas amaestradas por Zonas.

2.5 Sistema de Control de Incendios (SCI)

Los Sistemas Automáticos de Detección de Incendios tienen una importancia fundamental en la detección temprana de un incendio, para poder extinguirlo al inicio con medios manuales, como por ejemplo los extintores portátiles o por medio de las B.I.E.'S. (Redes Interiores de Bocas de Incendios Equipadas).

Un Sistema Automático de Detección de Incendios, está integrado por las siguientes partes:

A:) Central Automática de Detección de Incendios

B:) Sensores o Detectores de Incendio

2.5.1 Notifier

Sistema de detección de incendios fabricado por la empresa Honeywell. Este sistema inteligente cuenta con un panel digital y un sistema de evacuación por voz, activación de alarmas visuales y sonoras, así como también el manejo del sistema de supresión del incendio.

CAPITULO III – PROCESOS EXISTENTES

3.1 Procesos manejados en los sistemas de Detección de Intrusos y Control de Acceso

1. Activación y desactivación de las alarmas de las localidades (CACs).
2. Activación y desactivación de las tarjetas enviadas desde las diferentes recepciones.
3. Atender las llamas de los clientes con problemas de accesos.
4. Procesar los requerimientos enviados vía e-mail tales como:
Creación o eliminación de accesos previamente autorizados.
Brindar asistencia y en casos ajenos al CMPI canalizar las vías para su pronta ejecución y/o conclusión de manera satisfactoria.
5. Asistir a los técnicos que llaman al centro para las pruebas de los sistemas de alarma y accesos de las localidades a las cuales dan mantenimiento.
6. General reportes de los empleados solicitado/requerido por el personal de RRHH.
7. Procesar las alarmas que llegan por el sistema ADEMCO.
8. Actualización de las bases de datos de las diferentes localidades a las cuales los clientes no pueden acceder con el Pin Asignado.
9. Recarga de los paneles de acceso cuando uno de estos esta OFFLINE/Averiado y si es necesario reportarlo al personal técnico correspondiente.
10. Reportar las averías de los sistemas a la compañía contratista que le corresponda la solución de dicha avería.
11. Creación y asignación de pin de accesos a las localidades remotas con el control de acceso KERI previamente autorizado Gerente de Protección Integral.
12. Mantener un monitoreo constante en lo que se refiere al buen funcionamiento de los Sistemas Operacionales (Compass-ADEMCO, Door Keri, Micro Key Station, Continuum, DL900).
13. Actualización semanal de los reportes que conciernen al estatus de los Sistemas de Detección de Intruso (alarmas) y Sistemas Electrónicos de Acceso (Key Pad) y en caso de averías notificarlo al personal técnico correspondiente.
14. Velar por el buen funcionamiento de los equipos (hardware) operacionales del CMPI tales como: Computadoras, MODEM, Recibidoras, etc.

3.2 Procesos que maneja el Sistema de Control de Acceso SIGAR IV

1. Al iniciar la jornada de trabajo el operador del sistema debe generar un reporte, este consiste en verificar cada CR de la zona metro y norte, para así detectar las averías que se presentan a diario, este se genera desde el sistema SIGAR IV, el mismo detecta diferentes tipos de averías como son: comunicación CA en falla, línea conmutada, par abierto, ruido en canal, TA sobrealimentada, servomecanismo dañado, portadora en falla, IA en falla, CR en falla etc.
2. Este reporte debe ser enviado al personal de soporte técnico para darle seguimiento a cada avería. Corregida la avería el técnico debe comunicarse con el operador del SIGAR IV para este realizar las pruebas correspondientes y determinar que la CA funciona en condiciones normales.
3. Verificar las alarmas que llegan por el SIGAR Monitor, con este software podemos verificar las averías y eventualidades de todas las CA gestionadas por el SIGAR IV en tiempo real.
4. Desde la parte administrativa del SIGAR IV el operador gestiona otras funciones como son:
 - Programación y desactivación de llaves (llaves normales y maestras).
 - Reportes.
 - Inclusión y exclusión de empresas.
 - Inclusión y exclusión de empleados.
 - Otorgar cierres y aperturas a los técnicos (cuando las llaves presentan inconvenientes para acceder a las CA).
 - Crear CR y eliminar CR.
 - Configuración de alarmas.

