MODELACION DEL DIAGRAMA DE RED DE TELECOMUNICACIONES PARA TRANSMISION DE SEÑAL DE VIDEO DEL SERVICIO DE VIDEO- VIGILANCIA EN LA EMPRESA SERVICIOS DE VIGILANCIA Y SEGURIDAD DE BOYACA - SERVIBOY LTDA

SANDRA LILIANA PARDO RUIZ

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA ELECTRONICA

TUNJA

2016

MODELACION DEL DIAGRAMA DE RED DE TELECOMUNICACIONES PARA TRANSMISION DE SEÑAL DE VIDEO DEL SERVICIO DE VIDEO- VIGILANCIA EN LA EMPRESA SERVICIOS DE VIGILANCIA Y SEGURIDAD DE BOYACA - SERVIBOY LTDA

SANDRA LILIANA PARDO RUIZ

TRABAJO DE MONOGRAFIA PARA OBTENER EL TITULO PROFESIONAL DE INGENIERA ELECTRONICA

TUTOR DE TRABAJO DE GRADO:

ING. ELECTRONICO- OSCAR EDUARDO UMAÑA MENDEZ

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA ELECTRONICA

TUNJA

2016

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL PRESIDENTE DEL JURADO

_____

FIRMA DEL PRESIDENTE DEL JURADO

TUNJA,

AGRADECIMIENTOS

Primero que todo, agradezco enormemente a Dios, por el don de la vida y por las cosas bonitas que nos regala día a día, porque nunca me ha faltado techo ni comida, por regalarme a la hermosa familia que tengo, porque he gozado de buena salud y por permitirme estudiar y prepararme.

Infinitas gracias a mi mamá: MARTHA ELISA PARDO RUIZ, quien ha entregado su vida para darme todo lo necesario y más, y para verme feliz. Gracias a su dedicación, esfuerzos y desvelos, por estar paso a paso siempre a mi lado. Por conocerme tanto, por estar conmigo cuando estoy cansada, porque no me dejo desfallecer y me alentó a seguir. A mi hermana DIANA PARDO, gracias por ser mi compañera, mi guía, un modelo a seguir; por aportar mucho a mi crecimiento personal, porque me impulsa a ser una mejor persona. Las tres hemos ha llorado y reído juntas, apoyándonos incondicionalmente, y hemos compartido momentos inolvidables.

A mi abuela CLEMENCIA RUIZ, mil gracias por sus consejos, sus dichos, sus regaños y, aunque hoy ya no está con nosotros, sé que me cuidas desde el cielo. En general gracias a toda mi familia, tías, tíos, y demás, pues su compañía y colaboración también ha estado presente.

Agradezco a la universidad SANTO TOMAS, a todos ingenieros de la Facultad de ingeniería electrónica y a los demás docentes, quienes compartieron conmigo su conocimiento, experiencias personales y de vida. En especial le agradezco al ingeniero Oscar Umaña por su contribución, durante mi práctica profesional.

Le agradezco al Doctor CARLOS ALBERTO WAKED y al Ingeniero YAMIR LOPEZ, por darme la oportunidad de conocer el mundo laboral y en general, a todo el personal de SERVIBOY por dejarme ser parte de esta empresa y ayudarme a aprender tanto del trabajo y de la vida. Quiero agradecerle al ingeniero MIGUEL PIRACOCA, con quien establecí una excelente relación laboral, compartiendo e intercambiando conocimientos.

Finalmente, también agradezco a mis amigos y amigas con quienes compartí vivencias, en diferentes escenarios de la vida, y de una u otra manera, han aportado a mi aprendizaje personal.

TABLA DE CONTENIDO

AGRADECIMIENTOS 4
LISTA DE FIGURAS 10
LISTA DE TABLAS 12
GLOSARIO 13
RESUMEN 18
PROLOGO 19
INTRODUCCION 20
JUSTIFICACION 21
PLANTEAMIENTO DEL PROBLEMA 22
OBJETIVOS 23

1. MARCO REFERENCIAL 24
1.1. ¿QUE ES SEGURIDAD? 24
1.1.1. SEGURIDAD PÚBLICA 25
1.1.2. SEGURIDAD PRIVADA 26
1.1.3. INDUSTRIA DE LA SEGURIDAD PRIVADA 27
1.1.4. PERSONAL DE VIGILANCIA PRIVADA 27
1.1.5. CONTRASTE: SEGURIDAD PÚBLICA Y SEGURIDAD PRIVADA 29
1.2. LOS RIESGOS 30
1.2.1. ESCENARIO DE LOS RIESGOS 31
1.2.2. AGENTES O ACTORES DE LOS RIESGOS 31
1.2.3. TIPOS DE RIESGOS 31
1.3. ELEMENTOS BÁSICOS DE LA SEGURIDAD 34
1.3.1. EL OBJETO DE PROTECCIÓN: 35
1.3.2. LAS AMENAZAS O RIESGOS: 35
1.3.3. EL ESPACIO Y EL TIEMPO: 36
1.3.4. LOS MEDIOS DE PROTECCIÓN: 36
1.4. ALGO DE HISTORIA: SEGURIDAD PRIVADA 37
1.4.1. APARICION DE LA SEGURIDAD PRIVADA 37
1.4.2. LA SEGURIDAD PRIVADA EN LATINOAMERICA 38

1.4.3. LA SEGURIDAD PRIVADA EN COLOMBIA 39
1.5. SEGURIDAD ELECTRONICA 43
1.6. REDES DE TELECOMUNICACIONES 44
1.6.1. COMUNICACIÓN 44
1.6.2. INFORMACION 44
1.6.3. TELECOMUNICACIONES 44
1.6.4. ¿QUÉ ES UNA RED? 45
1.6.5. SISTEMA DE TELECOMUNICACIONES 45
1.7. ALGO DE HISTORIA: TELECOMUNICACIONES 46
1.8. RADIODIFUSIÓN 48
1.9. FORMAS DE TRANSMISION EN TELECOMUNICACIONES 52
2. ENTORNO 61
2.1. LA EMPRESA 61
2.2. UBICACION 61
2.3. DEPARTAMENTO DE INGENIERIA 63
2.3.1. COMMAND CENTER 65
2.3.2. RACK 67
2.3.3. EQUIPOS: COMMAND CENTER Y RACK 68
2.3.4. DESCRIPCION DE EQUIPOS 68
3. SISTEMAS DE CAMARAS 73
3.1. COMPONENTES DE LOS SISTEMAS DE CAMARAS 73
3.1.1. MEDIOS DE ADQUISICIÓN DE LA IMAGEN 73
3.1.2. MEDIOS DE TRANSMISIÓN DE LA IMAGEN 74
3.1.3. MEDIOS DE VISUALIZACIÓN: MONITORES 74
3.1.4. MEDIOS DE REPRODUCCIÓN: VIDEOGRABADORES 74
3.1.5. MEDIOS DE TRATAMIENTO DE LA IMAGEN 75
3.2. DESARROLLO DEL TRABAJO 75
3.2.1. CONOCIMIENTO DE LOS TIPOS DE DISPOSITIVOS: 75
3.2.2. VISITAS REALIZADAS A LOS USUARIOS: APLICACIÓN DEL CONOCIMIENTO ADQUIRIDO: 75
3.2.3. OBJETIVOS DE LA VIGILANCIA CON SISTEMA DE CAMARAS 76
3.3. EVOLUCION DE LA TECNOLOGIA DE SEGURIDAD POR CAMARAS 76
3.4. TIPOS DE SISTEMAS DE CAMARAS 78

3.4.1. CIRCUITO CERRADO DE TELEVISION 78
3.4.2. VIDEO- VIGILANCIA 78
3.5. EQUIPOS PARA LA VIGILANCIA CON SISTEMAS DE CAMARAS 79
3.5.1. DESCRIPCION DE EQUIPOS PARA VIGILANCIA CON SISTEMAS DE CAMARAS 80
3.6. INSTALACION DE SISTEMAS DE CAMARAS 83
3.7. MODIFICACIONES EN LA DOCUMENTACION 85
3.7.1. IMPLEMENTACION DEL FORMATO PARA REPORTAR MANTENIMIENTOS 85
3.7.2. REALIZACION DE MANUALES 85
3.8. CAPACITACION 86
3.9. ATENCION A LAS NECESIDADES DE LOS USUARIOS 86
4. RED DE TELECOMUNICACIONES 87
4.1. ESTRUCTURA 87
4.2. REDES INALAMBRICAS 87
4.2.1. TOPOLOGIAS 88
4.2.1.1. MODO AD HOC: 88
4.2.1.2. MODO INFRAESTRUCTURA: 88
4.3. IEEE 802.11 89
4.4. CARACTERIZACION DE LA RED 91
4.5. SISTEMA DE COMUNICACIONES DE LA EMPRESA 91
4.5.1. ROUTER CISCO 92
4.5.2. PATCH PANEL - PANEL DE CONEXIONES 92
4.5.3. ROUTER INALAMBRICO TP- LINK N750 93
4.5.4. CAJA CZ4530-000 FOWB-T 94
4.5.5. MODEM MARCA HUAWEI 94
4.5.6. ANTENAS 95
4.6. FORMAS EN QUE SERVIBOY ESTABLECE LA COMUNICACIÓN 97
4.6.1. ENLACES PUNTO A PUNTO 97
4.6.2. ENLACES PUNTO A MULTIPUNTO 97
4.6.3. PROTOCOLO DE TÚNELES PUNTO A PUNTO 98
4.7. MODELAMIENTO DE LA RED 99
4.7.1. UBICACIÓN DE LOS LUGARES MONITOREADOS 99
4.7.2. INFORMACION DE LA RED DE LA EMPRESA SERVIBOY LTDA 100
4.7.3. SOFTWARE 104

4.7.4. ESQUEMAS DE RED 105
5. OTRAS LABORES 109
5.1. SISTEMAS DE ALARMAS 109
5.1.1. EVOLUCION DE LOS SISTEMAS DE ALARMA 109
5.1.2. COMPONENTES DE LOS SISTEMA DE ALARMAS 110
5.1.2.1. SENSORES INFRARROJOS 111
5.1.2.2. BARRAS FOTOELECTRICAS 111
5.1.2.3. CONTACTOS DE APERTURA 111
5.1.2.4. DETECTORES DE ROTURA 112
5.1.2.5. TECLADO 112
5.1.2.6. SALIDA DE ALARMA 113
5.1.2.7. COMUNICADOR 113
5.1.2.8. PANEL DE CONTROL 114
5.1.3. EQUIPOS PARA EL MONITOREO DE LAS ALARMAS 114
5.1.3.1. CENTRAL Y RECEPTOR DIGITAL MULTI LINEA SG-DRL2A SG-CPM2 115
5.1.3.2. RECEPTORA DIGITAL PARA MONITOREO DE ALARMAS SENTRY PIMA 116
5.1.3.3. RECEPTORA VIRTUAL PARA MONITOREO DE ALARMAS OSM 116
5.1.3.4. SOFTWARE DE MONITOREO DE ALARMAS: BYKOM 117
5.1.4. MANTENIMIENTOS E INSTALACIONES 118
5.1.5. SISTEMAS DE COMUNICACION DE LAS ALARMAS EN SERVIBOY 118
5.2. CONTROL DE ACCESO 119
5.2.1. COMPONENTES DE LOS SISTEMAS DE CONTROL DE ACCESO 120
5.2.1.1. CABINA DE CONTROL O CONTROLADORA 121
5.2.1.2. DISPOSITIVOS DE IDENTIFICACIÓN 121
5.2.1.3. DISPOSITIVOS DE ENTRADA 122
5.2.1.4. DISPOSITIVOS DE SALIDA 122
5.2.1.5. RED DE COMUNICACIONES 122
5.2.1.6. SOFTWARE DE CONFIGURACION Y CONTROL 122
5.2.2. INTERVENCIONES EN LOS CONTROLES DE ACCESO 123
5.2.2.1. CONTROL DE ACCESO EDIFICIOS MONACO Y ALTOS DE VALIZA 123
5.2.2.2. CONTROL DE ACCESO VILLA TOSCANA 123
5.2.3. INSTALACIONES 124

5.2.4. IMPLEMENTACION DEL CONTROL DE ACCESO EN EL CONJUNTO MARIA FERNANDA 124
5.2.5. CAPACITACIONES 125
5.3. LABORES ADMINISTRATIVAS 125
5.3.1. INVESTIGACION SOBRE HABEAS DATA Y SU RELACION CON SERVIBOY 126
5.3.1.1. CONCEPTO 126
5.3.1.2. ANALISIS 126
5.3.1.3. PRINCIPIO DE CONFIDENCIALIDAD 126
5.3.2. CREANDO CONCIENCIA SOBRE LA COMUNICACIÓN EN LA EMPRESA 127
5.3.2.1. REPORTES DE FALLAS TECNICAS PARA EL DEPARTAMENTO DE INGENIERIA 127
5.3.2.2. IMPLEMENTACION DE LA MINUTA 127
5.3.3. CREACION DE CARPETAS PARA CADA UNIDAD MONITOREADA 128
5.3.4. COORDINACION EN EL COMMAND CENTER 128
5.3.5. PROYECTOS LIDERADOS 128
6. BASE DE DATOS 132
6.1. ¿EN QUE CONSISTE UNA BASE DE DATOS? 132
6.2. COMPONENTES DE UNA BASE DE DATOS 132
6.2.1. APACHE 133
6.2.2. MY SQL 134
6.2.3. PHP 134
6.3. CREACION DE LA BASE DE DATOS DE SERVIBOY LTDA 135
6.3.1. OBJETIVOS DE LA BASE DE DATOS DE SERVIBOY 135
6.3.2. DESARROLLO 135
6.3.3. VENTANAS DE LA BASE DE DATOS DE SERVIBOY LTDA 137
6.3.4. ANALISIS DE DATOS 138

CONCLUSIONES 139
RECOMENDACIONES 140
BIBLIOGRAFIA 141
INFOGRAFIA 142
ANEXOS 143

LISTA DE FIGURAS

FIGURA 1. SEGURIDAD: CAJA FUERTE 24
FIGURA 2. SEGURIDAD PÚBLICA 25
FIGURA 3. FUERZA PÚBLICA COLOMBIA: NAVAL, EJERCITO Y FUERZA AEREA 25
FIGURA 4. SEGURIDAD PRIVADA 26
FIGURA 5. VIGILANCIA HUMANA PRIVADA 40
FIGURA 6. UBICACIÓN DE LA SUPERVIGILANCIA EN EL ESTADO COLOMBIANO 42
FIGURA 7. SEGURIDAD ELECTRÓNICA 43
FIGURA 8. LAS TELECOMUNICACIONES 45
FIGURA 9. RED CON EQUIPOS TERMINALES 46
FIGURA 10. TRATAMIENTO DE LA SEÑAL DE VOZ 49
FIGURA 11. BARRIDO DE UNA IMAGEN 50
FIGURA 12. SISTEMA DE TRANSMISION DE RADIODIFUSIÓN 51
FIGURA 13. SEÑAL DIGITAL CON RUIDO 53
FIGURA 14. SISTEMA DE POLIBIO 54
FIGURA 15. a) CONVERSION ANALOGA-DIGITAL b) CODIFICACIÓN DEL MENSAJE 55
FIGURA 16. EJEMPLO DE ZONA AMBIGUA POR EFECTO DE RUIDO EN EL MENSAJE 57
FIGURA 17. TRANSMISION PUNTO A MULTIPUNTO 58
FIGURA 18. SISTEMA DE COMUNICACIONES CON TRANSFORMACIONES 59
FIGURA 19. LOGO SERVIBOY 61
FIGURA 20. SEDE PRINCIPAL DE LA EMPRESA 61
FIGURA 21. DISPOSITIVOS EMPLEADOS EN VIGILANCIA ELECTRONICA 63
FIGURA 22. PERSONAL VIGILANDO UN CCTV 64
FIGURA 23. CONTROL DE ACCESO 64
FIGURA 24. CENTRAL DE VIDEO- VIGILANCIA 65
FIGURA 25. COMMAND CENTER - SERVIBOY LTDA 66
FIGURA 26. RACK - SERVIBOY LTDA 67
FIGURA 27. CAJA DE CONEXIONES ELECTRICAS 69
FIGURA 28. ESQUEMA DE CONEXIONES PBX 70
FIGURA 29. PBX - SERVIBOY LTDA 70
FIGURA 30. TELEFONIA DIGITAL 71
FIGURA 31. ESQUEMA DE CONEXIONES PARA UNA LINEA ADSL 72
FIGURA 32. FUNCIONAMIENTO DEL SPLITER 72
FIGURA 33. CAMARA DE SEGURIDAD- SERVIBOY LTDA 73
FIGURA 34. MONITOR - SERVIBOY 74
FIGURA 35. DVR - SERVIBOY LTDA 75
FIGURA 36. SISTEMA ANTIGUO DE VIGILANCIA POR VIDEO 76
FIGURA 37. FOTO CAMARA IP 77
FIGURA 38. ESQUEMA GENERAL DE LA VIGILANCIA BASADA EN CAMARAS 79

FIGURA 39. DVR 81
FIGURA 40. VIDEO- BALUN 81
FIGURA 41. CABLE NEXT 82
FIGURA 42. SOFTWARE SIERA PANTHER 83
FIGURA 43. RED INALAMBRICA EN MODO AD HOC 88
FIGURA 44. RED INALAMBRICA EN MODO INFRAESTRUCTURA 89
FIGURA 45. RED INALAMBRICA QUE INTEGRA LOS DOS MODOS: AD HOC E INFRESTUCTURA 91
FIGURA 46. ROUTER CISCO DE LA SERIE 1900 92
FIGURA 47. PANEL DE CONEXIONES AMP NETCONNECT 93
FIGURA 48. TOPOLOGIA TIPICA FIGURA 49. TOPOLOGIA ESPECIAL 93
FIGURA 50. CAJA DE CONEXIÓN DE FIBRA OPTICA 94
FIGURA 51. MODEM MARCA HUAWEI 94
FIGURA 52. ANTENA NANOBEAM 95
FIGURA 53. CONEXIONES DVR- SERVIBOY 96
FIGURA 54. ENLACE PUNTO A PUNTO 97
FIGURA 55. ENLACE PUNTO A MULTIPUNTO 97
FIGURA 56. ESQUEMA DEL ENVIO DE SEÑAL AL COMMAND CENTER 98
FIGURA 57. UBICACIÓN DE SERVIBOY LTDA EN GOOGLE MAPS 99
FIGURA 58. SOFTWARE RADIO MOBILE: PROPIEDADES DEL MAPA 101
FIGURA 59. MAPA DE TUNJA CON LA UBICACIÓN DE LAS ANTENAS DE SERVIBOY LTDA 101
FIGURA 60. MAPA DE TUNJA EN EL PROGRAMA RADIO MOBILE 102
FIGURA 61. MAPA DE TUNJA EN EL PROGRAMA RADIO MOBILE 102
FIGURA 62. SOFTWARE RADIO MOBILE: PROPIEDADES DE LAS UNIDADES 103
FIGURA 63. SOFTWARE RADIO MOBILE: PROPIEDADES DE LAS REDES 104
FIGURA 64. INTERFACE DEL SOFTWATE AIR OS 105
FIGURA 65. MAPA DE RED EN EL PROGRAMA CISCO PACKET TRACER 106
FIGURA 66. MAPA DE RED EN EL PROGRAMA CISCO PACKET TRACER 106
FIGURA 67. ESQUEMA DEL MAPA DE RED 107
FIGURA 68. MAPA DE RED DE SERVIBOY LTDA 108
FIGURA 69. ALARMA ANTIGUA 109
FIGURA 70. ESQUEMA GENERAL DE LA VIGILANCIA CON ALARMAS 110
FIGURA 71. SENSOR INFRARROJO E INTRUSO 111
FIGURA 72. FOTO MAGNETICO EMPRESA 112
FIGURA 73. FOTO SENSOR EMPRESA 112
FIGURA 74. FOTO TECLADO DE ALARMA SERVIBOY 113
FIGURA 75. PANEL DE CONTROL DE ALARMA HONEYWELL 114
FIGURA 76. RECEPTORA SG-DRL2A SG-CPM2 115
FIGURA 77. RECEPTORA SENTRY PIMA 116
FIGURA 78. ESTRUCTURA DE LAS ALARMAS QUE COMUNICAN POR GPRS 116
FIGURA 79. INTERFAZ DEL SOFTWARE BYKOM 117
FIGURA 80. TIPOS DE CONTROL DE ACCESO 119
FIGURA 81. ESQUEMA DE UN SISTEMA DE CONTROL DE ACCESO 120
FIGURA 82. CONTROLADORA DE ACCESOS ROSSLARE 121
FIGURA 83. SOFTWARE CONTROL DE ACCESO 122

FIGURA 84. CARACTERIZACION DE UNA BASE DE DATOS 132
FIGURA 85. COMPONENTES DE UNA BASE DE DATOS 133
FIGURA 86. SIMBOLO MYSQL 134
FIGURA 87. ESQUEMA BASE DE DATOS SERVIBOY LTDA 135
FIGURA 88. VENTALLA DEL PROGRAMA DE EDICION DE TEXTO SUBLIME TEXT 136
FIGURA 89. PAGINA DE INICIO DE LA BASE DE DATOS DE SERVIBOY 137
FIGURA 90. GESTOR DE LA BASE DE DATOS DE SERVIBOY 138

LISTA DE TABLAS

TABLA 1. ESTANDARES IEEE 802.11 90
TABLA 2. RELACION DE LAS ANTENAS DE SERVIBOY 96
TABLA 3. UBICACIÓN DE LAS ANTENAS DE SERVIBOY LTDA 100
TABLA 4. DATOS ANTENAS USADAS EN SERVIBOY LTDA 103

GLOSARIO

AGC (AUTOMATIC GAIN CONTROL): El control automático de ganancia que se emplea en las cámaras de seguridad, sirve para ajustar de manera automática, la sensibilidad de la luz que entra al sensor y con ello conseguir una mejor calidad de imagen.

ALARMA: Señal sonora o visual, por medio de la cual se informa sobre la presencia real o inminente de una amenaza.

AMENAZA: Expresión o situación de inseguridad, creada por la inminencia de un accidente o acto malintencionado.

ANTENA: Dispositivo que permite la recepción y el envío de ondas electromagnéticas hacia un espacio libre. Existe una variada cantidad de antenas que estarán determinadas por el uso para el que se empleen. La ubicación física de las antenas incide en su funcionamiento.

AWG (AUTOMATIC WHITE BALANCE): Es el proceso por el cual, la cámara de manera automática, controla el equilibrio de color, partiendo de la fuente de luz en el momento, logrando con ello mejorar la visualización de la imagen.

BALUN (BALANCED- UNBALANCED LINES TRANSFORMER): Es un dispositivo que convierte líneas de transmisión no balanceadas, en líneas balanceadas.

BLC (BACK LIGHT COMPENSATION): Es la función donde la cámara ajusta automáticamente el brillo y contraste de la imagen para que se vean más claros los espacios poco iluminados.

BCN: Es un tipo de conector, de rápida conexión/ desconexión, utilizado para cable coaxial.

CCD (CHARGE- COUPLED DEVICE): Dispositivo de acoplamiento de carga. Es un sensor que capta la luz y de forma digital, la convierte en imágenes. Del tamaño del sensor depende la calidad de la imagen, entre más grande es, mejor.

CCTV (CIRCUITO CERRADO DE TELEVISION): Es un sistema de video vigilancia, como su nombre lo indica: cerrado; utilizado para supervisar actividades en un espacio determinado.

CENTRAL DE MONITOREO: Es la dependencia donde se reciben las señales de alarma efectivamente enviadas, atendidas por operadores de medios tecnológicos.

CMS: Es una aplicación para conectar el DVR desde cualquier equipo, ya sea por medio de internet o una red privada.

CODEC: Abreviatura de codificador-decodificador. Describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos o una señal.

COMPRESION DE IMAGEN- VIDEO: Tecnología que se hace posible, gracias a los códec de audio y video. La finalidad de la compresión de imágenes, es reducir el tamaño y peso de un archivo de video, sin sacrificar la calidad al reproducirse. Un tipo de códec, es aquel que permite comprimir y descomprimir video digital.

CONTACTOS DE EMERGENCIA: Es el listado de funcionarios o personas designadas por el usuario, a quienes la central de monitoreo de alarmas contactara para brindar información acerca de eventos generados por el sistema de alarma monitoreado. Estas personas deben tener la autoridad suficiente para poder coordinar o realizar cualquier verificación interna de las instalaciones ante el requerimiento del personal de la empresa prestadora del servicio. La información de contacto suministrada de estas personas, debe contener números de teléfono de su residencia, números de celular y en general, cualquier número telefónico a través del cual se logre establecer comunicación oportuna y eficaz.

DAÑO: Es la pérdida de vidas humanas, lesiones corporales, perjuicios materiales y/o financieros y deterioro del medio ambiente, como resultado directo o indirecto de un accidente o una acción violenta.

DETECTOR DE MOVIMIENTO: Es uno de los dispositivos que hacen parte del sistema de alarma, se encarga de enviar una señal, en caso de presentarse movimiento en su rango de acción.

DVR (DIGITAL VIDEO RECORDER): Es el dispositivo que se encarga de digitalizar (grabar) las imágenes procedentes de las cámaras conectadas. El DVR clásico es el que va con las cámaras analógicas. Generalmente, también comprime las imágenes.

EVENTO: Se refiere a cualquier actividad que se realice dentro de una unidad donde se preste servicio alarmas, y que envía una señal a la central de monitoreo. Puede ser una operación del normal funcionamiento de la alarma, como: apertura, cierre; o puede ser una acción proveniente, de una posible amenaza, generando un código de alerta.

FALLO DE TEST: Es uno de las clases de evento en seguridad electrónica. Se presenta cuando el sistema no registra conexión con la alarma que está monitoreando.

FIBRA OPTICA: Tecnología diseñada para transmitir señales en forma de pulsos de luz. Los cables de fibra óptica son notables por sus propiedades de aislamiento eléctrico y resistencia a interferencias electrostáticas y electromagnéticas. Transmiten vídeo- señales eficientemente hasta algunos kilómetros. Es costoso y su manipulación es compleja.

FPS (FRAMES PER SECONDS): Hace referencia a la velocidad (tasa) a la cual un dispositivo muestra imágenes: llamadas cuadros o fotogramas. La continua sucesión de estos frames produce la idea de movimiento, lo cual ocurre por las mínimas diferencias de entre ellos. Es el número de cuadros por segundo que se genera, al momento de gravar o reproducir un video.

H.264: Es un estándar de compresión de video también conocido como MPEG-4 Part10, que es utilizado por la industria especialmente para la codificación de video de alta definición HD. Aprovechando la alta velocidad de los procesadores actuales, codificando en H264 es posible distribuir contenido de video con tamaño de fotogramas hasta cuatro veces mayor, reduciendo considerablemente y hasta en una tercera parte, el ancho de banda requerido para reproducirlo.

HIBRIDO- GRABADOR DIGITAL HIBRIDO: Con los adelantos en CCTV, es el dispositivo dado por la evolución del DVR. Es un videograbador, que combina dos tecnologías, en primera medida fue implementado con cámaras análogas y cámaras AHD (análogas de alta definición); con el tiempo, permitieron la conexión de cámaras análogas y cámaras IP. Su implementación aprovecha instalaciones analógicas y se combinan con las bondades de la tecnología IP.

HDMI (HIGH DEFINITION MULTIMEDIA INTERFACE): Es una interfaz digital que permite la transmisión de datos, (Audio, Video e imágenes), por medio de un solo cable.

INFORMACION CONFIDENCIAL: Es aquella que describe la configuración del sistema de alarma y los protocolos de servicio. También hacen parte de esta información: acta de inventario de equipos, el acta de distribución de zonas, el bosquejo de sonorización, la información de los usuarios y contactos.

IR (INFRARROJO): Dependiendo de la cantidad de leds que posee la cámara, es la claridad nocturna. El rango (distancia), depende de ello.

LUX: Para los sistemas CCTV, es la medida mínima de luz que capta la cámara para así generar imágenes de un modo aceptable.

MONITOREO: Información de sistemas electrónicos de seguridad, instalados en el sector residencial o establecimientos financieros, industriales, y que es atendida por una central.

NOISE (RUIDO): Una señal indeseada producida por todos los circuitos eléctricos trabajando sobre el nivel absoluto de cero. El ruido no puede ser eliminado, pero si minimizado.

NTSN (NATIONAL TELEVISION SISTEM COMMITTE): Es un sistema análogo de televisión a color, empleado en casi todo el continente americano, en Japón y en otros países.

NVR (NETWORK VIDEO RECORDER): Videograbador de red. Es un dispositivo similar al DVR. Apareció por la necesidad de mejoras en los CCTV. Al NVR se conectan las cámaras IP. En el sistema IP las imágenes ya llegan procesadas (codificadas) al grabador. Este sistema ofrece en cuanto a calidad mayores resoluciones y menos ruido, que los CCTV análogos tradicionales, aunque es más costoso. El sistema puede estar basado en PC o en sistemas autónomos. Una de las ventajas, es el uso de cable UTP para la instalación de las cámaras o incluso WIFI.

PAL (PHASE- ALTERNATING LINE): Es un sistema de televisión análogo a color, utilizado en la mayoría de los países de Europa, Asia y África.

PANEL DE ALARMA: Parte principal del sistema de alarma, a la que se conectan todos los dispositivos y que contiene toda la electrónica necesaria para el procesamiento de la información del sistema de alarma y la comunicación con el centro de control o central de monitoreo.

PELIGRO: Riesgo o contingencia inminente de que sucede algún mal. Es un hecho o un fenómeno que puede ser causante de daños.

PENTAPLEX: Es la función que le permite al DVR no dejar de gravar o realizar sus demás opciones de trabajo, mientras remotamente el usuario revisa sus equipos de CCTV.

POE (POWER OVER ETHERNET): Esta tecnología permite que los equipos de red, como lo son las cámaras de acceso remoto IP, adicional a los datos, reciban alimentación directamente del cable UTP de Ethernet.

PPP (POINT-TO-POINT PROTOCOL): Protocolo que utiliza una interfaz serie para las comunicaciones entre dos dispositivos de red. Por ejemplo, un PC conectado mediante una línea telefónica a un servidor.

PROTOCOLO DE SEGURIDAD DEL SERVICIO DE VIGILANCIA ELECTRONICA: Implica para la empresa o cooperativa de vigilancia y seguridad privada, implementar los estándares mínimos de calidad que debe cumplir y los aspectos que debe tener en cuenta, para prestar un servicio.

PTZ (PAN- TILT- ZOOM): PAN= Hacer girar/ rotación; TILT= inclinar/ ladeo; ZOOM= captar/ acercar o alejar. Las cámaras PTZ, tienen la ventaja de visualizar su entorno en un rango radial de 360° con acceso remoto. Su rotación es manipulable en 2 ejes: horizontal y vertical, con gran capacidad de visualización cercana y lejana (zoom), poseen la opción de vista panorámica.

RJ11: Es un tipo de conector que se une al cable telefónico y tiene 6 posiciones con cuatro contactos centrales, por los cuatro hilos del cable telefónico.

RJ45: Es una interfaz física comúnmente usada para conectar redes de cableado estructurado.

RS485: Protocolo de comunicación, es una salida digital. En el caso de CCTV, este se utiliza para controlar el envío y recepción de datos de una cámara PTZ.

SATA: Serial ATA. SERIAL ADVANCED TECHNOLOGY ATTACHMENT= tecnología avanzada adjunta serial. Sistema controlador de discos sustituye al P- ATA (conocido simplemente como IDE/ ATA o ATA Paralelo). S-ATA proporciona mayor velocidad, además de mejorar el rendimiento si hay varios discos duros conectados; además de esto, los cables son más delgados que en ATA Paralelo y pueden medir hasta 1 metro, en P- ATA solo pueden medir 40 cm de largo. Es una conexión en serie, en un cable con un mínimo de cuatro alambres que crea una conexión punto a punto entre dos dispositivos. Permite la “conexión en caliente”, es decir, se conectan y desconectan los discos, sin necesidad de apagar el computador.

SISTEMA DE ALARMA: Un elemento de seguridad pasiva, preparado para recibir un estímulo de entrada y proporcionar como respuesta una señal eléctrica de salida que es capaz de advertir la intrusión o allanamiento de una propiedad o inmueble, posibilitando una adecuada intervención para lograr frustrar la comisión de un delito.

TEST PERIODICO: Señal emitida por el panel del sistema de alarma de forma periódica, con el fin de verificar la comunicación entre el sistema de alarma y la central de monitoreo.

TVL (TV LINES): Es la unidad que se utiliza para medir la resolución de las cámaras de seguridad análogas. Mientras más TVL tenga la cámara, mejor será su resolución.

TRIBIDO- GRABADOR DIGITAL TRIBIDO: Es el término que se le otorga a las ventajas que posee un DVR, que cuenta con la conexión de diferentes tipos de cámaras, ya sean IP, AHD o Análogas.

USUARIOS DEL SISTEMA: Es el listado de funcionarios designados por la persona natural o jurídica que contrata el monitoreo, autorizados para operar el panel de alarma, a través de una clave numérica personal e intransferible asignada cuando se entrega el sistema de alarma, al inicio del servicio y posteriormente, cada vez que el cliente o administrador del sistema lo requieren.

VARIFOCAL: Es la función que permite graduar su amplitud dentro de un rango especificado, por ejemplo: 2,8mm y 12mm; esto nos dice que hay un mayor rango de amplitud de zoom.

VGA (VIDEO GRAPHICS ARRAY): Es una norma de visualización de gráficos para ordenadores, en la mayoría de los equipos que requieran visualización. En un monitor, tienen una entrada VGA.

WDR (WIDE DINAMIC RANGE): El amplio rango dinámico se refiere a la manera en que actúa el sensor de la cámara, permitiendo estabilizar las zonas de luz, es decir si la imagen tiene luz directa de fondo, los objetos que están delante de esta, se verán sin claridad, al activarse el WDR, regula y permite observar la imagen sin interferencia.

720p: es el nombre corto para una de las categorías de video. El número representa 720 líneas horizontales de resolución de pantalla y p se refiere a barrido progresivo; lo que quiere decir que para cada fotograma es proyectado por todas las líneas progresivamente, obteniéndose mejor visualización. Sus sucesores son 1080p y 2160p.

RESUMEN

El presente libro tiene como finalidad detallar los fundamentos del trabajo realizado en la empresa SERVICIOS DE VIGILANCIA Y SEGURIDAD DE BOYACA- SERVIBOY LTDA, durante el tiempo de realización de la práctica profesional. Se aprecia una profunda documentación a cerca del entorno y la actividad desarrollada por esta empresa. También se presenta una amplia descripción de componentes, dispositivos, tecnologías e interfaces utilizados durante el desarrollo de la mayoría de las actividades. El lector observara seis capítulos, en los que se expone con claridad cada uno de los temas tratados durante el desarrollo de los diferentes trabajos.

El capítulo 1, comprende la historia y el contexto sobre los elementos que son materia de estudio para la realización de la practica en esta empresa, como son: seguridad en general, la seguridad pública, privada y la seguridad electrónica; como también, sobre las telecomunicaciones.

En el capítulo 2, se describe la historia y el contexto de la empresa SERVIBOY LTDA, y de los servicios que presta en cuanto a seguridad electrónica: equipos, distribución, composición y funcionamiento.

Para el capítulo 3, se aborda todo lo concerniente a los sistemas de vigilancia mediante cámaras, se especifica el funcionamiento de cada componente, que permitieron realizar análisis, mantenimientos e implementación de sistemas de vigilancia de este tipo.

El capítulo 4 corresponde a la red de telecomunicaciones con la que trabaja la empresa. Se hace una descripción los equipos y las tecnologías que intervienen. Se presenta el trabajo realizado con el software RADIO MOBILE, para evaluar la calidad de los enlaces y se presenta el análisis y diseño del mapa de red con el que trabaja la empresa.

El capítulo 5 presenta la descripción de otras labores realizadas durante la pasantía: se aprecian las características y funciones de los sistemas de alarmas y control de acceso, así como las configuraciones realizadas para su implementación. También se relaciona el trabajo realizado, en cuanto a la coordinación y labores administraciones.

En el capítulo 6, se expone el diseño e implementación de la base de datos para el departamento de ingeniería de SERVIBOY.

PROLOGO

El presente documento es el resultado del trabajo realizado en la empresa SERVIBOY en la modalidad de pasantía de un estudiante de Ingeniería Electrónica de la Universidad Santo Tomas Tunja, quien por medio de la investigación en el campo de las comunicaciones y la administración, analizo el estado de la red establecida por la empresa, para dar cumplimiento a la misión de esta, en el campo de la seguridad tanto de la comunidad como de los bienes.

El lector de este escrito, encontrara una extensa documentación sobre los conceptos que se relacionan con la seguridad electrónica, la explicación del trabajo realizado en particular por la empresa SERVIBOY LTDA y el desarrollo de las temáticas y actividades que abordaron esta pasantía.

La aplicación de los conocimientos adquiridos durante los estudios adelantados en la Facultad de Ingeniería Electrónica de la Universidad Santo Tomas de Tunja; dieron los resultados esperados al ser aplicados, durante el desarrollo de la modalidad de trabajo de grado, denominada pasantía cumplida, por la autora Sandra Liliana Pardo Ruiz, quien incrementándolos con su estudio de los equipos instalados y su estadía en la Central de Comunicaciones o "Command Center" de SERVIBOY, logro culminar con éxito el objetivo propuesto: adicionando a las labores de modelamiento de la red de comunicaciones, la generación de documentación para el seguimiento de la operación y mantenimiento de los diversos equipos tales como: antenas, elementos de trasmisión, recepción y enrutamiento de señales de video y audio , cámaras de video y sistemas de monitoreo instalados en los puntos de servicio en la ciudad de Tunja; calibración de equipos y aplicaciones electrónicas; así como la divulgación de la actividad realizada, mediante academias con los colaboradores de la empresa, impulsando la capacitación y mejoramiento de la calidad del servicio.

INTRODUCCION

Desde su aparición sobre la Tierra, diversos peligros han seguido al hombre, en gran parte, atribuibles, a las fuerzas de la Naturaleza. La inseguridad y la incertidumbre, han llevado a la búsqueda de protección ante esos fenómenos. Además, en la lucha por la supervivencia, el ser humano se ha enfrentado con el mundo vegetal y animal de su entorno; y también, con sus propios congéneres. A lo largo de los siglos, guerras, grandes epidemias, fanatismos religiosos, políticos y sociales, incendios, naufragios y los riesgos propios de la Naturaleza, han acompañado al ser humano en todas las latitudes. Dentro de la evolución histórica, el ser humano ha ido desarrollando medidas de protección proporcionales a esos riesgos.

La evolución de la sociedad en el siglo XIX, produjo un nuevo universo de riesgos. Lentamente y sin una conciencia clara de la precisión de seguridad, evoluciona de manera paralela, la necesidad de protección frente a los nuevos riesgos; se hacen cosas para evitar los efectos de los riesgos, pero no se considera un plan de Seguridad. La evolución de la tecnología, en el pasado siglo, tiene en el desarrollo prodigioso de la Información a uno de sus más altos exponentes. El volumen de datos que procesan hoy las empresas, las instituciones y las personas, hubiera sido impensable hace tan sólo unas décadas. Cualquiera de los ordenadores creados hace diez años resulta menos poderoso frente a un equipo personal fabricado el mes pasado. Creció también rápidamente, el número de satélites y de centrales digitales, que procesan las comunicaciones telefónicas. Se expandió el empleo de mensáfonos, teléfonos portátiles, fax, fotocopiadoras, contestadores... todos esos instrumentos que en la época actual se consideran elementales, en 1970, no eran tan cotidianos. En definitiva, la trascendencia y la necesidad de la Información en la sociedad moderna la convierten en uno de los bienes más importantes, tanto para el mundo empresarial como para las áreas política, social, económica, cultural e, incluso, personal. El siglo XXI abre una era post-industrial que está caracterizada por el predominio de la Información y la Comunicación y por el desarrollo imparable de los avances tecnológicos de los procesos productivos.

Se produce, consecuentemente, un amplio incremento de los riesgos, al sumarse las amenazas inherentes al desarrollo de la tecnología, las derivadas de la información y las comunicaciones y el incremento cuantitativo y cualitativo de la delincuencia, resultante de los profundos desequilibrios sociales. Este universo actual de riesgos requiere unos principios de acción diferentes a los tradicionales. Así como se presentan nuevos riesgos, aparecen nuevas formas de enfrentar los riesgos; el uso de dispositivos electrónicos para la protección de personas, establecimientos o residencias, se hace cada vez más popular y esto, se traduce en la aplicación de un nuevo concepto de seguridad: la Seguridad Integral.

JUSTIFICACION

Con el presente proyecto, se busca dotar a la empresa SERVICIOS DE VIGILANCIA Y SEGURIDAD DE BOYACA, con herramientas desde la ingeniería electrónica, para solucionar problemáticas y contribuir a que la empresa cumpla con su labor, de manera exitosa.

En este momento, la empresa SERVIBOY LTDA cuenta con diferentes servicios tanto de seguridad humana como de seguridad electrónica. El departamento de ingeniería se encarga de los servicios de seguridad electrónica, que son: Circuito cerrado de televisión, Sistemas de alarmas, Control de acceso, Video-vigilancia, Seguimiento personal y vehicular GPS. En cuanto al tema de instalaciones de los diferentes sistemas según sea el requerimiento, la empresa ha logrado cumplir con lo propuesto. Sin embargo, el hecho de que falten documentos generados por personal de ingeniería, ha empezado a traer complicaciones al normal funcionamiento del trabajo, y a la posibilidad de ampliar su área de operación.

La proyección de una empresa (independiente de cual de su actividad principal), depende de que tan preparada se encuentra la compañía para generar cambios. El desarrollo del trabajo en la empresa SERVIBOY LTDA es importante, ya que esta se encuentra en pleno crecimiento y tiene trazada una alta expectativa. Actualmente, es la empresa líder en seguridad y Tunja y sus alrededores, la idea es poder continuar así, consolidándose a nivel departamental y nacional.