3.3 Procesos que maneja del sistema CCTV

1. Supervisión de los sistemas de alarmas, cabinas, control de acceso y CCTV.
2. Supervisión de la asistencia de los representantes de la seguridad en los CACs.
3. Reporte del control de entrada y salida de los técnicos en las diferentes de la empresa.
4. Coordinación con los diferentes asistentes de seguridad en caso de novedades como Robo o Activación de sensores de movimiento.
5. reportes de alarmas recibidas, estatus de los sistemas manejados en el CMPI, novedades y/o robo.
6. Reportes de averías en las localidades las cuales son reportadas a los encargados del mantenimiento de dichas localidades.

CAPITULO IV – DISEÑO DE NUEVOS PROCESOS

4.1 Centro de Monitoreo

El centro de monitoreo es el lugar donde se manejan todos los procesos del departamento de tecnología de seguridad electrónica. Este centro con la entrada de los nuevos procesos que estará manejando el área, es necesario hacerle una restructuración completa.

En la actualidad el centro está dividido en dos áreas:

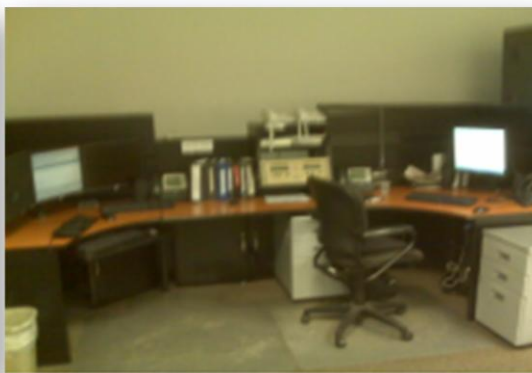
1. Monitoreo del control de acceso y detección de intrusos a localidades.
2. Monitoreo del sistema del CCTV (circuito cerrado de televisión).

Estas dos áreas son manejadas por diez operadores que trabajan las 24 horas los 7 días de la semana en turnos de 7:00 AM a 3:00PM, 3:00 PM a 11:00 PM a 7:00 AM.

Con la incorporación de los nuevos procesos y la restructuración que es necesario hacer en el centro de monitoreo pretendemos pasar de la actual infraestructura:



Monitores Sistema Visual Remoto



Sistema de Control de Acceso y Recibidora de Alarmas

A una nueva infraestructura más moderna, donde podamos integrar las tecnologías existentes en una sola plataforma que nos permita manejar los procesos existentes y los nuevos de una forma más óptima y con una mejora significativa en el servicio.

La propuesta sería la siguiente:



Sistema Visual Remoto



Detección de Intrusos y Sistema de Control de Incendios



Sistema de Control de Accesos



Sistema de Control de Fraudes

Este nuevo diseño permitirá la optimización del uso de los recursos, agrupando los procesos en grupos para un mejor desempeño de los operadores.

4.2. Nuevos procesos

La incorporación de los nuevos procesos es básicamente hacer una mejor distribución de los procesos existentes, incorporar algunos nuevos y dividirlos en los siguientes grupos:

- **Sistema de Detección de Intrusos (SDI)**

- 1) Monitoreo de las alarmas en las Localidades Críticas.
- 2) Monitoreo de las alarmas de los Centro de Atención de Clientes y Empresariales.
- 3) Monitoreo localidades a nivel general.
- 4) Monitoreo Red de TI

- **Sistema de Monitoreo Visual Remoto (SVR)**

- 1) Visualización vía CCTV de las Localidades Críticas.
- 2) Visualización vía CCTV de los Centro de Atención de Clientes y Empresariales.
- 3) Visualización vía CCTV de las Localidades a nivel general.