Con la implementación del mapeo de la red de telecomunicaciones de la empresa, se busca no solo tener el documento, sino entrar a revisar la manera en la que se vienen implementando las nuevas unidades, para determinar la eficiencia con la que se está trabajando; que tendrá un impacto económico en la empresa ya que la idea es aprovechar al máximo la capacidad de los equipos sin sacrificar calidad; así como asegurar que en adelante se va a implementar un estudio detallado de la manera en la que se establece la conectividad desde las unidades monitoreadas, hasta la central. Por otro lado, al ejercer la coordinación del departamento de ingeniería, se busca obtener un impacto positivo económico y medioambiental, pues diseñar y planear bien desde el principio permite una inversión correcta y evita el tener exceso de equipos obsoletos; además de implementar un diagrama de los procesos de ingeniería que se llevan a cabo, hacer un seguimiento formal, garantizando la transparencia de dichos procesos, para contribuir con la mejora cualitativa y cuantitativa, en la prestación del servicio.

PLANTEAMIENTO DEL PROBLEMA

FALTA DE DOCUMENTACION EN EL DEPARTAMENTO DE INGENIERIA DE LA EMPRESA, LO QUE DIFICULTA UNA OPERACION EFICAZ, ESPECIFICAMENTE EN LA SEGURIDAD ELECTRONICA.

FORMULACION DE PREGUNTAS:

- ¿Exactamente que equipos se tienen instalados y dónde?
- ¿con que tipo de red se trabaja en la empresa y con qué criterios de diseño se cuenta, para el momento en el que ingresa una nueva unidad para ser monitoreada?
- ¿se realiza un itinerario para realizar los mantenimientos, teniendo en cuenta: lugares a visitar, distancia, disponibilidad del cliente y así hacer un recorrido de visitas técnicas en unidades cercanas que garantice un desplazamiento oportuno?
- ¿se cuenta con un listado donde se relacionen los usuarios y el tipo de equipos que se tienen, para que luego se pueda encontrar y utilizar fácilmente la información?

DEFINICION DEL PROBLEMA:

El Departamento de ingeniería de la empresa SERVIBOY LTDA, es relativamente nuevo. El crecimiento que la empresa ha tenido con la implementación de la vigilancia electrónica, ha sido bastante y se ha dado rápidamente. La infraestructura que hizo posible implementar la seguridad electrónica, fue realizada por un ingeniero electrónico, su trabajo consistió en el diseño general.

Por temas administrativos y de sociedad, las cosas del departamento de ingeniería, quedaron en manos de personal que no estaba involucrado con la seguridad electrónica; razón por la cual, las cosas empezaron a implementarse y aunque se logró que funcionara, no se llevaba un orden ni se tenía la documentación suficiente para hacer el tratamiento a la información. Esto, tanto en los datos de equipos como en los datos de los clientes.

DELIMITACION DEL PROBLEMA:

El problema que en este momento presenta la empresa SERVIBOY LTDA, tiene que ver con la forma en la que se maneja la información, en cuanto a vigilancia electrónica se refiere. Mi trabajo como ingeniera electrónica, está enfocado en el tratamiento de las dificultades que se vienen presentando alrededor del problema general trazado y en cuanto a las preguntas formuladas. Planteado esto, se tienen dos planes de acción: recopilación de información para realizar el modelamiento de la red de telecomunicaciones de la empresa y para llevar un manejo adecuado de la información; y paralelamente, llevar a cabo labores de liderazgo con el personal técnico en cuanto al mantenimiento de equipos.

OBJETIVOS

OBJETIVO GENERAL

- Describir la red de telecomunicaciones usada en el servicio de video- vigilancia de la empresa SERVIBOY LTDA.

OBJETIVOS ESPECIFICOS

- Precisar a través de una amplia investigación, los servicios que presta la seguridad electrónica, los dispositivos existentes para la prestación de dichos servicios, sus especificaciones y cómo funcionan.

- Establecer soluciones en el departamento de ingeniería de SERVIBOY, para el soporte, mantenimiento y configuración de equipos.

- Determinar los lugares en donde SERVIBOY LTDA presta el servicio de video- vigilancia, realizando inventario de los equipos y tabulando los datos recopilados.

CAPITULO 1

1. MARCO REFERENCIAL

1.1. ¿QUE ES SEGURIDAD?

Definición de seguridad, según la Real Academia Española:

Del latín securĭtas, -ātis.

1. femenino. Cualidad de seguro. 2. femenino. Servicio encargado de la seguridad de una persona, de una empresa, de un edificio, etc. Llama a seguridad. 3. femenino. desusado. Fianza u obligación de indemnidad a favor de alguien.

FIGURA 1. SEGURIDAD: CAJA FUERTE

FUENTE: https://www.mindomo.com/mindmap/instituciones-de-apoyo-de-los-mercados-de-valores-bc7613555b954b978399fdf8300b25a5

El término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto, hace foco en la característica de seguro, es decir, realza la propiedad de algo donde no se registran peligro, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza.

Existen muchos tipos de seguridad, tantos, como actividades pueda realizar el ser humano. Ejemplo: seguridad social, seguridad laboral, seguridad pública, seguridad privada, seguridad jurídica, seguridad ciudadana, seguridad alimentaria. También es aplicable esta palabra, para crear conceptos de mecanismos: cerradura de seguridad, anillo de seguridad, mecha de seguridad, medida de seguridad, cinturón de seguridad, distancia de seguridad, guardia de seguridad, lámpara de seguridad, válvula de seguridad. [1]

[1] http://definicion.de/seguridad/#ixzz40XEHd94V

1.1.1. SEGURIDAD PÚBLICA

La seguridad pública implica que los ciudadanos de una misma región puedan convivir en armonía, cada uno respetando los derechos individuales del otro. El Estado es el garante de la seguridad pública y el máximo responsable a la hora de evitar las alteraciones del orden social.

FIGURA 2. SEGURIDAD PÚBLICA

FUENTES: http://cgfm.mil.co/ http://oasportal.policia.gov.co/

En este sentido, la seguridad pública es un servicio que debe ser universal (tiene que alcanzar a todas las personas) para proteger la integridad física de los ciudadanos y sus bienes. Para esto, existen las fuerzas de seguridad (como la policía), que trabajan en conjunto con el Poder Judicial.

Las fuerzas de la seguridad pública deben prevenir la comisión de delitos y reprimir éstos, una vez que están curso. También es función de las fuerzas de seguridad perseguir a los delincuentes y entregarlos a la Justicia, que será la encargada de establecer los castigos correspondientes de acuerdo a la ley.

Así las cosas, hay que destacar entidades u organismos de todo el mundo que se encargan de llevar a cabo las acciones pertinentes para lograr que los ciudadanos de una zona o país en concreto estén a salvo de actos delictivos y vivan en armonía.

FIGURA 3. FUERZA PÚBLICA COLOMBIA: NAVAL, EJERCITO Y FUERZA AEREA

FUENTE: http://cgfm.mil.co/conozcanos

Por lo general, las grandes ciudades sufren problemas de seguridad pública, al presentar altas tasas de delitos. En cambio, los pequeños pueblos suelen ofrecer mejores condiciones de seguridad.

Esto, en cierta forma, está vinculado a la masividad, ya que los millones de habitantes de una urbe se vuelven anónimos. En los pueblos, es menos probable que una persona pueda delinquir sin que nadie se entere.

La seguridad pública también depende de la eficacia de la policía, del funcionamiento del Poder Judicial, de las políticas estatales y de las condiciones sociales. El debate respecto a la incidencia de la pobreza en la inseguridad siempre es polémico, aunque la mayoría de los especialistas establece una relación entre la tasa de pobreza y la cantidad de delitos.[2]

1.1.2. SEGURIDAD PRIVADA

Con origen en el término latino securĭtas, el concepto de seguridad hace referencia a aquello que tiene la cualidad de seguro o que está exento de peligro, perjuicio o riesgo.

Por su parte, la palabra privada, que se establece como la segunda mitad del término que se analiza, tiene su origen etimológico en el latín. Más concretamente, procede del vocablo privatus, que a su vez emana del verbo privare que puede traducirse como sinónimo de “privar”.

FIGURA 4. SEGURIDAD PRIVADA

FUENTE: http://definicion.de/seguridad-publica/

La seguridad privada es un servicio adicional, al de la seguridad pública. Es el conjunto de bienes y servicios brindados por entes privados, para proteger a sus clientes y a sus bienes y patrimonio, de delitos, daños e inseguridades, a auxiliarlos en caso de delitos, siniestros o desastres, y a colaborar en la investigación de delitos que los involucren. Los clientes pueden ser personas naturales o jurídicas, públicas o privadas. El préstamo de estos servicios se puede ofrecer a una o

[2] http://definicion.de/seguridad-publica/#ixzz40XTHPETy

varias personas, instalaciones y eventos (en los que se ofrece protección tanto a las personas que asisten como a los bienes).

La seguridad privada tiene sus limitaciones en términos legales y no tiene los mismos poderes que la autoridad dependiente del estado como la policía o el ejército; habitualmente trabaja en forma auxiliar y complementaria a la seguridad pública, y requiere previa autorización, licencia o permiso expedido por las autoridades competentes.[3]

1.1.3. INDUSTRIA DE LA SEGURIDAD PRIVADA

Se denomina INDUSTRIA DE LA SEGURIDAD PRIVADA al conjunto de efectores individuales y organizacionales que brindan servicios de seguridad, vigilancia, protección, investigaciones, transporte de fondos, electrónica y múltiples otros conexos a particulares, empresas, instituciones, reparticiones gubernamentales y otros demandantes. La industria de la Seguridad Privada ha ganado un lugar de relevancia tanto económica, por su dimensión y tasa de crecimiento, como por haberse convertido en uno de los principales creadores de empleo formal, y por su aporte sustancial en la mejora de la situación general de Seguridad de la Comunidad.[4]

1.1.4. PERSONAL DE VIGILANCIA PRIVADA

El Personal de Seguridad desarrolla sus funciones en un amplio abanico de trabajos, que van desde la vigilancia y protección de bienes, establecimientos, personas y valores monetarios hasta el control de centrales de alarmas. En todos ellos existen situaciones de riesgos, basadas en circunstancias tan variadas como pueden ser el terrorismo y la delincuencia, por un lado, o los accidentes laborales y profesionales, por otra parte. Por esto, el personal de seguridad esté sujeto a riesgos, tanto en su trabajo como fuera de él, y es preciso que esté preparado para identificarlos y superarlos; es necesaria la AUTOPROTECCIÓN.

AUTOPROTECCIÓN: Concepto entendido como "el conjunto de medidas, normas, medios y actuaciones personales que tienen por objeto garantizar la función, el trabajo y la integridad física de la persona a proteger". Dentro del objeto de protección se incluye, como no puede ser de otra forma, el personal de seguridad, el propio Vigilante de Seguridad.

1.1.4.1. ANÁLISIS DE RIESGOS

Un plan de autoprotección analiza los riegos inherentes a la actividad del Vigilante de Seguridad:

a) RIESGOS PROFESIONALES: derivados de su cometido laboral, como pueden ser:

- Identificación de personas.
- Persecución de delincuentes.
- Custodia de detenidos, hasta la puesta a disposición de las Fuerzas y Cuerpos de Seguridad.

[3] http://www.significados.com/seguridad/

[4] http://www.forodeseguridad.com/artic/discipl/4163.htm

- Control de accesos.
- Actuaciones en recintos con eventos deportivos o elevadas concentraciones de personal.
- Manipulación de los instrumentos de trabajo.
- Auxilio a víctimas.
- Conducción de vehículos.

b) RIESGOS AJENOS A LA ACTIVIDAD LABORAL: Fuera del ejercicio de su actividad laboral, el personal de Seguridad Privada ha de contemplar otros riesgos, como:

- En el domicilio
  - Entrada y/o salida.
  - Apertura de la puerta, Accesos al garaje.
  - Recepción y apertura de correspondencia y paquetería.
  - Uso de ascensores.
  - Coincidencia con desconocidos.
- En los desplazamientos
  - A pie.
  - En vehículo particular, En transporte público.
  - La detención en determinados puntos.
- En lugares de ocio
  - Práctica de deportes.
  - Establecimientos públicos.

c) RIESGOS DERIVADOS DE ACTIVIDADES ANTISOCIALES:

- Atentado. - Extorsión. - Atraco. - Robo.

1.1.4.2. MEDIDAS DE SEGURIDAD

No hay que confundir autoprotección con obsesión por la protección. Sin embargo, al estar relacionada su actividad con la protección de valores – sean del tipo que sean –, el vigilante de seguridad ha de extremar la prudencia, tanto en el desarrollo de su actividad como en su vida privada. Las consecuencias que puedan derivarse de una charla en un bar no son las mismas si el contenido de las conversaciones se refiere a los problemas laborales de dos administrativos que a lo que alberga la nave custodiada por dos vigilantes. Parece evidente que el sentido común impone discreción, a la hora de hablar de la actividad profesional del personal de Seguridad Privada.

Ante situaciones de riesgo, hay una serie de medidas de seguridad para poder prevenirlas:

MEDIDAS ACTIVAS: Son las propias habilidades desarrolladas por la persona:

- Observación, Percepción.
- Información
- Prudencia, Prevención
- Decisión
- Variación de hábitos, huida de la rutina
- Meticulosidad

- Confianza y Desconfianza medida

MEDIDAS PASIVAS: Son los medios de defensa personal:

- Chaleco antibalas
- Silbato
- Spray
- Armas
- Medidas de seguridad física: Blindajes, Alarmas, Circuito cerrado TV.

1.1.5. CONTRASTE: SEGURIDAD PÚBLICA Y SEGURIDAD PRIVADA

Las fuerzas de seguridad del Estado se encargan de prevenir la comisión de delitos y de perseguir a los delincuentes, con la misión de entregarlos al Poder Judicial. Este organismo tiene la misión de aplicar los castigos que estipula la ley, que pueden ir desde una multa económica hasta la pena de muerte, según el país y la gravedad del delito. Sin embargo, la ineficacia de la seguridad estatal y su falta de alcance en ciertos casos ha generado el negocio de la seguridad privada, donde distintas empresas se encargan de ofrecer custodios, vigilantes y distintos dispositivos para cualquier ciudadano que pueda pagarlos.

Por cuestiones de número, no hay suficientes policías para cuidar a cada persona o empresa. Por eso, aquellos que se sienten en riesgo, acuden a la contratación de un custodio permanente o la implementación de algún sistema que les brinde protección. Así, en la actualidad nos encontramos con el hecho de que multitud de negocios suelen apostar por la contratación de profesionales del sector de la seguridad privada para garantizar el desarrollo de su labor sin que haya ningún tipo de problemas y para evitar lo que son distintos actos delictivos en sus instalaciones.

Entre el conjunto de empresas que optan por la seguridad privada nos encontramos con grandes almacenes, tiendas de ropa que de esta manera intentan paliar que delincuentes consigan robar prendas, e incluso joyerías. Y es que estas últimas están en el punto de mira de muchos de esos delincuentes que urden sus planes para robar mercancías de gran valor en aquellas, por lo que se hace necesario contratar a servicios privados que puedan evitar hurtos de todo tipo.

Y todo ello sin olvidar tampoco que en el ámbito de la vida privada también se ha producido un incremento del número de personas que también deciden contar con profesionales de la seguridad privada para vivir más tranquilamente en sus hogares sin correr el peligro de que estos sean asaltados. Así, tanto a nivel particular como en urbanizaciones de cierto poder adquisitivo ya se encuentran miembros de la seguridad privada velando por el bienestar de quienes les han contratado.

Dependiendo del país, los vigilantes privados pueden portar o no armas de fuego y contar con diferentes atribuciones que les delega el Estado. Por lo general, el control del espacio público sigue estando exclusivamente limitado a las fuerzas de seguridad estatales.[5]

[5] http://definicion.de/seguridad-privada/#ixzz40XCa7l5y

1.2. LOS RIESGOS

Es la incertidumbre ante la posibilidad de que ocurra un hecho, con resultado contrario al esperado. Hay que precisar que la palabra RIESGO, aceptada como causa potencial de daño, tiene una segunda aplicación, como medida en la Evaluación de Riesgos: La probabilidad de ocurrencia de accidente. De la misma forma, daño es empleado en metodologías de Análisis de Riesgos como parámetro de la medida del mal sufrido en el accidente.

El ser humano, influido por las circunstancias de cada situación, percibe los riesgos de una forma subjetiva. Esa percepción, aunque no está basada en ninguna metodología científica, tiene validez social, influyendo en la consideración y decisiones que adoptan los responsables políticos y empresariales. Como ejemplos de la valoración subjetiva están los riesgos nucleares, químicos, medio ambientales, epidemiológicos, de inseguridad ciudadana y, también, de conservación del empleo. Esa percepción subjetiva se deriva de la influencia de los factores de conocimiento (riesgo conocido o desconocido, con poca o ninguna información), severidad (catastróficos e incontrolables, o leves y fácilmente controlables), número de personas afectadas y voluntariedad respecto a la exposición al riesgo (riesgo impuesto o buscado). El adecuado tratamiento de los riesgos, ha de ser dado desde un conocimiento objetivo; por tanto, con fundamentos científico-técnicos, que estén a disposición de quienes han de tomar decisiones.

Los acelerados cambios de los últimos años (en los ámbitos social, político, económico, comercial y tecnológico) y su continua evolución, han incrementado la habitual incertidumbre que caracteriza a la actividad de las empresas, grupos e instituciones, tanto en sus riesgos de gestión como en los riesgos accidentales. El progreso del ser humano ha ido desarrollando nuevos sistemas, que proporcionan notables beneficios pero que, simultáneamente, conllevan nuevos riesgos. El ser humano ha de convivir con los riesgos aparejados a los avances sociales, pero procurando un desarrollo compatible con su propia supervivencia y la de su medio de vida. Una de las características que ha llevado a este retraso en el conocimiento –o, incluso, desconocimiento– de ciertos riesgos ha sido la evolución desde unas estructuras sociales limitadas (locales, individualizadas) a una estructura social común compleja y con interdependencias entre sus componentes, que son difíciles de conocer y de controlar (la 'aldea global'). El reto que se plantea es el de adelantarse a situaciones futuras, identificando y evaluando nuevos riesgos, que se añaden a los tradicionales, que pueden a su vez, evolucionar también. Teniendo ese conocimiento, se estará en mejor situación para poder adoptar las medidas de seguridad que controlen los riesgos y minimicen las pérdidas, en el caso de que lleguen a materializarse en accidentes.

Como ejemplos de aspectos que repercuten en la generación y agravamiento de los nuevos riesgos, sin olvidar que también propician importantes beneficios, están:

- Los grandes avances tecnológicos.
- La internacionalización del comercio ('mercado global').
- La vulneración de los mercados financieros. Las tendencias socio-políticas extremas.
- El deterioro medio ambiental, - Los cambios climáticos.
- El descompensado crecimiento demográfico y los movimientos migratorios.

- Las comunicaciones, cada vez más rápidas.

Una consideración inicial de los riesgos en la empresa lleva a diferenciar dos tipos:

RIESGOS ESPECULATIVOS. Su materialización puede dar lugar a ganancias o a pérdidas. Son riesgos del negocio empresarial y dependen del acierto de, por ejemplo: las inversiones realizadas, el lanzamiento de productos, la selección de personal, etc.

RIESGOS PUROS. Su materialización sólo dará lugar a pérdidas. No tienen que materializarse, necesariamente, en un accidente o siniestro, pudiendo mantener, de forma indefinida, el carácter de riesgo 'potencial'.

1.2.1. ESCENARIO DE LOS RIESGOS

El desarrollo de cualquier actividad, con la incertidumbre de que se alcance el resultado según estaba previsto (seguridad) o en forma contraria (riesgo) es analizado como un sistema que tiene lugar en un medio determinado (escenario), en el que participan una serie de agentes que conducen a un resultado final.

1.2.2. AGENTES O ACTORES DE LOS RIESGOS

Los agentes protagonistas de los riesgos y de la seguridad son aquellos componentes del sistema, sobre los que se puede reflejar el daño de un accidente. Estos intervienen en un escenario determinado. Se agrupan en:

· Personal propio, vinculado a la empresa y catalogado en función de la influencia que tiene en la actividad empresarial: Personal clave: ejecutivos, investigadores, puestos críticos... Personal en general, catalogado por funciones, condiciones de trabajo, edad.

· Activos y materiales propios. Bienes inventariados: terrenos, edificios, maquinarias, instalaciones, equipos, mercancías, productos...

· Activos inmateriales propios. Elementos sin apreciación física: finanzas, inversiones, beneficios, tecnología, conocimiento, información, patentes, imagen, prestigio, reputación, interrupción de la actividad...

· Sujetos terceros: personas (consumidores y clientes, vecinos de las instalaciones...).

1.2.3. TIPOS DE RIESGOS

~ RIESGOS DE LA NATURALEZA: Probabilidad de ocurrencia de fenómenos de la Naturaleza cuyo acaecimiento puede suponer una amenaza para la vida humana o una pérdida económica. En esta clasificación están: Terremoto o sismo, Rayo, Huracán, Tifón, inundación, nevada, helada, granizo, avalancha, entre otros.

~ DEL SER HUMANO: Entre estos se tienen los involuntarios, accidentales y sin intervención de ningún elemento técnico: caídas, golpes, lesiones musculares, enfermedades naturales... También están los actos criminales: robos, atracos, secuestros, fraudes, espionaje, atentados... Por último, se tienen las actividades sociales y políticas: manifestaciones, campañas de protesta, guerras, motines, huelgas, expropiaciones...

~ RIESGOS TECNOLOGICOS: Derivados de las aplicaciones y elementos desarrollados por la técnica, pueden ser químicos, físicos, nucleares o técnicos. Con la intervención de elementos técnicos en el origen del accidente, aunque participen factores humanos: - Físicos: mecánicos (atrapamientos, cortes, colisiones...), eléctricos (descargas eléctricas, cortocircuitos...), acústicos (ruido), termodinámicos (explosiones, fusiones...), radiaciones no ionizantes... - Químicos: combustiones (incendios, explosiones químicas...), corrosiones, toxicidad (escapes, ingestión, inhalación...), nucleares...

~ RIESGOS DERIVADOS DE LAS ACTIVIDADES SOCIALES: Por su trascendencia, destacan en este apartado las alteraciones en el ambiente, consecuencia de un desarrollo incontrolado de diversas actividades que producen la liberación de productos contaminantes.

· Vertido de líquidos contaminantes en aguas: pudiendo derivar la contaminación de agua potable.

· Filtración de productos contaminantes en suelos: dejándolos inservibles para su explotación agrícola, ganadera y de consumo.

· Emisión de contaminantes en el aire: produciendo graves perturbaciones en los ecosistemas receptores, con posible posterior incorporación a la cadena trófica (nutritiva).

~ RIESGOS DERIVADOS DE LAS ACTIVIDADES ANTISOCIALES: El cuarto grupo de amenazas, se caracteriza por el origen humano de las actuaciones y la voluntad expresa de realizar daño. El fin perseguido con tales acciones es diferente y, con frecuencia, muy complejo. El ánimo de lucro representa el objetivo normal de atracos, robos, hurtos y estafas; también está presente en actuaciones de secuestro y espionaje industrial. Algunos actos tendrán objetivos de carácter político-social, acordes con su ideología, pero perseguirán, con cierta frecuencia, fines inmediatos de lucro, venganza o notoriedad. La intrusión está vinculada a una actuación posterior, en tanto que el acto vandálico se caracteriza por su irracionalidad, mientras que los disturbios y agresiones tienen un amplio abanico de motivaciones y finalidades.

· La trascendencia de las amenazas de carácter antisocial, viene representadas por diversos factores. Las sociedades modernas afrontan el incremento de las amenazas antisociales con un redoblado esfuerzo mediante la implantación de sistemas de seguridad que integren medios de protección técnicos y humanos, con medidas, normas y procedimientos que permitan la coordinación del conjunto de Seguridad.

1.2.3.1. TIPOLOGÍA DE LOS RIESGOS DE CARÁCTER ANTISOCIAL

a) INTRUSIÓN: Consiste en la entrada, sin derecho, en un espacio ajeno, con simulación o sigilo. Esta definición contempla las dos formas habituales en las que se puede producir la intrusión: - Entrada, mediante simulación o engaño, por los accesos naturales del edificio o la residencia. - Infiltración, con sigilo, a través de las fachadas, cubiertas, sótanos o patios interiores del inmueble. La intrusión, por sí sola, carece de sentido y siempre se vincula a actuaciones posteriores, constitutivas de la verdadera amenaza. La intrusión puede ser llave de amenazas de robo, hurto, sabotaje, amenaza de bomba, daños a la información, agresiones, atentado y/o secuestro. Su solución eficaz permite abordar todas las amenazas citadas, derivadas de ella.

b) ROBO: Se entiende por robo la apropiación de una cosa mueble ajena, contra la voluntad de su dueño, con ánimo de lucro y empleando fuerza. Este empleo de fuerza puede ser:

- Con medios no violentos, que no producen daño en el lugar del robo, como el escalamiento (entrada por vía no prevista al efecto) y el uso de llaves falsas.

- Con medios violentos, mediante fractura exterior o interior. Butrón o fractura de puertas y ventanas, en el primero; rotura de armarios, vitrinas, etc., en el segundo.

c) HURTO: Se define el hurto como la apropiación de una cosa mueble ajena, contra la voluntad de su dueño, con ánimo de lucro y sin intimidación o violencia en las personas. Su incidencia es considerablemente menor que la del robo, en razón de la escasa repercusión de estos hechos, de una parte, y de la limitada cuantía de los botines, por otra. Son elementos que propician el hurto: el descuido, la rutina, las aglomeraciones y las situaciones confusas.

d) SABOTAJE: Conceptualmente, es la realización de daños o deterioro en la maquinaria, productos, etc., como procedimiento de lucha contra el Estado y sus instituciones, o contra empresas, en conflictos sociales y políticos. Puede tener su origen en empleados descontentos, adversarios políticos o sociales, etc., y ser ejecutado por medios manuales o mecánicos. El acto sabotaje se vincula, normalmente, a las organizaciones terroristas, con el empleo de medios de destrucción.

e) AVISO DE BOMBA: Consiste en una actuación informativa de colocación de artefacto, cuya veracidad o falsedad crea incertidumbre, siendo frecuentemente su único objetivo. Constituye normalmente falsas alarmas que producen trastornos en la vida y trabajo de cualquier empresa.

f) ATAQUES A LA INFORMACIÓN: La información constituye un bien legítimo de la empresa, cuya destrucción, manipulación fraudulenta o conocimiento por terceros, puede acarrearle graves daños. Al solo efecto de su protección, la información se clasifica en:

- Documentaciones. Información sobre soporte papel, fotográfico y similares.

- Soporte magnético. Información contenida en el proceso lógico o informático.

- Comunicaciones. Información que se transmite a través de la conversación directa, ondas de radio y líneas físicas de transmisión.

- Actividades constitutivas de información, tales como reuniones de alta dirección, relaciones con otras empresas, preparación de campañas y otras.

g) DISTURBIOS. AGRESIONES. VANDALISMO: La posibilidad de que se produzcan disturbios externos, que puedan ocasionar daños a personas y bienes, constituye una amenaza potencial para una entidad. Al igual que en el caso de actos vandálicos injustificados, los disturbios internos, por los daños que, pueden producir sobre el mobiliario, materiales o estructuras del propio edificio, pueden también traducirse en agresiones sobre personas.

h) ATENTADO: Se define como la agresión al Estado o a una persona constituida en autoridad y con carácter general, la agresión contra la integridad física o moral de una persona. El atentado constituye la forma de amenaza más violenta, siendo su objetivo el de la muerte de una o varias personas concretas, cuya selección está directamente relacionada con las personas constitutivas de objetivos. En la realidad, se suele producir un incremento de víctimas inocentes, ajenas a esa selección, como consecuencia de errores o precipitaciones del agresor.

En cuanto a los procedimientos de actuación empleados en un atentado, pueden ser los siguientes:

- Empleo de armas convencionales, de tiro tenso y proyectil macizo (pistola, metralleta, fusil, rifle, carabina, etc.), con la posibilidad de utilización de alza telescópica y equipo de visión nocturna.

- Lanzamiento de proyectiles explosivos, sobre el objetivo, desde una posición exterior al mismo.

- Colocación de artefactos explosivos. Pueden tener el aspecto exterior que la imaginación del agresor quiera darles y los lugares de colocación pueden ser, también, muy variados:

· En el interior de un edificio (aseos, áreas de acceso al público, despachos, etc.).

· En el subsuelo de los edificios (estacionamiento de vehículos y galerías subterráneas).

· En los vehículos; ocultos en su interior o adosados a la parte inferior.

· En aeronaves, trenes o barcos; ocultando del artefacto en equipajes, cargas, etc.

· En las vías de comunicación (carreteras, ferrocarriles), con preferencia por los puentes y túneles.

· Aviso de bomba y envío de carta o paquete-bomba: A través de Correos o mediante mensajeros.

- Coche-bomba: Es el procedimiento más frecuentemente empleado por el terrorismo.

1.3. ELEMENTOS BÁSICOS DE LA SEGURIDAD

El planteamiento de cualquier problema de seguridad responde, por definición, a la existencia de una o varias amenazas que pueden producir daños a personas o a bienes. Sin la presencia de esos riesgos, o causas potenciales de daño, la Seguridad carecería de sentido y, de la misma forma, sin la existencia de un objeto susceptible de recibir un daño, la seguridad constituiría una irrealidad. Siempre habrá dos elementos básicos: las amenazas y los objetos amenazados; estos dos elementos son los factores primordiales. La existencia de esos dos factores procede de la propia

naturaleza del concepto de seguridad y del estudio de su entorno, que proporcionará un tercer factor. Finalmente, se implica un cuarto factor: la protección, que se traduce en la aplicación de unos medios. En definitiva, los factores, o elementos, básicos de la seguridad, son:

- ✓ El Objeto a proteger (Qué protegemos)
- ✓ Las Amenazas, o Riesgos (De qué, o de quién, lo protegemos)
- ✓ Los elementos dimensionales: Espacio y Tiempo (Dónde y cuándo lo protegemos)
- ✓ Los Medios de Protección (Cómo, con qué, lo protegemos)

1.3.1. EL OBJETO DE PROTECCIÓN:

El primero de los elementos responde, a una cuestión básica: Qué vamos a proteger. Es, en síntesis, la finalidad perseguida y fundamental del trabajo de la seguridad. El objeto a proteger son personas y bienes. Será preciso realizar un completo análisis de cada uno de ellos, siempre en relación directa con los riesgos que le afecten. Bajo el concepto 'personas a proteger' cabe desde un individuo aislado, de cualquier nacionalidad, raza o nivel, hasta un colectivo nacional o continental. La protección del presidente de una gran empresa, o de un alto cargo de la Administración, revestirá unas características especiales, en razón de los riesgos peculiares que comporta, y dará lugar específicamente a la 'Seguridad Personal'. La protección de las personas ubicadas en un gran estadio deportivo reviste, a su vez, riesgos específicos. De la misma forma, cabe realizar el tratamiento de la protección de diferentes colectivos: población de un penal, personas ubicadas en un hotel, habitantes de una ciudad, población de un hospital, personas trasladadas por tierra, mar o aire, empleados y clientes de una oficina bancaria, población de un aeropuerto, población de una instalación portuaria, empleados y clientes de un hipermercado... De acuerdo con los riesgos propios de cada uno de esos colectivos se producirán formas de seguridad penitenciaria, hotelera, de medio urbano, hospitalaria, de los trasportes, bancaria, portuaria, etc...

En cuanto al tratamiento de la seguridad de los bienes, se puede establecer la protección de: dinero y documentos de valor, obras de arte, instalaciones industriales, áreas forestales, centros de proceso de datos, comunicaciones, documentaciones... Así, en consecuencia, con los diferentes riesgos que conllevan esos bienes, se producirá el tratamiento de seguridad bancaria, seguridad del patrimonio artístico y cultural, seguridad industrial, forestal, informática, de las comunicaciones... Ésta última agrupa la seguridad de la documentación, seguridad informática y seguridad de la información.

1.3.2. LAS AMENAZAS O RIESGOS:

El segundo de los factores. El concepto de protección conlleva implícita la existencia de una amenaza: "de quién, o de qué" es preciso defender a las Personas, a los Bienes o a la Información. Hay que realizar, por lo tanto, un riguroso análisis de todas las amenazas que, de una forma u otra,

se ciernen sobre el objeto de protección. La determinación de los riesgos que realmente afectan, la selección de los riesgos que hay que afrontar, es una tarea básica en el Estudio de Seguridad. No debe quedar sin tratamiento ningún riesgo que realmente pueda producirse, pero no deben tratarse amenazas al problema concreto.

1.3.3. EL ESPACIO Y EL TIEMPO:

El fenómeno real de la agresión es una actividad que se produce, invariable e inevitablemente, en un lugar y en un momento determinados y tendrá, normalmente, un desarrollo en el espacio y una duración en el tiempo. Son las respuestas a las cuestiones de "dónde y cuándo" se va a producir la amenaza, siendo generalmente previsibles su itinerario y su tiempo de acción. El concepto de espacio es más amplio que el del tiempo, ya que puede estar constituido por cualquier lugar en el que pueda producirse la realización de un riesgo sobre un objeto de protección. El edificio constituye el más frecuente de los espacios a tratar, en materia de seguridad, pero también son frecuentes los espacios abiertos. El espacio, como factor de seguridad, tiene una importante relación con el objeto de protección que se encuentra en el mismo, y con las amenazas o riesgos que allí puedan producirse. Teniendo un tratamiento concreto con diferentes colectivos: - La población de un penal tiene un hábitat específico –el establecimiento penitenciario– y responde a unos riesgos inherentes a los reclusos y al edificio: evasión, motines, incendio... - Las personas ubicadas en un hotel, y en él, son previsibles determinados riesgos: incendio, hurto, robo... - Los empleados y clientes de una oficina bancaria, así como los bienes allí ubicados, pueden ser objeto de atraco, robo, hurto, estafa y fraudes, por ejemplo, dado el uso al que está destinado el inmueble. En cuanto al tiempo, hay que tener en cuenta que la ejecución de una amenaza sobre un objeto de protección tendrá, siempre, un momento de iniciación y una duración, por pequeña que ésta sea. La importancia de la estimación del factor tiempo está directamente relacionada con la posterior aplicación de los medios de protección, una de cuyas finalidades es la de proporcionar retardo a la acción agresora –medios pasivos– para facilitar la actuación de los medios humanos en contra de la agresión.

1.3.4. LOS MEDIOS DE PROTECCIÓN:

El cuarto y último factor de la seguridad, es la respuesta al problema planteado en el análisis de los tres anteriores: "Cómo, con qué" medios se pretende realizar la protección de las personas, los bienes o la información frente a las amenazas. Históricamente, el empleo tradicional de medios pasivos –muros, rejas, vallas...– sufrió una importante transformación con la incorporación al mundo de la seguridad de los medios electrónicos y óptimos, hacia la década de los sesenta del pasado siglo. La confianza en los nuevos medios indujo, sin embargo, al error de considerarlos autosuficientes, lo que produjo numerosos fracasos en sus primeros años de aplicación, haciendo evidente la necesidad de mantener los tradicionales medios pasivos. La concepción actual de la integración e interrelación de los medios técnicos –activos y pasivos– con los humanos, debidamente coordinados, constituye una sólida forma de dar solución a los problemas de Seguridad. Con carácter general, cada uno de los medios de protección, tienen unas funciones genéricas diferentes y complementarias.

1.3.4.1. MEDIOS MATERIALES

MEDIOS PASIVOS. - Muros, rejas, vallas, cristales especiales, puertas de seguridad... Su finalidad principal es la de proporcionar el retardo suficiente a la acción agresora, para asegurar la actuación de los medios humano de seguridad.

MEDIOS ACTIVOS. - Son el conjunto de sistemas de detección, centralización y óptica, principalmente. Su función es la de producir la necesaria alarma, desde el momento en el que se desencadena la amenaza y proporcionar información permanente de su desarrollo. Los medios ópticos pueden asegurar el seguimiento de la acción agresora en tiempo real, facilitando la actuación eficaz de los medios humanos de seguridad.

1.3.4.2. MEDIOS HUMANOS

MEDIOS OPERATIVOS. - Integrados por Vigilantes de Seguridad que pueden asumir los cometidos de operadores del centro de control, vigilancia y protección, en sus diversas formas. Tienen la función básica de reaccionar contra la acción agresora, para anularla o neutralizarla; además de personal capacitado para realizar funciones de control técnico de los sistemas.

MEDIDAS ORGANIZATIVAS. - Representadas por los planes parciales de actuación, las normas de seguridad, los procedimientos de seguridad de todo tipo y las órdenes de puesto. Tienen la finalidad esencial de garantizar la coordinación de los medios anteriormente citados.[6]

1.4. ALGO DE HISTORIA: SEGURIDAD PRIVADA

1.4.1. APARICION DE LA SEGURIDAD PRIVADA

En la antigüedad, mucho antes que apareciera el concepto de soberanía, el poder sobre la tierra, el control y gobierno sobre las personas, era medido en virtud de las capacidades bélicas de defensa, ocupación y de poder militar que determinado reino, imperio, feudo o cualquier tipo de seudo-estado demostraran; esto conllevaba al apoderamiento de territorios y de sociedades completas, desencadenando innumerables guerras y batallas que hicieron imposible un "orden". Ese modelo priorizaba la organización y mantenimiento de sus ejércitos a cualquier costo, inclusive si para ello fuera necesario incorporar soldados vencidos en batalla, dominados por ocupación o diplomacia, presentándose una combinación permanente de ejércitos y fuerzas multiculturales, raciales, religiosas y étnicas, como por ejemplo los persas: a medida que los persas iban incorporando a su imperio nuevas zonas, tenían una gran tolerancia religiosa, e incluso liberaron a muchos pueblos sometidos, como por ejemplo los hebreos que se hallaban deportados en Babilonia y estaban felices de contar con un gobierno que respetara y apoyara su religión; además de ser respetados, les proporcionaron nuevos mercados por tierra y apoyaron su desarrollo naval. El caso de los romanos: Este ejército había empezado a llamarse Legión. Todos los pueblos de Italia sometidos a

[6] http://docplayer.es/12345791-Indice-la-seguridad-nociones-generales-el-sistema-integral-de-seguridad-teoria-esferica-de-la-seguridad-zonas-y-areas-de-seguridad.html

Roma debían enviarle sus tropas y estos soldados estaban a las órdenes de oficiales romanos. Los mongoles: Gengis Kan utilizó con éxito la guerra psicológica en muchas de sus batallas, al sembrar terror y miedo. Él siempre ofrecía a sus enemigos la oportunidad de rendirse y pagar tributo, invadía y exterminaba los pueblos y ciudades, dejando vivos a los ingenieros, si los había, para incorporarlos a su ejército.

Después de siglos y siglos de desorden tanto en la seguridad interna como en la externa; se llega a un evento sin precedentes históricos. Se da el primer gran tratado internacional llamado, LA PAZ DE WESFALIA, que concedió la victoria del concepto de soberanía en contra del concepto de imperio. A partir de este momento, los estados empezaron a construirse y fortalecerse. Su génesis es un proceso complejo en donde el Estado moderno debe poseer el monopolio legítimo de la fuerza y que por tanto el poder que ostenta el estado es superior al poder de todos los individuos e instituciones dentro de un territorio dado. No obstante, la aparición de la industria de la seguridad privada no solo en Colombia si no en el mundo entero es producto de un fenómeno apenas lógico de necesidad de seguridad del ser humano; utópicamente la mayoría de las cartas constitucionales de todos los países, ofrece a los ciudadanos unas fuerzas militares y policiales para que hagan respetar sus derechos, sin embargo, es imposible responsabilizarse o cumplir con los fines del estado a todos y cada uno de los ciudadanos. [7]

1.4.2. LA SEGURIDAD PRIVADA EN LATINOAMERICA

La seguridad privada es un mercado que, a pesar de ser relativamente joven en América Latina, ha crecido rápidamente. Actualmente emplea formal e informalmente a un importante grupo poblacional, y suple la creciente demanda de seguridad que las sociedades requieren y que el Estado moderno no logra cubrir satisfactoriamente. El sector de la seguridad privada está compuesto por varios tipos de servicios como son: vigilancia, protección e investigaciones, los cuales son ofertados a ciudadanos/as individuales, empresas, instituciones y entidades gubernamentales, entre otros demandantes.

A nivel mundial, las empresas de seguridad privada han crecido substancialmente. En el 2003 el mercado de este servicio alcanzó los 85.000 millones USD, con una tasa de crecimiento anual del 7% al 8%. En el mismo año, el país con el mercado más grueso en seguridad privada fue Estados Unidos, con un valor de 42.000 millones USD. América Latina es la región que más se ha expandido en esta actividad (del 9% al 11%) valorizándose en 4.000 millones USD durante el 2003. Esta región es también una de las que más personal intensivo emplea parcialmente, a causa de una falta de mayor incorporación tecnológica. En el sector formal, Brasil tiene un aproximado de 570.000 guardias, seguido por México con 450.000, y en tercer lugar por Colombia con 190.000 vigilantes. Los países con el número más bajo de guardias legalmente registrados fueron Chile y Perú con 45.000 y 50.000, respectivamente. Así, se estima, bajo "especulación fundada", que existen alrededor de 2.000.000 guardias informales; es decir, el sector de la seguridad privada emplea a 4.000.000 de personas en América Latina. Dos de los grandes problemas de la seguridad privada en América Latina consisten en la creciente ilegalidad del sector y su falta de entrenamiento". Las

[7] http://repository.unimilitar.edu.co/bitstream/10654/9842/1/LopezGarciaRicardoAndres2012.pdf

empresas ilegales de seguridad privada del continente crecen a saltos más largos que las legales. En Argentina y Brasil, por ejemplo, el número de guardias empleados informalmente supera a los formales; mientras que Chile, no ha logrado identificar el número de guardias y de empresas ilegales que posee. Además, tanto la seguridad legal como la ilegal carecen de entrenamiento apropiado en toda la región (en cuanto a habilidades gerenciales y operativas).