- **Sistema de Control de Accesos (SCA)**

- 1) Manejo del sistema de control de acceso de Personas y Vehículos
- 2) Manejo del sistema de Cabinas de PE (Plata Externa).

- **Sistema de Control de Incendios (SCI)**

- 1) Monitoreo del sistema de Incendios en las Localidades Críticas.
- 2) Monitoreo del sistema de Incendios en los Centro de Atención de Clientes y Empresariales.
- 3) Monitoreo del sistema de Incendios localidades a nivel general.

- **Sistemas de Detección de Fraudes**

- 1) Manejo de los sistemas de Fraudes Bypass
- 2) Manejo de los sistemas de Robo de Líneas
- 3) Manejo de los sistemas de Fraude Clone
- 4) Manejo de los sistemas de Fraude de Suscripción

- **Otros servicios**

- 1) Servicio al Cliente y Apoyo en general
- 2) Control de Proveedores de Servicios Contratados de Seguridad

Conclusión

Con la implementación de los nuevos procesos y la mejora de los procesos actuales, el centro de monitoreo de Protección Integral pasara a ser el Centro de Gestión de Protección Integral. Un centro donde estaremos dándole soporte a todas las áreas del departamento de protección integral y las operaciones se realizaran las 24 horas del día los 365 días del año sin interrupciones.

Esta transformación permitirá un mejor desempeño de los operadores en el uso de la tecnología y de los procesos que soportan a las mismas.

La integración de las diferentes tecnologías de seguridad en una sola plataforma, permitirá sacar mayor provecho de los recursos tecnológicos con que cuenta el centro de monitoreo.

La reestructuración del centro de monitoreo, permitirá reagrupar los procesos en procesos más simples para mejor optimización de los recursos, aumentar la calidad del servicio al cliente y mejorar el tiempo de respuesta.

Bibliografía

1. Kotler, Philip. (2006). Dirección de mercadotecnia: (12va. Ed.), México: Prentice – Hall.
2. Hill, Charles W. y Jones, Gareth R. (2005) Administración estratégica: un enfoque integrado: (6ta Ed.), Colombia: McGraw-Hill Interamericana
3. Historia de Codetel. Disponible: www.codetel.com.do/pdf/historia.pdf
4. Sistemas Automáticos de Incendios. Disponible:
[http://www.construmatica.com/construpedia/Sistemas Automáticos de Detección de Incendios](http://www.construmatica.com/construpedia/Sistemas_Automáticos_de_Detección_de_Incendios)
5. Sistema de Detección de Intrusos. Disponible:
<http://es.kioskea.net/contents/detection/ids.php3>

Anexos

Anexo 1: Anteproyecto Aprobado.

Anexo 2: Software para Integración de Tecnologías de Seguridad.

UNIVERSIDAD APEC



ESCUELA DE GRADUADOS

Anteproyecto De Monografía Para Optar Por El Título De:

Postgrado En Alta Gestión Empresarial

Título:

“Redefinición de los procesos del área de tecnología de seguridad electrónica de una empresa de telecomunicaciones en el periodo-2010-2011”. Caso específico Claro Codetel

Sustentante

José Miguel Soriano Hernández

Matrícula

1999-1036

Asesor:

Edda Freitas, MBA

***Santo Domingo, D.N
Enero, 2010***

Planteamiento del problema

En los últimos años la República Dominicana ha experimentando un incremento considerable en el fenómeno social de la delincuencia, esto ha traído como consecuencia que tanto las personas como las corporaciones tengan que invertir grandes cantidades de dinero para la protección de su patrimonio.

La modalidad de robo de cables, robo de baterías, combustible, fraudes y demás activos de la compañía, se ha convertido en un negocio lucrativo donde intervienen múltiples entes los cuales aprovechan cualquier brecha de seguridad para cometer los delitos.