La flexibilidad de la legislación de algunos países que no exigen ni controlan niveles de capacitación, y la falta de disposición de los clientes para pagar costos más altos por guardias con entrenamiento, son situaciones que dificultan los procesos de capacitación dentro de las empresas de seguridad privada. De este modo, considerando que este sector se halla en continuo crecimiento y posee una importante presencia en las dinámicas económicas latinoamericanas y mundiales, el gran desafío al que está expuesto el Estado es la regulación de esta fuerza corporativa; pues si bien va cubriendo las demandas de seguridad que exige la sociedad, también va superando la competencia estatal sobre la seguridad como bien público.[8]

1.4.3. LA SEGURIDAD PRIVADA EN COLOMBIA

Desde hace más de cinco décadas y debido al problema de origen socio- político suscitado en el país desde aquel 9 de abril de 1948, donde después de ser asesinado en Bogotá el caudillo Jorge Eliecer Gaitán se diera el famoso bogotazo; acción desbordada que originaría la cruenta guerra que se extendió por el territorio colombiano, entre los integrantes de los partidos liberal y conservador, lapso conocido dentro de la historia nacional como LA EPOCA DE LA VIOLENCIA, que resultó ser finalmente la real originadora de la toma del poder por parte del Sr. General Gustavo Rojas Pinilla, quien en 1953 realizara una tregua y diera fin a esa triste época Colombiana.

Teniendo en cuenta que la seguridad es un deber del estado para con sus ciudadanos sin distinción alguna como lo consagraba en su momento el artículo 19 de la constitución política de 1886: “Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en sus vidas, honra y bienes, y asegurar el respeto recíproco de los derechos naturales, previniendo y castigando los delitos”. Dadas las circunstancias socio– políticas por las que pasaba en este momento la nación, es donde comienzan aparecer las primeras compañías de Vigilancia y Seguridad Privada, motivadas estas por ciudadanos con ganas de proteger sus vidas y bienes del enfrentamiento entre partidos que amparados en unos ideales políticos causaban miedo y terror dentro de la población. Cabe resaltar que para esta época no existía más que un deficiente control de las mismas por parte de la Policía Nacional.

Fue inicialmente en 1966 con el Decreto 1667 dentro del "Estatuto Orgánico de la Policía" que se empieza a controlar, bajo tutela de la Policía Nacional, con la emisión de conceptos favorables para la prestación de vigilancia Privada en Colombia. Posteriormente, con el decreto 1355 de 1970, se faculta a la Dirección General de la Policía para la regularización del mismo. Un año después: 1971, el Decreto 2347 autoriza al Ministerio de Defensa Nacional a expedir licencias de funcionamiento para las compañías de vigilancia: “ARTÍCULO 15. Las empresas o sociedades privadas, destinadas a

[8] Libro Ciudad Segura (Seguridad Privada en Latinoamérica)

la vigilancia particular, solamente pueden constituirse o funcionar con autorización del Ministerio de Defensa Nacional, previa solicitud tramitada y conceptuada por la Dirección General de la Policía Nacional, y bajo control directo del respectivo Comandante del Departamento de Policía". En la década siguiente y debido al interés del gobierno nacional en reorganizar la Policía, se dictan medidas respecto de la vigilancia privada. Hasta este momento la reglamentación del servicio de vigilancia, recaía en manos de la Policía nacional, pero en el año de 1990 el Ministerio de Defensa Nacional, expide el "Estatuto de Vigilancia Privada" y el decreto 1195 del mismo año, apareciendo por primera vez una normativa clara en lo que concierne al servicio prestado por particulares de Vigilancia. Esta normatividad hace que toda la responsabilidad en cuanto a control quede bajo la tutela del Ministerio de Defensa nacional, con apoyo continuado de la Policía Nacional.

FIGURA 5. VIGILANCIA HUMANA PRIVADA

FUENTE: http://www.serviboyltda.com/

En los años venideros es donde realmente la Vigilancia privada toma un rumbo definitivo hacia la consolidación jurisprudencial, de la mano de la nueva Constitución Política Colombiana del año de 1991. Título I, Artículo 2, así:

> Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.
>
> Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los Particulares.

Teniendo en cuenta lo anterior y con la problemática socio-política colombiana, el gobierno Nacional decide que el Presidente está extraordinariamente facultado para dictar normas sobre armas, municiones y explosivos y Reglamentar la Vigilancia y Seguridad Privadas. Con la Ley 62 del 12 de agosto de 1993 "Por la cual se expiden normas sobre la Policía, se crea un establecimiento público de Seguridad social y Bienestar para la Policía Nacional, se crea la Superintendencia de

Vigilancia y Seguridad Privada y se reviste de facultades extraordinarias al Presidente de la República". Es en esta época, donde por primera vez se toca el concepto de seguridad privada de manera directa e independiente en nuestra nación. Para el año de 1994, precisamente el 11 de febrero, es promulgado el decreto 356, el cual rige hasta la actualidad el servicio de Vigilancia y Seguridad privada en Colombia.[9]

1.4.3.1. DECRETO LEY 356 DE 1994: POR EL CUAL SE EXPIDE EL ESTATUTO DE VIGILANCIA Y SEGURIDAD PRIVADA

En este decreto se reglamenta todo en cuanto a la prestación de los servicios de vigilancia y seguridad privada; desde la definición de lo que es una empresa de este tipo, o lo que se entiende por departamento de seguridad en una empresa de cualquier actividad hasta la definición de las cooperativas y de los servicios comunitarios de vigilancia y seguridad privada así como de los servicios especiales de vigilancia y seguridad privada, pasando por los requisitos necesarios para la constitución de una empresa en el ámbito de la seguridad, incluyendo datos sobre la obtención de licencia de funcionamiento para cada una de las definiciones nombradas y su renovación, pólizas de seguro; hasta las instalaciones que se deben tener.

Algunos artículos importantes dentro de lo que el decreto ley 356 de 1994 regula, son:

ARTÍCULO 1. OBJETO. El presente decreto tiene por objeto establecer el estatuto para la prestación por particulares de servicios de vigilancia y seguridad privada.

ARTICULO 2. SERVICIOS DE VIGILANCIA Y SEGURIDAD PRIVADA. Para efectos del presente decreto, entiéndase por servicios de vigilancia y seguridad privada, las actividades que en forma remunerada o en beneficio de una organización pública o privada, desarrollan las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones a la seguridad y tranquilidad individual en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, instalación, comercialización y utilización de equipos para vigilancia y seguridad privada, blindajes y transportes, con este mismo fin.

ARTICULO 3. PERMISO DEL ESTADO. Los servicios de vigilancia y seguridad privada, de que trata el artículo anterior, solamente podan prestarse mediante la obtención de licencia o credencial expedida por la Superintendencia de Vigilancia y Seguridad Privada, con base en potestad discrecional, orientada a proteger la seguridad ciudadana.

ARTICULO 8. DEFINICION. Se entiende por empresa de vigilancia y seguridad privada, la sociedad de responsabilidad limitada legalmente constituida, cuyo objeto social consista en la prestación remunerada de servicios de vigilancia y seguridad privada, en la modalidad de vigilancia fija, móvil y/o escoltas, mediante la utilización de cualquiera de los medios establecidos. [10]

[9] http://repository.unimilitar.edu.co/bitstream/10654/9842/1/LopezGarciaRicardoAndres2012.pdf
[10] Decreto Ley 356 de 1994

El presente decreto consta de 7 títulos: Aspectos generales; Servicios de Vigilancia y Seguridad Privada con Armas; Servicios de Vigilancia y Seguridad Privada sin Armas; Capacitación y Entrenamiento; Principios, Deberos y Obligaciones que rigen los servicios de seguridad; Medidas Cautelares y Sanciones; Disposiciones Comunes. En total, son 117 artículos.

1.4.3.2. REGULACION DE LOS SERVICIOS DE VIGILANCIA Y SEGURIDAD PRIVADA EN EL PAIS

LA SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA: es un organismo del orden nacional, de carácter técnico, adscrito al Ministerio de Defensa Nacional, con autonomía administrativa y financiera. Le corresponde ejercer desde el punto de vista técnico y administrativo el control, la inspección y vigilancia sobre el servicio público de vigilancia y seguridad privada en Colombia, contribuyendo a garantizar la confianza pública, la seguridad ciudadana, la armonía social y la convivencia, desarrollando mecanismos que promuevan la calidad, transparencia, responsabilidad, respeto y compromiso para el cumplimiento de los fines del Estado.

Para constituir una empresa de vigilancia y seguridad privada se deberá solicitar autorización previa a la Superintendencia de Vigilancia y Seguridad Privada, informando los nombres de los socios y representantes legales, adjuntando las hojas de vida con las certificaciones académicas y labores correspondientes. [11]

El lugar que la Superintendencia de Vigilancia y Seguridad Privada, ocupa dentro de la estructura del estado colombiano, es el siguiente:

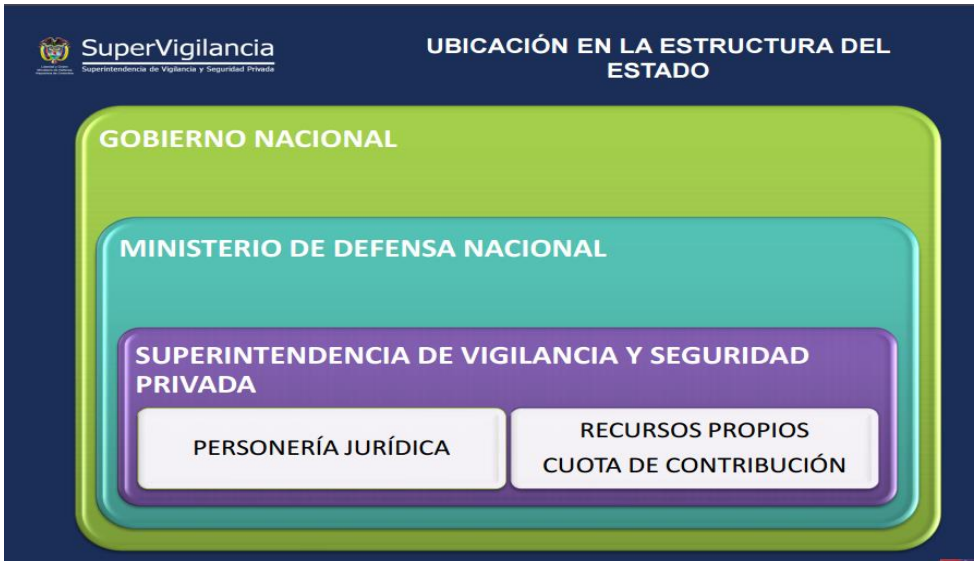


FIGURA 6. UBICACIÓN DE LA SUPERVIGILANCIA EN EL ESTADO COLOMBIANO

FUENTE: UNODC%20VIENA%2012%20al%2014%20de%20octubre%20de%202011.pdf

[11] http://www.supervigilancia.gov.co/

1.5. SEGURIDAD ELECTRONICA

Existen muchas definiciones de seguridad y en este caso puntual, se involucra el riesgo dividiéndola en seguridad humana y seguridad electrónica. La seguridad humana tiene como objetivo hacer presencia física con personas y la seguridad electrónica ayuda a través de la tecnología, a disminuir los riesgos.

FIGURA 7. SEGURIDAD ELECTRÓNICA

Fuente: http://www.techvolucion.com/en-en/inferencia.php

Hoy por hoy, se presenta la integración de la vigilancia con la presencia masiva de todo tipo de alarmas y detectores. Es de notar que la seguridad electrónica por sí sola no puede prestar la seguridad, se requiere del factor humano, tanto para el manejo como para la reacción en contra de la amenaza. Su tarea es la de alertar local o remotamente de un intento de violación o sabotaje de las medidas de seguridad física establecidas. El conjunto de medios que constituyen la seguridad electrónica, pueden utilizarse de forma oculta o visible.

Un sistema de seguridad electrónica será la interconexión de recursos, redes y dispositivos (medios técnicos activos) cuyo objetivo es cautelar y guardar la integridad de las personas y su entorno previniéndolas de peligros y presiones externas. El uso de estos recursos, dependerá de las características y necesidades de aquello que se va a proteger, considerándose el número de sitios a proteger, los riesgos potenciales de los mismos y necesidades especiales que se puedan presentar. Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, etc.), la vigilancia óptica mediante fotografía o circuito cerrado de televisión y la intercomunicación por megafonía y protección de las comunicaciones. [12]

[12] https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-1-definiciones

1.6. REDES DE TELECOMUNICACIONES

1.6.1. COMUNICACIÓN

La comunicación es un proceso que consiste en la transmisión de información entre un emisor y un receptor que decodifica e interpreta un determinado mensaje. La comunicación deriva del latín communicatïo que significa compartir, participar en algo o poner en común. A través de la comunicación, los seres humanos y los animales comparten información diferente entre sí, haciendo del acto de comunicar una actividad esencial para la vida en la sociedad.

El término comunicación también se utiliza en el sentido de conexión entre dos puntos, por ejemplo, el medio de transporte que realiza la comunicación entre dos ciudades o los medios técnicos de comunicación (telecomunicaciones).[13]

1.6.2. INFORMACION

La información está constituida por un grupo de datos supervisados y ordenados, que forman un mensaje. Es coleccionable, almacenable o reproducible. Así cómo es posible comunicar una noticia, también se comunican los estados de ánimo, opiniones o conocimientos. La información se origina en una fuente y se hace llegar a su destinatario por medio de un mensaje a través de un canal de comunicación; el destinatario generalmente se encuentra en un punto geográfico distante, o por lo menos, separado de la fuente. La distancia entre fuente y destinatario, puede variar desde pocos centímetros, hasta cientos y miles de kilómetros.

1.6.3. TELECOMUNICACIONES

Las telecomunicaciones son la trasmisión a distancia de datos de información por medios electrónicos y/o tecnológicos. Los datos de información son transportados a los circuitos de telecomunicaciones mediante señales eléctricas. Un circuito básico de telecomunicación consiste en dos estaciones, cada una equipada con un receptor y un transmisor, que se pueden combinar para crear un transceptor.

El tema central de las telecomunicaciones, radica en que una fuente y un destinatario están dos puntos geográficos distantes; y se trata de saber cuál es la mejor manera de hacer llegar al destinatario la información generada por la fuente, de manera rápida (por la dependencia temporal de la importancia de la información), segura (para garantizar que la información no caiga en manos de alguien que haga mal uso de ella, o a quien simplemente no estaba destinada), y veraz (garantizando que en el proceso de transmisión no se alteró el contenido de la información). En nuestros días, influidos fuertemente por aspectos económicos, intervienen factores como el costo de hacer llegar la información de la fuente a su destino. Si el factor costos no fuera determinante, con seguridad conversaríamos telefónicamente con amistades o parientes en otros países, sin importar la duración de las llamadas. [14]

[13] http://www.significados.com/comunicacion/

[14] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_4.htm

FIGURA 8. LAS TELECOMUNICACIONES

FUENTE: https://iutirlatelecomunicaciones.wikispaces.com/

1.6.4. ¿QUÉ ES UNA RED?

El término genérico red hace referencia a un conjunto de entidades (objetos, personas, etc.) conectadas entre sí. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas. Una red informática, es un conjunto de equipos y dispositivos periféricos conectados entre sí, la implementación de herramientas y tareas para conectar equipos de manera que puedan compartir recursos en la red. La red más pequeña posible está conformada por dos equipos conectados.[15]

1.6.5. SISTEMA DE TELECOMUNICACIONES

Consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones.

Se llama Red de Telecomunicaciones a la infraestructura encargada del transporte de la información. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales. Por ejemplo, para tener acceso a la red telefónica, el equipo terminal requerido consiste en un aparato telefónico; para recibir el

[15] https://sistemascomunic.wordpress.com/redes-de-telecomunicaciones/

servicio de telefonía celular, el equipo terminal consiste en teléfonos portátiles con receptor y transmisor de radio, etcétera. [16]

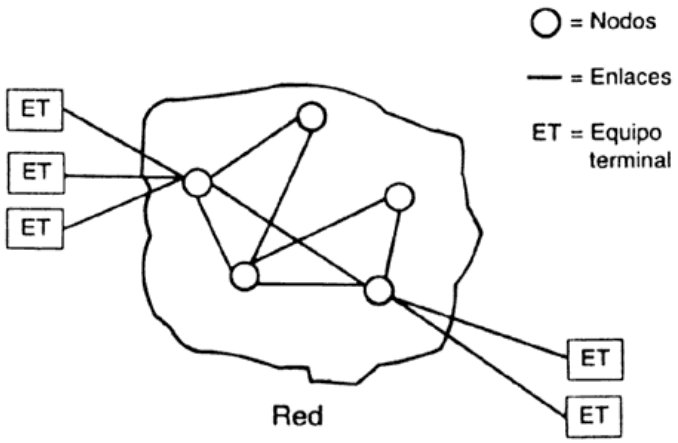


FIGURA 9. RED CON EQUIPOS TERMINALES

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

1.7. ALGO DE HISTORIA: TELECOMUNICACIONES

Durante un largo periodo en la historia de la humanidad, el correo fue la única forma de comunicación a distancia, desde luego adaptándose a las posibilidades que iban ofreciendo los nuevos adelantos tecnológicos: en lo que se refiere al transporte, del caballo se pasó a los barcos y los ferrocarriles, después a los automóviles y por último a los aviones. Fue necesario el descubrimiento de muchos fenómenos elementales de la física, tales como la electricidad y el magnetismo, para que surgieran competidores para el sistema postal. Los principios de las telecomunicaciones en que se apoyaron los científicos a partir de 1940, fueron las transmisiones radioeléctricas (las cuales permitieron el desarrollo de la televisión, la radio, las microondas y los satélites) y eléctricas (que a su vez dieron origen al teléfono, los cables submarinos, el télex y al concepto genérico de redes de telecomunicaciones).

Todo lo relacionado con las comunicaciones: las técnicas, la ciencia, la tecnología; se ha visto fuertemente impulsado por las necesidades militares de cada época. Una infinidad de hechos históricos documentan la caída de personajes, derrota de ejércitos y la pérdida de enormes fortunas, porque alguna de las partes en pugna contaba con información estratégica que las otras partes no poseían. La mayor influencia sobre las comunicaciones la tuvo la segunda Guerra Mundial: en esa época la humanidad ya se encontraba en la frontera de la revolución tecnológica, que las actuales generaciones hemos tenido la oportunidad de presenciar desde hace algunos años. Muchos de los sucesos que condujeron a la conclusión de la guerra, con el resultado conocido,

[16] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_8.htm

estuvieron relacionados con la disponibilidad de información oportuna o con la intercepción ingeniosa de información del enemigo. Los requerimientos de comunicaciones instantáneas, seguras y privadas de esa época fueron determinantes para que las comunicaciones sean lo que son hoy en día. La historia cuenta que en los últimos días de la guerra, Churchill y Roosevelt se comunicaban telefónicamente sólo si existía la seguridad de que nadie los escuchaba o si alguien lo hacía, no los entendería; esto se resolvió con el siguiente esquema: después de establecer una perfecta sincronización entre los equipos de ambos líderes, se usaban dos copias idénticas de grabaciones de ruido. Entonces, en las habitaciones donde iban a realizarse las conversaciones se activaba el inicio de las grabaciones idénticas, con la mayor precisión de tiempo posible, (por ejemplo: a las 00:00 horas GMT). Con esa ruidosa "música de fondo" transmitían su conversación: mientras uno de ellos sumaba el ruido a su voz antes de la transmisión, el otro lo restaba de lo que recibía (o sea, de la suma de voz y ruido); con esta última operación quedaba sólo la voz en el receptor. Cualquier intercepción de las transmisiones sólo hubiera sido capaz de reproducir el ruido, totalmente ininteligible, debido a que su volumen era mucho mayor que el de la voz.

El crecimiento y la maduración de las telecomunicaciones, la disminución de los costos reales de los servicios, y el aumento en disponibilidad, confiabilidad, seguridad y conectividad de los servicios ofrecidos, no han sido producto de desarrollos aislados y espontáneos de las comunicaciones independientemente; sino que han sido resultado de avances muy importantes en diversos campos del conocimiento como la ingeniería espacial y la aeronáutica, pasando por la ciencia de materiales y la física, hasta la tecnología digital, o sea, la electrónica y la computación. Aunque muchos avances, se lograron a partir de fines y propósitos militares, muchos otros, tuvieron sus orígenes en aplicaciones civiles; específicamente, en el caso del teléfono, la meta original ni siquiera era resolver un problema de telecomunicaciones, sino que fue producto de experimentos conducidos por Bell para ayudar a su esposa, quien tenía problemas auditivos. De hecho, lo que Bell pretendía era obtener un sistema que permitiera visualizar las señales de voz para auxiliarlo en sus labores de enseñanza a personas sordomudas.

El fascinante mundo de la transmisión de información a distancia, ha presentado considerables adelantos que fueron introducidos lentamente, mejorando lo existente hasta ese momento, conforme la ciencia y la tecnología lo iban permitiendo. Se desarrollaron el sistema telegráfico, el del teléfono, el de la radio y el de la televisión monocromática (blanco y negro). Sin estas experiencias no se hubiera podido evolucionar al sistema global de telecomunicaciones con que hoy se cuenta, y que permite establecer prácticamente de manera instantánea y automática la comunicación entre dos aparatos telefónicos cualesquiera del planeta. Tampoco se contaría ahora con el correo electrónico, la televisión cromática, las transmisiones de FM estereofónica, o las transmisiones de televisión de alta resolución con sonido de alta fidelidad. Por supuesto, no podríamos pensar ahora tampoco en las redes de computadoras.

Ambas guerras fueron las responsables de convertir experimentos caseros en trabajos de grupos bien coordinados, patrocinados por gobiernos y corporaciones, buscando colectivamente nuevos desarrollos y aplicaciones novedosas de técnicas conocidas. 1965: El producto de una interesante colaboración multinacional para el uso del espacio fue el lanzamiento y puesta en operación del primer satélite comercial de comunicaciones, el INTELSAT I, conocido también como el "Pájaro madrugador". El INTELSAT I tenía una capacidad de 240 circuitos telefónicos. Dos años después se

integraba un sistema global de comunicaciones vía satélite con la colocación en órbita de dos satélites adicionales de mayor capacidad, los INTELSAT II del Pacífico y del Atlántico, con lo cual se podía establecer comunicación telefónica (cerca de 720 circuitos para voz) entre cualesquiera ciudades del planeta. El INTELSAT V, puesto en órbita en 1980, puede procesar 12.000 llamadas telefónicas de manera simultánea, aparte de dos canales de televisión.1988: El primer cable transatlántico de fibras ópticas, el sistema TAT-8, fue puesto en operación entre Estados Unidos y Gran Bretaña. Sus propietarios son ATT y un consorcio de 27 compañías y oficinas gubernamentales europeas. Puede transportar simultáneamente 40.000 conversaciones telefónicas, lo cual es más que lo que pueden transportar todos los otros cables y enlaces satelitales transatlánticos combinados. Esto ocurrió 146 años después de que el primer conductor de señales sub-acuático fuera probado, en 1842 por S. Morse y E. Cornell, entre ambos lados del río Hudson.

Las comunicaciones internacionales vía satélite siguen creciendo. El sistema INTELSAT cuenta con 16 satélites en operación; 11 de ellos pueden transmitir entre 12.000 y 15.000 canales de voz y adicionalmente, dos de televisión. De acuerdo con estas tendencias es posible suponer que dicha capacidad podrá ser expandida en el futuro a una cantidad cercana a los 100.000 circuitos telefónicos. En los noventa se han incorporado los satélites a sistemas integrales de transmisión de información, con una gran variedad de medios de comunicación tales como fibras ópticas y cables metálicos. En 1996, se da el crecimiento explosivo de redes que enlazan todo el planeta, computadoras que se comunican a velocidades de millones de bits por segundo, telefonía celular, localización global de personas, redes personales de comunicación, televisión de alta definición, redes telefónicas interconectadas con redes de televisión por cable, realidad virtual, satélites de órbita baja, supercarreteras de información. Y es imposible concebir muchas actividades humanas cotidianas sin el apoyo de las telecomunicaciones: fax, teleconferencias, televisión a color, radiolocalización de personas, redes de computadoras, etc.

TELECOMUNICACIONES EN EL PRESENTE: A las épocas de grandes cambios en la historia de la humanidad, se les han asignado nombres especiales: Renacimiento, la Ilustración, Revolución industrial. En nuestros días, la última década del siglo XX, es de tal importancia poseer, administrar y transmitir información, que toda la humanidad se ve y se seguirá viendo afectada influida y posiblemente dominada por quienes tienen, administran y transmiten este recurso, razón por la cual a esta época se le han impuesto los calificativos de sociedad de la información o de Revolución electrónica, éste último debido a la facilidad con que se procesa y transmite la información por medio de los sistemas modernos basados en dispositivos electrónicos.

1.8. RADIODIFUSIÓN

Las transmisiones de radio y televisión tuvieron sus inicios en las dos primeras décadas del siglo XX, que darían origen a las transmisiones comerciales modernas. Tanto para el sistema de radio como para el de televisión (conocidos genéricamente como sistemas de radiodifusión) es necesario que las señales originales, que contienen la información que ha de ser transmitida, sean convertidas en

señales eléctricas, y posteriormente, convertirlas en señales electromagnéticas, las mismas que serán depositadas en la atmósfera para su transmisión.

En el sistema de la radio el proceso se realiza de la siguiente manera: las señales que contienen la información que se ha de transmitir son señales acústicas provenientes de la voz o de algún instrumento que genere música. La conversión de estas señales acústicas en eléctricas, se hace por medio de algún un sistema que acepta a su entrada señales acústicas (vibraciones mecánicas del aire) -un tipo de micrófono- y que a su salida genera señales con la información contenida, pero que ahora son de tipo eléctrico. En este caso, la información consiste en la forma de las señales, ya sea como función del tiempo, o bien, equivalentemente, en la manera en que está compuesta por señales de tipo senoidal. Es importante resaltar que para una reproducción exacta de la música es necesario conservar toda la composición de la señal, es decir, las frecuencias y las amplitudes a lo largo del tiempo, ya que esto es lo que permitirá diferenciar entre sonidos generados por una flauta, por un piano o por un coro, por ejemplo. La reproducción de las señales (es decir, la reconversión de señal eléctrica en señal acústica) se realiza por medio del proceso inverso: se inyecta la señal eléctrica en un sistema que genera, a partir de esta, señales acústicas. Normalmente esto ocurre por medio de bocinas o altavoces, los cuales tienen bobinas que mueven membranas de cartón, mismas que, a su vez, mueven el aire y generan las ondas perceptibles por el oído.

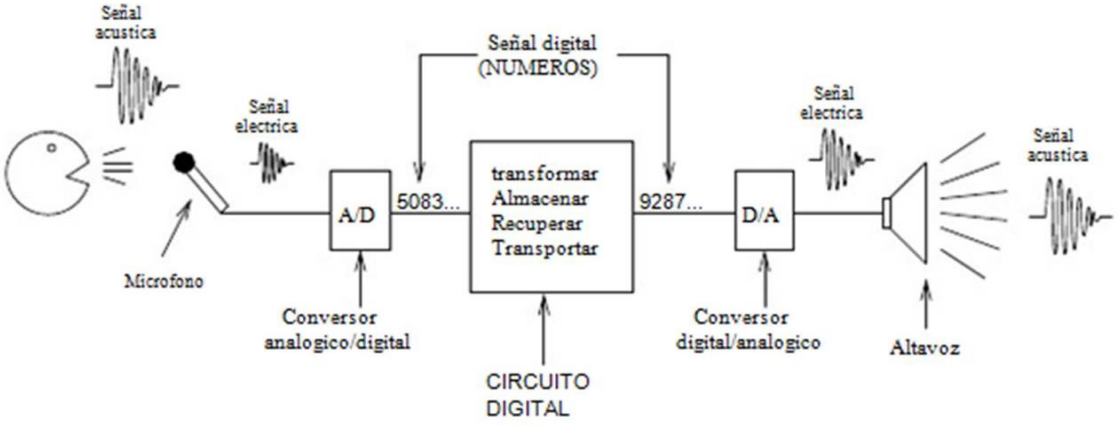


FIGURA 10. TRATAMIENTO DE LA SEÑAL DE VOZ

FUENTE: https://digitronica.wordpress.com/2009/09/10/electronica-analogica-vs-electronica-digital/

En el caso de la televisión, la señal que contiene los datos es de mayor complejidad que la de radio, ya que contiene, además de sonidos, información referente a composición luminosa de imágenes. El sonido, que recibe un tratamiento similar que en el caso de la radio.

Los tres elementos que contienen información acerca de las imágenes son:

- La distribución de luminosidad, es decir, la forma en que aparecen luces (blanco), sombras (negros) y las distintas tonalidades de grises;
- la composición de la imagen en función de las tres dimensiones espaciales; y
- los movimientos de los elementos mencionados

A través de cámaras de televisión se integran los tres factores anteriores en una señal eléctrica cuya amplitud varía con relación al tiempo. La conversión se realiza con un proceso de barrido: la cámara genera un haz que se mueve horizontalmente, detectando variaciones en las características luminosas de las imágenes. Al llegar al extremo derecho de la imagen, regresa el haz a la izquierda, se mueve ligeramente hacia abajo, y repite el proceso hasta llegar a la parte inferior derecha de la imagen. En ese momento el haz regresa a la esquina superior izquierda de la imagen y repite el proceso. El número de líneas horizontales determina la calidad de la imagen reproducida, y existen diferentes normas internacionales al respecto. Por otra parte, al igual que en el cine, para dar al ojo humano la sensación de imágenes que se mueven de manera suave, se generan imágenes fijas a razón de 60 por segundo. Cada imagen se genera por unas 525 líneas horizontales. Para no perder demasiado detalle, requieren captar y transmitir las variaciones más rápidas que sin la televisión podría captar el ojo humano. Esto requiere de un ancho de banda de 4.2 MHz. La parte de audio necesita una banda adicional de 25 kHz. Para evitar traslapes entre canales, entre dos canales adyacentes (por ejemplo, el 4 y el 5), se deja un espacio libre, conocido como banda de guardia.

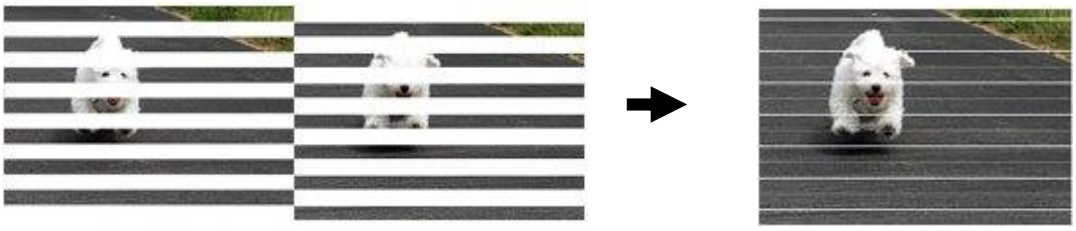


FIGURA 11. BARRIDO DE UNA IMAGEN

FUENTE: http://america.pink/interlaced-video_2093852.html

Además, para garantizar que la imagen en el aparato receptor sea de buena calidad, que no se mueva aleatoriamente, o que no aparezcan rayas horizontales o verticales en la pantalla, se requiere de información adicional en la señal; conocida como información de control o de sincronía y a través de ella se garantiza que el aparato receptor interprete cada imagen recibida como una imagen completa, es decir, que no tome y reproduzca la mitad de una imagen y la mitad de la siguiente para generar una imagen en el receptor. La reproducción se hace invirtiendo las operaciones realizadas en la conversión inicial: se toma la señal eléctrica y se inyecta en un sistema que realiza un barrido en la misma forma que la descrita, generando a su paso puntos de diferente luminosidad e intensidad en la pantalla; con 60 imágenes fijas por segundo, cada una compuesta por 525 líneas horizontales. La generación de imágenes cromáticas está basada en los mismos principios básicos, y con procedimientos más complejos necesarios para el envío y la recepción de la información de los colores.

Una vez que se cuenta con las señales eléctricas equivalentes, las transmisiones tanto de radio como de televisión se realizan de una manera muy parecida. Se emplean sistemas de transmisión que consisten básicamente en los siguientes componentes:

a) MODULADOR: su función consiste en trasladar el espectro de la señal a la banda en que debe realizarse la transmisión. Cada canal que se transmite, tanto en radio como en televisión, tiene una distinta frecuencia portadora, y esto es precisamente lo que ubica a un canal en el sitio adecuado del sintonizador del receptor. Por ejemplo, en radio (AM) la portadora de una señal que se recibe en 600 kHz del cuadrante, tiene una frecuencia de 600 kHz.

b) TRANSMISOR: cuya función consiste en amplificar la señal proveniente del modulador e inyectarla en la antena de transmisión.

c) ANTENA DE TRANSMISIÓN: encargada de inyectar en la atmósfera la señal proveniente del trasmisor.

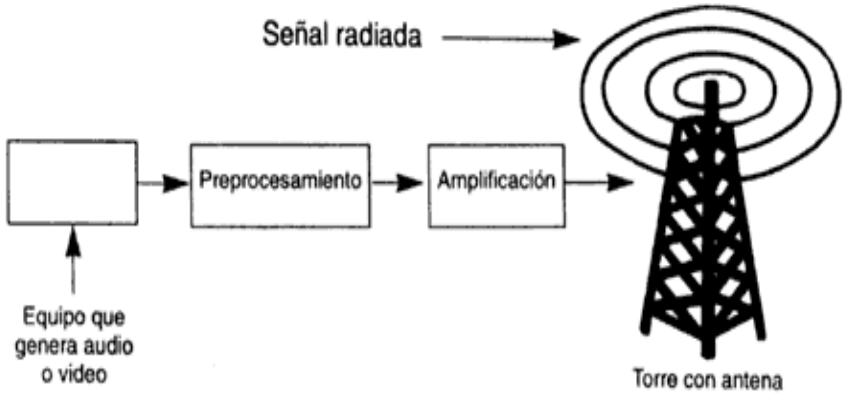


FIGURA 12. SISTEMA DE TRANSMISION DE RADIODIFUSIÓN

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_6.htm

Es conveniente resaltar que, si bien estos sistemas de telecomunicaciones no son los únicos que estaban disponibles durante la primera mitad de este siglo, en ellos se conjugan las bases que posteriormente serían utilizadas para desarrollar sistemas más avanzados. Los principios básicos de operación de estos sistemas tradicionales de comunicación tienen cada uno de ellos sus peculiaridades, pero comparten, sin embargo, muchos elementos comunes. Los elementos comunes de estos sistemas y las diferencias entre ellos han dado origen a los sistemas modernos de telecomunicaciones.[17]

[17] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_6.html

1.9. FORMAS DE TRANSMISION EN TELECOMUNICACIONES

Las telecomunicaciones se han convertido en un satisfactor de necesidades cotidianas de un importante número de habitantes y corporaciones del planeta. En un principio las telecomunicaciones se realizaban empleando señales cuya magnitud es una función directa del mensaje que se desea transmitir: en telefonía, por ejemplo, mediante la correspondencia de una señal de voltaje de amplitud grande a sonidos de volumen alto, y señales de amplitud pequeña a sonidos de bajo volumen (transmisión analógica). Las transmisiones de este tipo pueden tener problemas serios: si se le suma el ruido (invariablemente presente en todo canal de comunicaciones) a la señal transmitida, considerando que este ruido también tiene como efecto señales de amplitud variable desconocida e impredecible, entonces lo que se recibe en el receptor estará distorsionado por el ruido. Por ejemplo, el diálogo en una discoteca donde la música está a un volumen altísimo, es en realidad difícil, puesto que el "ruido del canal" normalmente tiene un volumen mucho mayor que el de la voz en una conversación, aun si se pretende hablar a gritos. (No obstante, es importante recordar, para este ejemplo, que los seres humanos contamos también con los lenguajes gestual y corporal.)

El ruido es un fenómeno inevitable en las comunicaciones. Desde la ingeniería, se diseñan sistemas que permitan hacer llegar la información de la fuente al destino a pesar del ruido, el cual, además, varía con el tiempo y es más perjudicial en algunas ocasiones que en otras.

Para resolver el problema del ruido se dispone de las comunicaciones digitales, que están basadas en el siguiente principio: suponiendo que la información está contenida en colores de cualquier tonalidad del espectro visible; al modificar ligeramente algún color, es difícil establecer de manera precisa cuál era el color original. Por ejemplo, si en lugar de ver azul rey se observa azul marino, no hay forma de saber si originalmente se tenía azul rey o azul marino. (El concepto mismo de la tonalidad de los colores es subjetivo y puede variar de persona en persona). Por otra parte, si únicamente se puede observar blanco o negro, es viable establecer reglas de decisión sencillas para determinar si un tono específico de gris originalmente era blanco o negro. Es decir, a partir de qué tono de gris (del más claro hasta el más oscuro) se decidirá negro, con el sentido de que las tonalidades más claras corresponden al blanco.

El mismo principio se aplica a las comunicaciones digitales, con la excepción de que se trata de "unos" o "ceros". Recordando que en toda transmisión hay ruido, si se transmite el voltaje correspondiente a un "cero" (0 volts) y se le suma ruido que hace aparecer a ese valor como un 0.4, se decidirá que lo transmitido fue un cero, mientras que si se reciben valores mayores de 0.5, la decisión a tomar será "uno". Recurriendo nuevamente al ejemplo de la discoteca con música a un volumen en extremo alto, si las personas que dialogan sólo disponen de dos palabras-gesto por ejemplo sí y no, aun estando muy alto el volumen resulta mucho más fácil decidir si lo que dijo la otra fue precisamente un sí o un no.

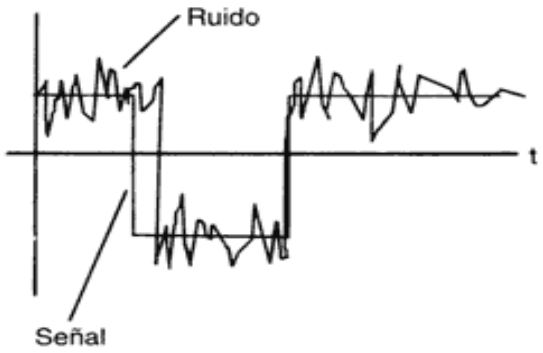


FIGURA 13. SEÑAL DIGITAL CON RUIDO

FUENTE: http://www.cubaeduca.cu/medias/cienciatodos/Libros_3/ciencia3/149/htm/sec_7.htm

Las comunicaciones digitales tienen las siguientes ventajas sobre las analógicas: como las computadoras trabajan con información digital, esta debe ser procesada en microprocesadores digitales (una de las razones por las cuales se habla de convergencia entre la electrónica, las telecomunicaciones y la computación), con lo cual se aumentan enormemente las posibilidades de procesamiento a grandes velocidades y de almacenamiento masivo de la información. Estando la información en formato digital, es posible explotar plenamente las técnicas modernas de criptografía, codificación, compresión de datos, corrección y detección de errores y el procesamiento digital en general.

Para explicar cada una de las ventajas de las comunicaciones digitales, se puede referenciar uno de los primeros sistemas de comunicaciones del que se tiene documentación: el sistema de Polibio, que podría ser llamado "telégrafo síncrono apoyado en medición hidráulica de tiempo y en señalización óptica."

Se trata de un sistema en el cual el mensaje que se desea transmitir pertenece a un conjunto finito de mensajes; es evidente que para que este tipo de comunicaciones tenga sentido, ambas partes (receptor y transmisor) deben estar conscientes de los posibles mensajes que uno transmitirá al otro. Conviene describir su operación: Mediante una antorcha se envía una señal de un punto geográfico a otro para poner en operación el sistema hidráulico por medio del cual el receptor obtendrá la información que se desea. Desde un punto de vista estricto, este sistema de comunicaciones digitales contiene también elementos de procesamiento distribuido: la información que se transmite es la señalización (las antorchas), que se usa para activar el sistema de procesamiento, que a su vez consiste en los cilindros con agua, y las reglas sobre las cuales están marcados los posibles mensajes; a estos últimos, en lo sucesivo, se les llamará cilindros codificadores. Con la señal de la primera antorcha se abren las dos válvulas por las que saldrá agua y bajará el nivel de los cilindros codificadores; con la segunda señal se cerrarán las válvulas para tomar la lectura (es decir, el mensaje) en el cilindro codificador del lado del receptor.

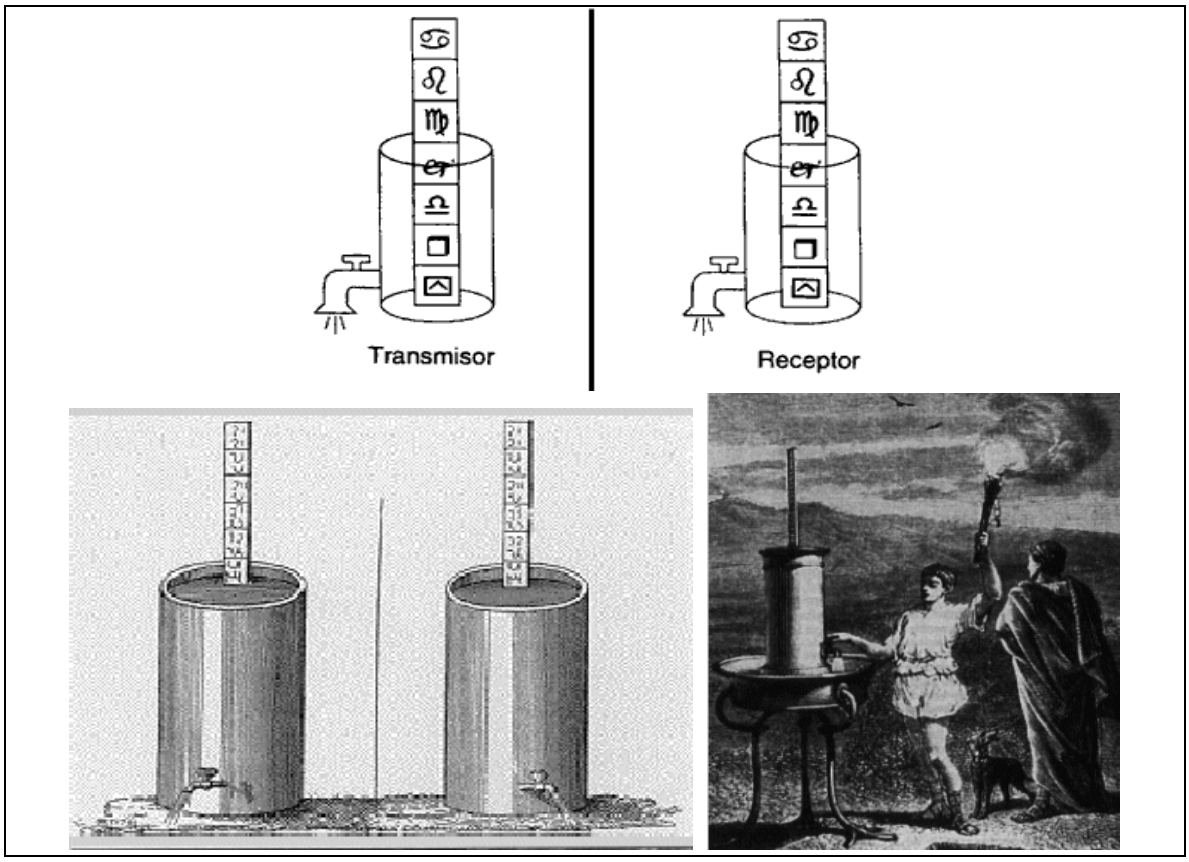


FIGURA 14. SISTEMA DE POLIBIO

FUENTE: http://www.ea1uro.com/eb3emd/Telegrafia_hist/Telegrafia_hist.htm

En este sistema se pueden identificar y explicar algunos problemas relacionados con y de fundamental importancia, para las telecomunicaciones digitales:

a) Conversión analógico-digital de una señal: La altura de los cilindros codificadores, sobre los cuales están marcados los mensajes, puede tomar cualquier valor entre la altura máxima (recipiente externo totalmente lleno) y la mínima (recipiente externo totalmente vacío). Es decir, la altura es una variable analógica. Sin embargo, cada mensaje tiene asociada una zona o un rango de alturas, al cual le corresponde cada uno de los mensajes. Si existen diez posibles mensajes, existen también diez posibles regiones de altura. Este proceso es, evidentemente, una conversión analógica a digital y tiene incorporado un proceso de cuantización.

b) Codificación de un mensaje: La salida del sistema, una vez se cierra la válvula es la altura del cilindro interno del sistema; sin embargo, como el cilindro está subdividido en regiones, y a cada región le corresponde un mensaje, el mensaje está codificado. A cada altura posible le corresponde uno y sólo uno de los posibles mensajes. El conjunto de mensajes se conoce con el nombre de alfabeto de salida del codificador o conjunto de mensajes codificados.