La compañía Dominicana de Teléfonos es una empresa que tiene un alto capital en activos, esto hace que invierta montos considerables en lo que es la protección de sus activos. Esta inversión va desde la capacitación del personal hasta la adquisición de tecnología de punta para la parte de vigilancia y resguardo de sus bienes. Nada de esto sería lo suficientemente eficaz si no existen procesos bien definidos que permitan a la empresa ser proactivos y a la vez tener la suficiente agilidad cuando se tenga que reactivo.

Este trabajo pretende presentar un desglose de los procesos implementados y por implementar en el área de tecnología de seguridad de Claro Codetel.

OBJETIVOS DE LA INVESTIGACION

Objetivo General:

Redefinir los procesos del área de seguridad electrónica para ser más eficientes en el uso de la tecnología con el fin de mejorar el tiempo de respuesta al monitoreo de las alarmas en las localidades de la Claro Codetel.

Objetivos Específicos:

1. Analizar los procesos existentes en el área de Tecnología de Seguridad Electrónica de Claro Codetel
2. Adecuar los procesos actuales a las exigencias de los nuevos tiempos.
3. Evaluar la estructura existente.
4. Evaluar la tecnología existente.
5. Definir el perfil de los integrantes del departamento de seguridad electrónica.

JUSTIFICACION de LA INVESTIGACION

El presente trabajo se presentará todos los procesos que intervienen en el área de Seguridad electrónica de Claro Codetel. Este estudio está basado en una situación real de una empresa existente.

En la república Dominicana, se ha desatado en los últimos años una gran ola de delincuencia, donde individuos organizados en grandes bandas diariamente se dedican a robar los activos de las empresas de telecomunicaciones. Con la mejora de los procesos en el área de seguridad electrónica pretendemos mejorar el tiempo de respuesta para evitar y capturar a los delincuentes infraganti cuando estén delinquiriendo.

Marco teórico

Parte I

ASPECTOS TECNOLOGICOS

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, enfoque, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a

claros... Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

El modelo es considerado una arquitectura de redes, ya que especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas:

TABLA DE CONTENIDO

Capítulo 1: Generalidades de la empresa

Objetivo: En este capítulo presentaremos de manera general la empresa para así tener un mejor conocimiento de su estructura actual. Los sub-temas a tratar son:

- Historia
- Misión
- Principios
- Valores
- Estructura del Dpto. de Tecnología de Seguridad Electrónica

Capítulo 2: Tecnología de Seguridad

Objetivo: Aquí conoceremos los diferentes equipos y tecnología de seguridad electrónica con que cuenta Claro Codetel.

Capítulo 3: Procesos Existentes

Objetivo: Este acápite es el centro de nuestro trabajo, aquí presentaremos de forma clara como son los procesos con lo que cuenta la empresa Claro Codetel en el área de Tecnología de Seguridad Electrónica.

Capítulo 4: Diseño de Nuevos Procesos

Objetivo: En este renglón presentaremos los nuevos procesos que servirán para reforzar el área de Tecnología de Seguridad Electrónica.

Conclusiones

Recomendaciones

Glosario

Bibliografía

Anexos

Aspectos Metodológicos

El presente trabajo será desarrollado utilizando varios métodos y técnicas.

La metodología de la realización de la investigación se auxiliara de varias técnicas como:

1. Recolección de información de fuentes primarias y secundarias,
2. Análisis de las fuentes mencionadas en el punto 1
3. Planteamiento de posibles soluciones a los problemas actuales.

El método utilizado será el Método de Análisis, mediante este analizamos los datos encontrados tanto en la investigación documental como en la investigación de campo. Con este método queremos llegar al planteamiento de conclusiones y recomendaciones que permitan a la organización salir adelante.

.

DEFINICIONES CONCEPTUALES

AC: Corriente Alterna

AI: Auto iris - Función del objetivo que permite regular automáticamente la cantidad de luz que entra en el sensor CCD simulando el funcionamiento del iris en el ojo humano.

ALARMA: Capacidad de respuesta del componente de CCTV a un impulso o señal externa de alarma, se usa para iniciar funciones pre-programadas en dispositivos como por ejemplo activar la grabación de un VCR o que un Domo PTZ se mueva a una ubicación determinada (preset)

ANGULO DE VISION: Area de visión de una cámara, dependiendo de la lente instalada.

APERTURA: Número de apertura "F" mide la sensibilidad del lente indicando la cantidad de luz que deja pasar a la cámara. Si el parámetro F es bajo significa que los lentes son más sensibles.

AUX: Auxiliar.

BIT: Digito binario, es el más pequeño elemento de información de un sistema binario (base 2) su valor puede ser "1" o "0". En los circuitos eléctricos digitales generalmente el "1" corresponde a un nivel de voltaje cercano a 5VDC y "0" la ausencia de dicho voltaje o un valor inferior a 2.5VDC

BNC: Sistema de interconexión utilizado en video profesional. Usualmente es el Standard de los conectores que se ponen a los coaxiales y que tienen detrás los grabadores digitales (DVR)

BPS: Abreviatura de "bits por segundo". Generalmente se escribe con minúsculas: "bps"

BUS: Dos o más conductores que transportan datos o señales en una tipología que simula una "autopista principal" (el BUS) conectada a "calles secundarias" que le llegan perpendicularmente (conexión de los dispositivos). En la Topología de BUS cada dispositivo debe tener un identificador (numero, ID, o dirección) que lo distingue de los demás que envían y reciben datos por el mismo BUS.

BUS NETWORK: Red de datos para conectar los equipos en un solo bus de comunicaciones.

BYTE: Conjunto de 8 bits.

CATV: Antena de televisión de uso público (Cable TV)

CABLE COAXIAL: Cable que contiene un conductor central sólido recubierto de material aislante, una malla, y un forro o protector exterior. Muy usado para transportar señales de video, mucho tiempo atrás se uso para Redes de Datos (10 Mbps)

CCTV: Circuito Cerrado de Televisión - Sistema de Vigilancia Utilizado para ver imágenes / videos en privado y no para uso público.

CMOS: Complimentary Metal Oxide Semiconductor - Dispositivo de conmutación de estado sólido, Tipo de Sensor de imagen de video de las cámaras.

C-MOUNT: Tipo de montaje para cámaras de CCTV. Una lente con montaje C puede ser usado con una cámara con montaje CS con un anillo adaptador de 5

mm., una lente con montaje CS no puede ser utilizada en una cámara con formato de montaje C.

CODIFICACION: En la terminología del multiplexor indica que una grabación de video tiene una marca en el fotograma que impide su manipulación.

COMPRESIÓN: Métodos que permiten disminuir el tamaño inicial de una imagen digitalizada aplicando algoritmos que eliminan información "supuestamente" redundante a expensas de la calidad de la imagen final.

CPU: Central Processing Unit - Placa principal que contiene la programación de los sistemas. También se le llama así a los Microprocesadores.

CRT: Tubo de rayos catódicos - Dispositivo utilizado para visualizar las imágenes en un monitor o TV usando el principio de "lanzar" electrones acelerados hacia una pantalla luminiscente.

DC: Corriente Continua.

DESCOMPRESION: Transformar la información comprimida digitalmente y reproducir las imágenes de video normal.

DEFINICION: Capacidad de una cámara, monitor, videograbador, de reproducir fielmente las imágenes capturadas.

DISTANCIA FOCAL: La distancia focal de un objetivo se mide en milímetros, es una relación directa entre el ángulo de visión que se obtiene. Una distancia focal corta significa un ángulo de visión amplio y una distancia focal larga supone un pequeño ángulo de visión.

DUPLEX: En la terminología de los Equipos de CCTV indica que pueden hacer dos funciones simultáneamente, ejemplo: un DVR Dúplex puede mostrar los videos en vivo en el monitor y a la vez grabar.

ESCLAVO: Aparato secundario con funciones limitadas con respecto a la unidad principal (máster).