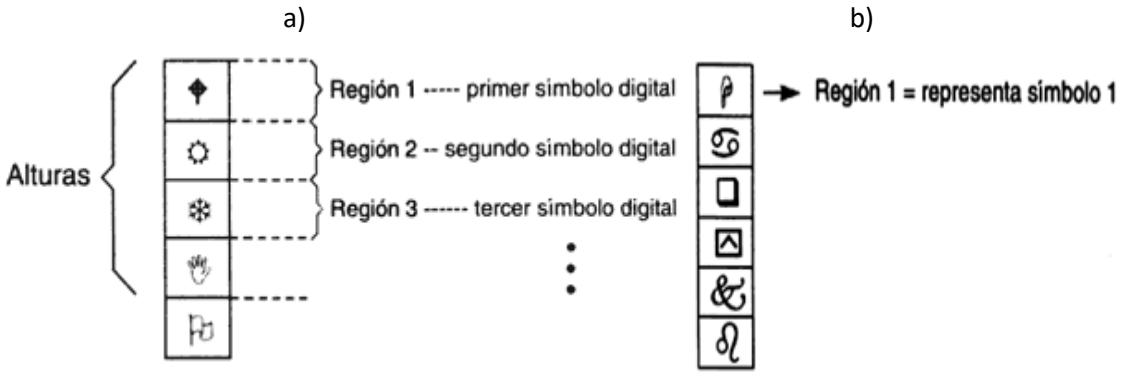


FIGURA 15. a) CONVERSION ANALOGA-DIGITAL b) CODIFICACIÓN DEL MENSAJE

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_7.htm

c) Criptografía del mensaje: La criptografía es la ciencia de cifrar información de manera tal que únicamente aquellas personas que conocen la forma en que fue cifrada la información y las claves con que fue realizado el proceso de cifrado, pueden descifrarla. Pues bien: a pesar de que cualquier persona podría, en teoría, construir su propio "telégrafo síncrono apoyado en medición hidráulica de tiempo y en señalización óptica", no cualquiera podría recibir adecuadamente los mensajes transmitidos por los guerreros romanos, ya que el sistema tiene intrínseco un sistema criptográfico con dos claves. La primera consiste en la forma en que fue codificada cada una de las alturas del cilindro codificador, esto es, el mensaje asociado a cada región tiene que ser conocido tanto por el receptor como por el transmisor. La segunda está en la apertura de las válvulas, ya que si el flujo de agua no es igual en transmisor y receptor, las alturas de los cilindros donde la información está codificada serán diferentes a la hora de cerrar las válvulas, por lo cual generarán diferentes mensajes. Es más, para darle mayor seguridad al envío de información, por ejemplo, receptor y transmisor podrían disponer de dos diferentes válvulas y tres cilindros codificadores con la información codificada de diferentes maneras; por medio de la antorcha se podría señalizar la válvula que será utilizada y cuál es el cilindro flotador empleado. El enemigo (técnicamente llamado "cripto-analista") no conoce el mensaje correcto, excepto si usó la misma válvula y el mismo cilindro. Cabe mencionar que el enemigo podría deducir las claves observando las acciones correspondientes a cada clave; por esto resulta recomendable que en cada transmisión se cambie la clave (clave dinámica).

d) Sincronización entre transmisor y receptor: El problema de la sincronización consiste en que tanto el receptor como el transmisor deben trabajar a la misma velocidad para que el primero extraiga del canal, la información a la misma velocidad que el transmisor la inyectó en el canal. En el Sistema de Polibio, la sincronización está implícita en la señalización por medio de la antorcha, así como en la velocidad con que se permite la salida del agua de los contenedores. Si en algún momento se pierde la sincronía, no puede realizarse adecuadamente el proceso de comunicación.

e) Necesidad de un protocolo: Así como dos personas necesitan establecer un conjunto de reglas por medio de las cuales puedan establecer comunicación, y en ausencia de ellas no es posible

comunicarse, esto también es aplicable en comunicaciones entre sistemas (equipos o computadoras). Por ejemplo, dos personas que se comuniquen telefónicamente, las reglas (que dependen de cada país y que aceptan ligeras variaciones) son las siguientes: al sonar el timbre del teléfono, el receptor toma el auricular y dice "bueno" en México, "hola" en España, "hello" en Estados Unidos, etc. Posteriormente, quien inició la llamada (transmisor) dice algo como "¿a dónde hablo? “, ... y así sucesivamente. La necesidad de contar con reglas que ambos interlocutores entiendan y respeten, se hace evidente; en este caso, son las siguientes:

- El transmisor enciende su antorcha y abre la válvula de su contenedor de agua,
- el receptor al ver la antorcha del transmisor, abre su válvula y espera, sin dejar de observar en la dirección del transmisor,
- al haber sido desalojada la cantidad de agua para que el mensaje del cilindro codificador sea el correcto, el transmisor envía nuevamente una señal con su antorcha,
- el receptor, al ver la nueva señal, cierra su válvula, observa el mensaje en su cilindro, toma una decisión e instrumenta la acción que corresponde al mensaje recibido.

Sin un protocolo sería muy difícil lograr establecer una comunicación entre seres humanos, y, por ende, sería prácticamente imposible entre entes tales, como equipos o computadoras.

f) Presencia de distorsión y de ruido en las comunicaciones: La distorsión en un sistema de comunicaciones consiste en todo aquello que perturba el contenido de la información de un mensaje. Es decir, lo que dificulta al receptor la interpretación correcta del mensaje que le envió el transmisor. En el sistema de Polibio, la distorsión se puede presentar cuando los orificios (válvulas) por donde sale el agua de los recipientes del transmisor y del receptor no son del mismo tamaño; en ese caso, aun si los orificios permanecieran abiertos el mismo tiempo permitirían que en cada uno de los recipientes escapara una cantidad diferente de agua y que, por tanto, al final del mensaje sus respectivos niveles de agua (código del mensaje) fueran distintos, impidiendo una comunicación correcta. Otras posibles fuentes de ruido en este sistema son distintos volúmenes de agua en los contenedores al iniciar la transmisión, diámetros diferentes de los cilindros de agua citados como recipientes, o bien, diferencias en la forma en que fueron marcadas las alturas correspondientes a las regiones en ambas reglas.

g) Detección y toma de decisiones en las comunicaciones: En todo sistema de comunicaciones digitales, en el lado del receptor deben ser tomadas decisiones acerca del mensaje que envió el transmisor, ya que, por el efecto del ruido y la distorsión, las salidas del sistema podrían estar en alguna zona ambigua en la que no esté totalmente claro el mensaje enviado. En los sistemas modernos, en que las señales son unos o ceros, representados por voltajes, al sumárseles el ruido, puede no estar claro cuál fue el símbolo transmitido. Por ejemplo, si no hubiera ruido, un voltaje de 1 volt podría ser un "uno" y un voltaje de cero, podría ser un "cero"; pero si el ruido contribuye con, por ejemplo, 0.25 volts, la decisión que debe tomar el receptor es si ese voltaje que, si bien no es cero, tampoco es un claro "uno", corresponde ya sea a uno o al otro símbolo. En el sistema de Polibio, puede ocurrir que al cerrar el orificio la marca de las alturas no quede exactamente a la mitad de una región, caso en el cual la decisión consiste en evaluar las posibilidades de que dicho desplazamiento pueda haber sido originado por el mensaje que está en la parte superior o en la inferior de la marca deseada.

FIGURA 16. EJEMPLO DE ZONA AMBIGUA POR EFECTO DE RUIDO EN EL MENSAJE

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_7.htm

El sistema descrito puede ser ampliado para darle una mayor precisión y mejorar su desempeño; esto podría ser realizado, por ejemplo, con las siguientes modificaciones:

1) Confirmando recepción correcta y/o solicitando una retransmisión. En el caso del telégrafo óptico-hidráulico, el papel que desempeña el receptor es pasivo, es decir, se limita a recibir los mensajes, pero no toma ninguna acción en caso de tener duda acerca de los mismos. Sin embargo, se podrían utilizar antorchas en el lado del receptor, pidiendo retransmisiones al transmisor hasta que el receptor esté satisfecho con el mensaje recibido y no tenga duda acerca de lo que debe hacer. Este sistema de telecomunicaciones puede funcionar de dos maneras: i) el transmisor envía mensajes y supone que el receptor los recibe adecuadamente, pero no espera que el receptor le confirme si esto ocurrió. ii) el transmisor comunica su mensaje, el receptor lo recibe y emite una señal de confirmación al transmisor cuando no tiene duda acerca del mensaje recibido; en caso de duda, le envía una solicitud de retransmitir. En este caso, tanto en la parte de transmisión como en la de recepción, tendrían que ser reinicializados los sistemas antes de la nueva transmisión (esto es, tendrían que volver a llenar de agua sus recipientes).

2) Introduciendo repetidoras. Cuando el alcance requerido por un sistema de telecomunicaciones es mayor que el permitido por la tecnología seleccionada, puede realizarse la comunicación por etapas, cubriendo distancias cortas y repitiendo los mensajes hasta que lleguen a su destino. En el sistema estudiado una ampliación lógica, consiste en la introducción de repetidoras; cada una de las repetidoras desempeñaría el papel de receptor, por una parte, con todas las funciones que éste tiene asociadas y, por la otra, el de transmisor hacia la siguiente etapa, también con cada una de las funciones que tiene asociado un transmisor.

3) Agregando redundancia. La redundancia consiste en agregar a un mensaje elementos que faciliten al receptor la toma de decisiones acerca del mensaje transmitido. En el caso del telégrafo óptico-hidráulico, esto puede ser realizado si el receptor tiene, por ejemplo, tres sistemas idénticos. Cuando observa la señal de la antorcha indicándole que debe abrir la válvula, lo hace simultáneamente en los tres, y hace lo mismo en el momento de cerrarlas. Al tomar la lectura, lo hace en los tres sistemas, y toma su decisión con base en los tres. Así, si las tres lecturas coinciden no hay duda, pero si una de ellas señala algo diferente a lo de las otras dos, el receptor basa la decisión en la mayoría. Con esto disminuye significativamente la probabilidad de errores.

4) Permitiendo transmisiones punto a multipunto. Frecuentemente es necesario contar con los mensajes transmitidos en más de un punto de manera simultánea. A diferencia del caso en que se transmite de un solo punto y el mensaje está destinado a un solo punto (transmisión punto a punto), esto se conoce como transmisión punto a multipunto (siendo el precursor de la radiodifusión). En caso de requerirse, el sistema en estudio es fácilmente convertible a un sistema punto a multipunto. Esto implica tener varios receptores en distintos lugares. Todos deben estar familiarizados tanto con los códigos como con las claves criptográficas, para que los mensajes sean recibidos exitosamente en tantos puntos geográficos como fuera necesario (evidentemente, dentro de la zona de cobertura del sistema, es decir, en aquellos puntos en que pudieran ser observadas las señales ópticas provenientes de la antorcha del transmisor).

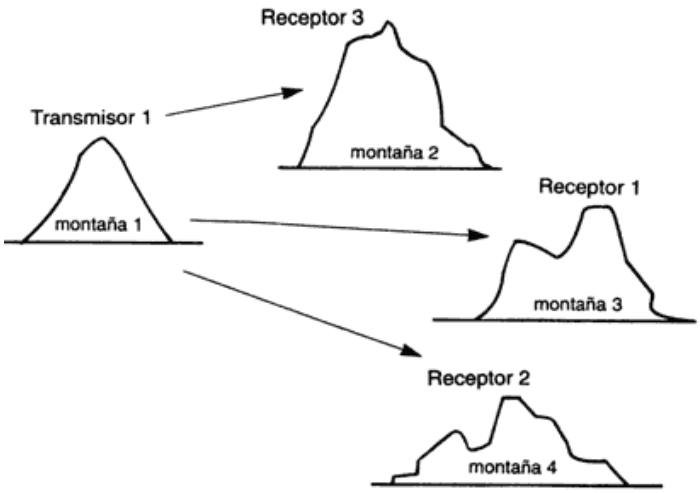


FIGURA 17. TRANSMISION PUNTO A MULTIPUNTO

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_7.htm

Al utilizar las ideas básicas de comunicación, con equipos y sistemas basados en tecnologías modernas, se han logrado manejos de cantidades de información a velocidades que aun en la primera mitad del siglo pasado, parecían imposibles de alcanzar.

Los científicos de la primera mitad del siglo XX, aunque desde luego no tenían sistemas digitales, estaban conscientes del efecto potencial que podría tener esta nueva forma de representar y procesar una señal por medio de dos símbolos únicamente, y empezaron a estudiar el problema desde el punto de vista teórico. En 1949, C. E. Shannon propuso lo que llamó una "Teoría matemática de la comunicación", donde analiza las siguientes cuestiones fundamentales: a) ¿Cómo se puede medir la cantidad de información contenida en un mensaje? b) ¿Cómo se puede medir la capacidad que tiene un canal para transmitir información? c) Cuáles son las características deseables para un codificador?; y cuando este proceso se realiza en forma eficiente, ¿cuánta información puede ser enviada a través de un canal? d) ¿Cuáles son las características generales de los procesos de ruido y cómo afectan la calidad de los mensajes recibidos en el receptor?

Los conceptos y las ideas contenidos en dicha teoría han servido desde su publicación, como semillas para la mayoría de los trabajos modernos de las comunicaciones digitales. Se postulan definiciones de índices óptimos de desempeño, y se demuestra la existencia de mecanismos de procesamiento de información: un buen número de los resultados actuales giran alrededor de la obtención, el diseño y la realización electrónica de sistemas y dispositivos electrónicos que alcancen o por lo menos se aproximen tanto como se desee a los desempeños predichos por Shannon.

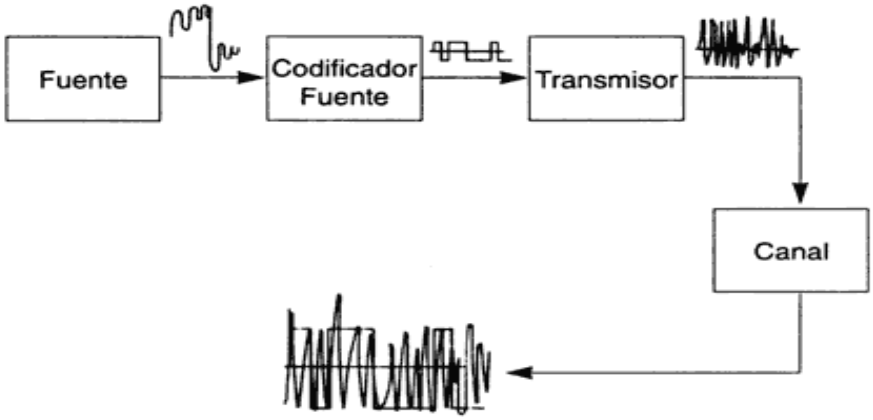


FIGURA 18. SISTEMA DE COMUNICACIONES CON TRANSFORMACIONES

FUENTE:
http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_7.htm

En el bloque que sigue a la fuente, es decir, el codificador de la fuente, se realiza la función de convertir el mensaje proveniente de la fuente (el cual no necesariamente es de tipo digital o binario) en un mensaje binario.

A su salida se tiene conectado el codificador del canal. Su función es proteger la información transmitida contra los efectos y fenómenos a que está expuesta al viajar a través del canal. Esto se logra agregando redundancia a la información transmitida, con el objeto de que en el lado del receptor se pueda identificar cuándo ocurrió esta situación. A través de bloques o palabras largas es más fácil la inmunización contra el efecto del ruido. Para ilustrar esto considérese un sistema que introduce redundancia de manera tal que se transmite tres veces cada letra de un mensaje que puede consistir en cadenas de letras del alfabeto de 32 posibilidades. Al ocurrir un error se toma una decisión basada en mayorías. Por ejemplo, si se desea transmitir la palabra "mamá", con este esquema se codifica en "mmmaaammmááá". Si en el receptor se recibe "mmmaaxmnmááá", al aplicar la decisión por mayoría, se llega nuevamente a "mamá", porque las tercias aax y mnm se interpretan o decodifican como "a y m" respectivamente. En el mejor de los casos se podrán corregir los errores, pero para facilitar el procesamiento muchas veces es suficiente detectar la presencia de uno o más errores, aunque no se identifique su posición (nótese que en un sistema binario, al identificar la presencia y posición de un error su corrección es inmediata, puesto que en

un sistema donde solamente hay dos posibles símbolos, un "uno" y un "cero", la única forma en que puede aparecer un error es cambiando un "uno" a un "cero" o un "cero" a un "uno"). Identificando la presencia de un error, aunque no su posición, el receptor puede solicitar al transmisor la retransmisión del mensaje.

El canal, desde un punto de vista estricto, no pertenece ni al lado del transmisor, ni al del receptor, sino que es el elemento que une a ambos lados del sistema. No hay canal perfecto, es decir, todo canal introduce ruido. Independientemente del material del que está construido el canal, éste transporta la información digital o binaria por medio de pulsos de dos distintos valores. Si el canal es metálico, los pulsos serán de voltaje; si es óptico, los pulsos se representan por medio de intensidades luminosas. La forma en que transmite la información es precisamente una de las características que hacen que un canal sea distinto de otro. Pero desde el punto de vista de la teoría de la información, el parámetro más importante de un canal consiste en lo que se denomina su capacidad, es decir, la cantidad de información que puede transmitir por unidad de tiempo. La capacidad de un canal depende, entre otros factores, del material del que está construido. Las capacidades de los canales han evolucionado desde valores pequeños, tales como las de los canales telefónicos (estas capacidades, aunque pequeñas, no fueron motivo de preocupación cuando fueron construidos los primeros canales telefónicos, porque no se disponía de los elementos tecnológicos para poder aspirar a alcanzar la capacidad de los canales). Las capacidades más grandes disponibles en la actualidad, son las de canales basados en fibras ópticas.

Finalmente, del lado del receptor se realizan las operaciones inversas a las efectuadas en el lado del transmisor: el decodificador del canal decide si en la transmisión de un símbolo hubo error o no, y hace lo posible por identificar su posición para corregirlo, o, en su caso, solicitar una retransmisión del mensaje. El decodificador de la fuente reconstruye la señal original a partir de la sucesión binaria que le envía el decodificador del canal, para así entregar al usuario final la versión reconstruida de lo que fue generado en la fuente. [18]

[18] http://bibliotecadigital.ilce.edu.mx/sites/ciencia/volumen3/ciencia3/149/htm/sec_7.html

CAPITULO 2

2. ENTORNO

2.1. LA EMPRESA

FIGURA 19. LOGO SERVIBOY

FUENTE: http://www.serviboyltda.com

SERVIBOY LTDA es una Empresa de Vigilancia Privada Boyacense con gran trayectoria y experiencia en la prestación de servicios profesionales de Vigilancia Humana y Seguridad Electrónica avalados por la Superintendencia de Vigilancia y Seguridad Privada.

2.2. UBICACION

La sede principal está ubicada en la ciudad de Tunja, se encuentra dotada con los últimos avances en telecomunicaciones incluyendo receptoras y software de monitoreo de última generación, planta telefónica basada en tecnología IP, video vigilancia y central de monitoreo para sistemas de alarmas.

FIGURA 20. SEDE PRINCIPAL DE LA EMPRESA

FUENTE: http://www.serviboyltda.com

MISIÓN

Ofrecer servicios de Vigilancia Humana, consultoría y asesoría, enfocados en las últimas tecnologías de seguridad para brindarle confort y tranquilidad en su residencia, empresa o donde quiera localizar nuestros servicios. Nuestro completo portafolio incluye: Vigilancia Privada, Video Vigilancia, CCTV, Acceso Peatonal, Control de Acceso, Detección y Control de Incendios, Detección y Control de Intrusos con Sistemas de Alarmas, Servicio Técnico de Instalación y Mantenimiento de Alarmas.