ESPECTRO SENSIBLE: Sensibilidad de un equipo de transmisión de imagen a diferentes frecuencias de luz. La luz visible es de 300 nm. A 750 nm. La luz infrarroja va de 715 nm. A 850 nm. Y es invisible en el espectro de 850 nm.

FIBRA ÓPTICA: Medio y/o Método para la transmisión de señales en forma de haces luminosos. Puede transmitir señales (datos, video o audio) a muy largas distancias (kilómetros) mediante

FIELD: Campo o Semicuadro: la mitad de una frame (cuadro) comprende 312,5 líneas cuando se trata de video análogo y barrido entrelazado.

FIELD OF VIEW: Campo o Angulo de Vista. El área de la imagen producida por una combinación de cámara y lente.

FM: Frecuencia modulada.

FORMATO IMAGEN: Se refiere al tamaño del plano de la imagen dentro de una cámara.

FOTOCELDA: Elemento electrónico usado para reconocer censar los niveles de intensidad o presencia de luz. Generalmente se usa para detectar niveles de luz bajos para activar o no iluminadores Infrarrojos.

FRAME (CUADRO): Una imagen de Video completa. 1 frame está compuesto de 2 field en el video análogo, y en el digital es como una foto estática. En el estándar de CCTV análogo o televisión el video tiene 30 frames por segundo (NTSC)

GIGA: Abreviatura de 10 elevado a 9 equivale a mil MEGAS

Hz: Hertzios - Ciclos por segundo: medida de la frecuencia.

ILUMINACION: Medida de la luz por metro cuadrado, la unidad de medida es el LUX.

ILUMINACION CON INFRARROJOS: Iluminación de una zona oscura por medio de emisores de luz en el espectro infrarrojo para permitir que se vean las imágenes aun en ausencia de luces visibles en la escena.

IMAGEN COMPRIMIDA: Una imagen reducida en tamaño que permite almacenar mas imágenes que en una imagen normal de video original.

IRIS: Mecanismo interno del lente para regular la cantidad de luz que pasa a través de él y llega al sensor CCD.

IR SHIFT: Diferencia de la sensibilidad de una cámara entre la visión normal y la luz Infrarroja

ISO: Organización Standard Internacional.

I/O: Entrada/Salida.

KILO: Abreviatura de 10 elevado a 3 o lo que es lo mismo: 1000

LAN: Local Área Network – Nombre dado a las Redes de Datos locales relativas a una Edificación. Usualmente con velocidad de 10Mbps a 1000 Mbps

LASER: Haz de luz concentrada y excepcionalmente pura que puede consistir en una sola longitud de onda (color), usada para transmitir datos, video o audio en forma de luz a través de fibra óptica.

LED: Diodo de Emisor de Luz.

LINEA DEDICADA: Conexión telefónica que permite una conexión punto a punto permanente.

LOOP DE TIERRA: Circulación de corriente eléctrica por la malla del cable coaxial causado por no poner correctamente la toma de tierra o por alimentar dispositivos en ambos extremos del cable de distintas fases eléctricas.

LOOPING: Característica de un equipo de video que permite que la señal de video pase a través de él para conectar otro equipo.

MATRIZ DE VIDEO: Conmutador de video que permite la visualización de entradas seleccionables (video de cámaras) en cualquier en monitores también seleccionables. También permite controlar las cámaras PTZ.

MEGA: Abreviatura de 10 elevado a 6 o sea (1, 000,000).

MODEM: Modulador/Demodulador - Dispositivo usado para enviar la señal digital (datos) a través de una línea analógica por línea telefónica.

MODULACION: Proceso de combinación de dos o más señales en la que una de ellas (la que representa la información) modifica ciertos parámetros de la otra (llamada portadora) y viajan como una sola por medios sólidos (ej.: cables) o por el aire.

MONITOR: Unidad de video usada para ver las imágenes de una cámara o de un ordenador. Similar a un televisor pero sin la parte relacionada a captar las señales de radio/tv.

MONOCROMATICO: De un solo color.

MULTIMODO: Fibra óptica que soporta más de un modo de propagación de la luz, generalmente tiene varios hilos.

MULTIPLEXOR: Equipo antiguo de CCTV capaz de visualizar a la vez en un monitor un número elevado de cámaras con salida para grabarlo en un solo video, similar a la matriz pero más sencillo y económico

MULTIPLEXADO: Capacidad/Procedimiento de sacar por una salida cualquiera o varias de múltiples entradas.

NANO: Abreviatura de 10 elevado a -9, o sea (0.000000001)

NTSC: National Television Standards Committee - Señal de video en color, estándar de la televisión en Norteamérica y Japón - 525 líneas, 60 Hz.

PICO: Subida de tensión o de señal momentánea.

PICO A PICO: Valor basado en diferencial entre el punto máximo positivo y el máximo negativo de una señal. Para las salidas de video es un estándar que tengan 1 Volt Pico a Pico.

PIP: Picture in Picture - Visualización de dos imágenes simultáneamente, una como un cuadro dentro de la otra, resultado del video digital.

PIXEL: Un punto en una imagen digital. El punto simple sensible de un sensor CCD o el más pequeño punto luminoso de un monitor LCD.

PRESET: Posición memorizada de las coordenadas horizontal, vertical y zoom, de una cámara robótica (speed dome) generalmente usada para ser activada a voluntad de un operador o automáticamente con alguna función programada como un recorrido o una alarma.

PROTOCOLO: Lenguaje de comunicación entre dispositivos que ha sido estandarizado.

PSTN: Public Switched Telephone Network - Red telefónica analógica utilizada para la transmisión de información de telefonía.

QUEMADO: Imagen que se "calca" en la pantalla de un monitor por haber estado mucho tiempo enfocando la misma imagen. Los "refrescadores de pantalla son para evitar este problema

REFLEXION: Nivel de luz que refleja sobre una superficie, normalmente expresado en tanto por ciento.

REPETIDOR: Dispositivo que amplifica y retransmite una señal.

RESOLUCION HORIZONTAL: Numero de líneas horizontales que componen una imagen de video

RESPUESTA DE FRECUENCIA: Capacidad de un dispositivo de detectar, transmitir o recibir una gama de frecuencias.

RUIDO: Efecto en pantalla que muestra elementos que no son parte de la imagen útil, como puntos, llovizna, nieve ondas, rallas. Es más evidente este efecto con baja luminosidad en escena.

SCANNER: Aparato para el control/posicionamiento/movimiento horizontal o vertical de la cámara.

SEÑAL DIGITAL: Una señal que ha sido convertida en "datos" y la conforma información binaria, es decir "1" y "0".

SINCRONIZACION: Dos o más impulsos eléctricos que se ejecutan con los mismos intervalos de tiempo para evitar la distorsión de imagen y el ruido.

TELEMETRIA: Método de señalización electrónica usado en el sistema de CCTV, para el control remoto de funciones de la cámara (horizontal, vertical, zoom, preset etc....)

TP: Twister Pair - Cable, apantallado o no, que consta de dos o más conductores trenzados a lo largo de toda su longitud.

TRANSDUCTOR: Aparato usado para convertir una ciertos tipos de energía en una señal eléctrica.

VARIFOCAL: Tipo de objetivo / lente que permite la regulación manual entre dos puntos focales para obtener el campo de visión deseado. Permite ajustar entre tomas más cercanas o lejanas

VELOCIDAD DE REFRESCAMIENTO: Tiempo utilizado para renovar / re-trazar completamente una imagen simple.

VIDEO COMPUESTO: Señal de video análogo completa, posee información tanto de vídeo como de sincronismos

VIDEO NO COMPUESTO: Señal de video completo pero que no incluye la información de sincronismo.

Anexo 2.

Software propuesto para la integración de las tecnologías y los procesos manejados en el área de seguridad electrónica.

Facility Commander Wnx Integrated Security Management System