VISIÓN

Nos proyectamos como la empresa de vigilancia líder en servicios de Seguridad Privada, incluyendo Seguridad Humana y Electrónica en Colombia. Con recurso humano estrictamente seleccionado y capacitado, utilizando tecnología de punta proveniente de proveedores líderes en el mercado mundial; brindamos soluciones integrales de seguridad y protección. Nuestro objetivo es ofrecerle tranquilidad y seguridad para su hogar, su empresa, o donde lo requiera.

HISTORIA

SERVIBOY LTDA, fue fundada en el año 1988, bajo la dirección del Mayor en retiro del Ejército, Héctor Amín Waked Hernández, con sede principal en la ciudad de Tunja, prestando servicios de Seguridad privada y Vigilancia humana en el departamento de Boyacá. En el año 2001, la empresa opta por adquirir nueva tecnología en comunicaciones, y así mismo, renovar el tipo de armamento existente; logrando así, incrementar los puestos de vigilancia y seguridad.

En el año 2004, se amplía nuestro portafolio de servicios incluyendo la Seguridad electrónica, con el fin de prestar servicios de monitoreo las 24 horas, video vigilancia, seguimiento infantil y vehicular, por medio de sistemas de seguridad electrónica como Alarmas, Cámaras de seguridad, Circuitos cerrados de televisión, controles de acceso y cerramiento electrónico.

Hoy en día, SERVIBOY LTDA se ha consolidado como una empresa líder en Vigilancia Humana y Seguridad electrónica, reconocida por su calidad y cumplimiento en el servicio; pues trabajamos bajo la norma ISO 9001, con el fin de incrementar el número de servicios de seguridad y vigilancia para nuestros clientes, y así mismo, expandir nuestro mercado actual del departamento de Boyacá, a otros territorios circunvecinos como es el caso de Bogotá. [19]

LOGO

El logo de la empresa SERVIBOY LTDA, es la letra S de seguridad y tiene aspecto de una caja fuerte sellada, haciendo alusión al compromiso que la empresa tiene en cuidar, proteger y resguardas tanto a las personas, como a sus viviendas, lugares de trabajo y/o pertenencias, del ataque de terceros.

[19] http://www.serviboyltda.com/index.php/2014-10-01-01-23-24/quienes-somos

2.3. DEPARTAMENTO DE INGENIERIA

Para cumplir con la finalidad de los servicios de vigilancia y seguridad privada, que se concentran en prevenir, detener, disminuir o disuadir los atentados o amenazas que puedan afectar la seguridad de las personas o bienes que se tengan a cargo, además de la vigilancia tradicional, es decir, tener personal supervisando que personas, lugares y/o bienes se encuentren en óptimas condiciones; también se cuenta con una amplia gama de dispositivos que se han desarrollado para la vigilancia y protección de personas y bienes.

FIGURA 21. DISPOSITIVOS EMPLEADOS EN VIGILANCIA ELECTRONICA

FUENTE: http://www.superinventos.com/S111093.htm

Con la creación de SERVIBOY LTDA se buscó atender una necesidad de la comunidad: seguridad. Cuando se concibió la idea de esta entidad boyacense en la industria de la seguridad privada, la vigilancia humana era la manera en la que se daba solución al tema del cuidado y la protección de personas, familias o entidades. Con el tiempo, la labor de los guardas de seguridad se quedaba corta ante las amenazas de los delincuentes, es por esto, que se hace necesaria la implementación de elementos tecnológicos que mejoren la condición de seguridad. Atendiendo a los peligros y las nuevas tendencias en materia tecnológica, la empresa crea el Departamento de Ingeniería que se encarga de la gestión, investigación y manejo; de hardware y software para los servicios de vigilancia apoyados en desarrollos de la electrónica.

Dentro de los servicios de seguridad electrónica, se tienen: sistemas de instalación de alarmas y su respectivo monitoreo, circuitos cerrados de televisión, video- vigilancia, controles de acceso tanto peatonal como vehicular, seguimiento vehicular por GPS, cerramiento eléctrico y, por último, se tiene el personal de apoyo en caso de presentarse una eventualidad en alguno de los lugares donde se presta la vigilancia electrónica, que es el servicio motorizado.

- MONITOREO DE ALARMAS 24 HORAS: El servicio de monitoreo, es la acción y efecto implícito, referente a aquello que se utiliza para llevar el control o supervisión de acciones, a través de un monitor. El Monitoreo en seguridad, se realiza con efectividad no solo a través de un "monitor" que transmite las señales captadas, sino del control que lleva la receptora de señales de los sensores de alarma ubicados estratégicamente en los espacios a cuidar. Además del capital humano entrenado para detectar señales de alarma acuerdo al tipo de dispositivos

instalados, que pueden ser: sensores de movimiento, contactos magnéticos, botones de pánico entre otros.

- CCTV: CIRCUITO CERRADO DE TELEVISION: Las cámaras de seguridad son una solución integral que permite blindar visual y digitalmente diferentes instalaciones. Esta alternativa ofrece la instalación por parte de personal calificado, de cámaras estratégicamente ubicadas en el espacio que se requiera. Incluyen sensores electrónicos con salidas de alarmas; haciendo de este un sistema inteligente con herramientas flexibles y adaptables a diversas necesidades. Actualmente, se encuentran CCTV que ofrecen grabación digital con alta calidad de video, mayor tiempo de grabación, integración con otros dispositivos electrónicos, visualización y configuración con acceso remoto vía internet.

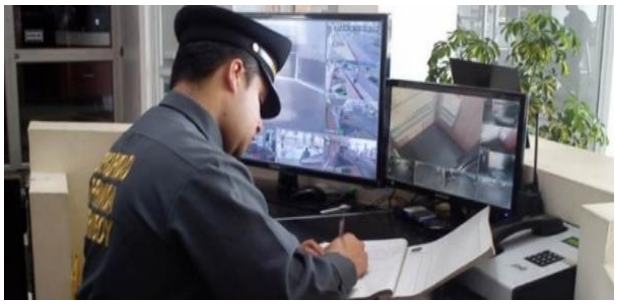


FIGURA 22. PERSONAL VIGILANDO UN CCTV

FUENTE: http://www.serviboyltda.com/index.php/servicios/servicios-seguridad-electronica

- CONTROL DE ACCESO: Está dado como una tecnología al servicio de la seguridad y protección de lugares de residencia, empresas, establecimientos comerciales, financieros e industriales. Este sistema, permite controlar la apertura de puertas, quién las abre, horas de apertura, monitorea y vigila el flujo de personas que entran y salen. Los controles de acceso son una solución ideal para espacios con flujo constante de entrada y salida de personas.

FIGURA 23. CONTROL DE ACCESO

FUENTE: CATALOGO

- SEGUIMIENTO VEHICULAR: Orientado a transporte de carga, pasajeros, maquinaria, vehículos particulares y personas. El Sistema de Seguimiento es un sistema de localización automática que permite conocer una ubicación, sobre nuestro mapa digital en la central de monitoreo. Los

vehículos equipados con un sistema de localización, reciben señales de un satélite del Sistema de Posicionamiento Global (GPS), transmitiéndolas a la central de monitoreo por medio de la red celular o satelital. Así se puede determinar la ubicación exacta y en tiempo real de cada vehículo, conocer las respectivas distancias, calcular tiempos de llegada y tener un control efectivo tanto de vehículos como de conductores.

- VIDEO- VIGILANCIA: Tecnología de vigilancia visual que combina beneficios analógicos de los tradicionales Circuito Cerrado de Televisión con las ventajas digitales de las redes de comunicación IP (Internet Protocol), permitiendo la supervisión local y/o remota de imágenes y audio, así como el tratamiento digital de las imágenes, para aplicaciones de reconocimiento facial o de matrículas.

FIGURA 24. CENTRAL DE VIDEO- VIGILANCIA

FUENTE: http://www.serviboyltda.com/index.php/servicios/servicios-seguridad-electronica

- REACCION MOTORIZADA: Consiste en un grupo de personal altamente capacitado que está preparado para reaccionar ante una señal de alerta, proveniente de cualquier sitio monitoreado. Al instante de recibir la información de la central, se dirigen al lugar e identifican lo que está sucediendo y actuar efectivamente ante dichas señales, ya sea por robo o por intrusión, situación de pánico, sabotaje, incendio o emergencia médica; para comunicarse con el contacto de emergencia y alertar a las unidades de Seguridad Pública o Cuadrante más cercano, Bomberos o Ambulancia, según sea el caso.

2.3.1. COMMAND CENTER

Si en algún momento una persona envía una señal de ayuda y cuenta con la vigilancia privada, surge la pregunta: ¿A dónde llega esa señal de ayuda o de emergencia? Pues efectivamente, tiene que concentrarse en una sola parte la recepción de estas señales.

SERVIBOY LTDA cuenta con un espacio dentro de las instalaciones de la empresa, donde se concentra la información acerca de la seguridad electrónica: se lleva a cabo el seguimiento de las

cámaras y el monitoreo de las alarmas; se hace la recepción de diferentes señales: algunas provenientes de los equipos de seguridad electrónica; y otras señales que envían los usuarios; con el fin de realizar el procedimiento pertinente, dependiendo del tipo de señal o alarma que se reciba. Este lugar se denomina: COMMAND CENTER (CENTRAL DE MONITOREO).

La central de monitoreo es el lugar físico donde se encuentran los recursos humanos y técnicos, necesarios para la recepción y procesamiento de las diferentes señales que generan los sistemas de alarmas instalados en las locaciones de los clientes; y desde donde se coordina la respuesta o reacción a las señales recibidas. Dentro de la central de monitoreo, se cuenta con personal calificado el cual está supervisando dichas señales. En el caso de presentarse una emergencia, el personal observa que no sea una falsa alarma, está al tanto de avisar a las personas encargadas del respectivo sitio para actuar frente a la situación que se esté presentando; y en si es el caso, se avisa a las fuerzas de seguridad para que vayan y actúen en la propiedad vigilada.

Con la instalación de equipos electrónicos de vigilancia y detección, como detectores infrarrojos, detectores de humo, contactos magnéticos en puertas y/o ventanas y otros tipos de detectores, según la necesidad de seguridad del cliente; y todos estos conectados a un panel de alarma con el que se establece comunicación con la central de monitoreo. Los detectores activaran la alarma al momento de detectar la apertura de alguna puerta y/o ventana, un movimiento extraño, una señal de humo o un evento extraño en alguna propiedad. También la alarma se activa en caso de corte de luz, baja batería o cualquier defecto o anomalía, que podría afectar el buen funcionamiento del sistema de alarma.

FIGURA 25. COMMAND CENTER - SERVIBOY LTDA

FUENTE: AUTOR

Cualquier tipo de alarma es recibida en la central de monitoreo para poder reaccionar con los procedimientos de seguridad ya establecidos y dependiendo el caso, se contacta a diferentes dependencias como policía, bomberos o ambulancias. El funcionamiento de la central de monitoreo, es constante: las 24 horas del día, los 365 días del año.

2.3.2. RACK

Para concentrar la actividad de la seguridad electrónica, es necesario estar dotado de los dispositivos que respondan eficazmente, a las exigencias de los servicios prestados. Como primera medida, se tiene el espacio denominado COMMAND CENTER y dentro de dicho espacio, están los elementos para el desarrollo de las operaciones de monitoreo; agrupados en la estructura que hace posible la ubicación, disposición y organización de dichos elementos: un RACK. La empresa dispone de un rack, en el que se tienen los equipos, que permiten la recepción de las señales de alarma, así como también hace posible recibir las señales de video, de los lugares a monitorear.

En el rack se colocan los equipos, y también sirve para mantenerlos seguros, separados de elementos que puedan interferir en su funcionamiento y brindando resistencia a cambios ambientales, para asegurar las condiciones óptimas de rendimiento. Dado que un rack suele estar en funcionamiento mucho más tiempo seguido que un computador particular, una parte esencial del mantenimiento se centra en la refrigeración, para evitar el sobrecalentamiento. Uno de los puntos fundamentales en este sentido es la limpieza del interior del hardware, ya que cuando se junta mucho polvo en los ventiladores, éstos pierden efectividad. Por último, gracias a esta estructura, es posible ordenar muchos dispositivos, facilitando también el acceso a los mismos y dando una buena presentación.

FIGURA 26. RACK - SERVIBOY LTDA

FUENTE: AUTOR

2.3.3. EQUIPOS: COMMAND CENTER Y RACK

Dentro de las labores del Departamento de ingeniería, está el propender por el buen funcionamiento de los equipos electrónicos y así mismo, todo el sistema eléctrico; para el correcto funcionamiento de la empresa, cumpliendo con el día a día de trabajo, de manera rigurosa, pues en la actividad en la empresa es 24 horas. Durante la pasantía, me familiarice con los equipos electrónicos, que se encuentran tanto en el RACK como ubicados por el COMMAND CENTER; atendiendo a las necesidades y la funcionalidad que tengan en la estructura de la organización. Los equipos con los que se cuenta, son:

- PBX Análogo Marca Panasonic. Modelo KX- TEM824
- Teléfonos Marca Panasonic. Modelo PKX- T7730
- Filtro de señales. HWSP 166 ADSL SPLITTER
- Centro de carga Home Line SCHNEIDER ELECTRIC
- Fuente Regulada 10 Amperios Marca MAGOM
- Router Cisco serie 1900. Modelo 1941W
- MODEM Movistar. Marca ASKEY Modelo: Mini BHS
- MODEM Movistar. Marca ZTE Modelo: ZXV 100
- PATCH CORE AMP CONNECTIONS
- Switch Cisco serie 100. Modelo SG100-24
- Router Gigabit Inalámbrico TP Link Modelo N750C
- Receptor Digital Multi Línea SG-DRL2 SG-CPM2
- Receptora Digital de Monitoreo SENTRY PIMA
- Servidor IBM MODELO SYSTEM X3500 M3
- Radio Móvil Marca Motorola Modelo M120
- FIBER OPTICA FRM220 10/ 100i
- Cable marca: NEXXT Cat6
- RADIO LAM 25SHD9 AA2AN
- CAMARAS PARA LA VIGILANCIA INTERNA DE LA EMPRESA
- DVR
- COMPUTADORES
- TELEVISORES
- UPS

2.3.4. DESCRIPCION DE EQUIPOS

La mayoría de los dispositivos anteriormente nombrados, están directamente relacionados con la actividad principal de la empresa: la vigilancia. Sin embargo, algunos de estos equipos están dispuestos para satisfacer necesidades internas de la empresa, es decir, que no están directamente relacionados con la seguridad; sino que se encargan de labores empresariales, como: el PBX, los teléfonos, los filtros de señales, la caja metálica Centro de Carga HOME LINE y las cámaras que se tienen para la vigilancia interna de las instalaciones de la empresa, con su respectivo DVR. Estos equipos apoyan la labor del personal encargado, del monitoreo de los sistemas de seguridad.

2.3.4.1. CENTRO DE CARGA HOME LINE SCHNEIDER ELECTRIC

Este dispositivo consiste en una estructura metálica, que técnicamente corresponde al Panel de distribución eléctrica de SERVIBOY LTDA, donde se tienen las conexiones eléctricas de los equipos de comunicación y demás; es el corazón de la instalación eléctrica, de este salen todos los conductores que alimentan los diferentes circuitos. Este panel de distribución cumple con las funciones de distribuir, controlar y proteger todos los circuitos instalados. Soporta 240 voltios AC máximo y 200 Amper. Tiene 3 fases y 5 hilos.

La distribución se refiere a las conexiones hasta los circuitos independientes: circuito para alimentación del rack, circuito para la iluminación, circuitos para tomacorrientes de uso general, para las oficinas y circuito para las mesas de trabajo de las operadoras de medios tecnológicos. La idea de ejercer control desde esta caja de conexiones eléctricas, está dado por la posibilidad de interrumpir un circuito para un mantenimiento o cualquier verificación, por medio de los breaker o interruptores automáticos, los cuales pueden poner en OFF el circuito específico o toda la instalación. Así mismo, estos dispositivos, junto con fusibles, se encargan de proteger cada circuito de fallas eléctricas que se presenten en la instalación, tales como sobrecarga, cortocircuito o falla a tierra.

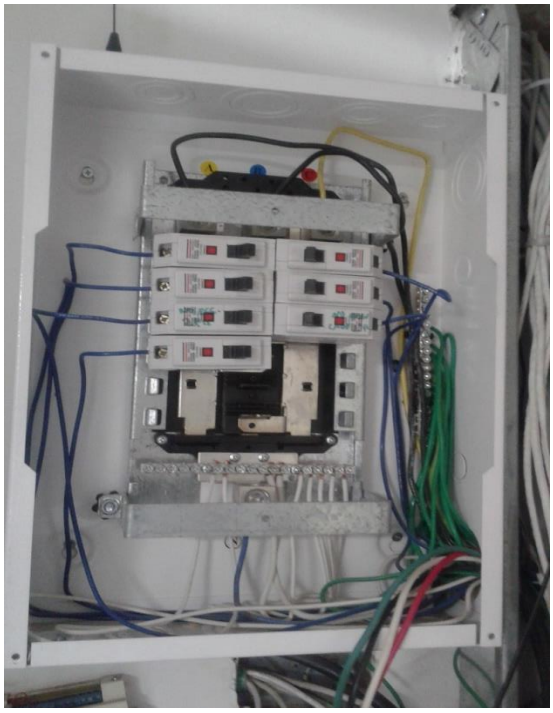


FIGURA 27. CAJA DE CONEXIONES ELECTRICAS

FUENTE: AUTOR

2.3.4.2. PBX ANALOGO PANASONIC KX- TEM824

El PBX es un conmutador privado empresarial, para direccionar las llamadas internas. Con esta PBX se da servicio a los teléfonos corporativos, que pueden ser analógicos, digitales, IP o celulares. De los cuales, se tienen teléfonos análogos y digitales. El PBX con que cuenta la empresa es un equipo

marca PANASONIC modelo KX- TEM824, cuenta con una capacidad básica de 6 líneas externas y 16 extensiones. Es compatible con teléfonos específicos Panasonic y dispositivos como faxes y terminales de datos. Se tienen cuatro líneas y 15 extensiones.

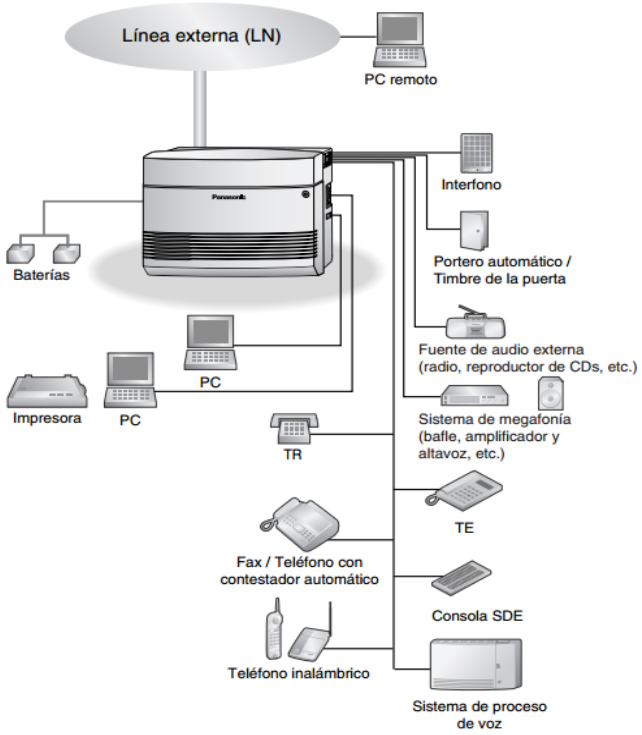


FIGURA 28. ESQUEMA DE CONEXIONES PBX

FUENTE:
http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Conceptos%20de%20Telefonia%20Corporativa.pdf

FIGURA 29. PBX - SERVIBOY LTDA

FUENTE: AUTOR

2.3.4.3. TELEFONOS PANASONIC KX- T7730

SEVIBOY LTDA cuenta con diversos teléfonos PANASONIC compatibles con el PBX que se tiene.

Para establecer señalización digital entre teléfonos y PBX se utiliza un par adicional para esta señalización; disponiendo de un canal digital de datos hacia la PBX, pero el audio se maneja en forma analógica por un par independiente, como se esquematiza en esta figura:

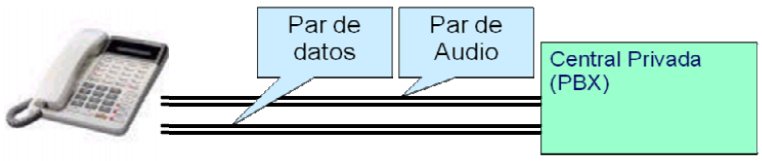


FIGURA 30. TELEFONIA DIGITAL

FUENTE:
http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Conceptos%20de%20Telefonia%20Corporativa.pdf

KX- T7730: Estos teléfonos son HIBRIDOS, transmiten la voz en forma analógica, desde el teléfono a la PBX. La digitalización se realiza en la PBX. Los datos de señalización utilizan un enlace digital independiente. Por ello este tipo de teléfonos requiere de cuatro hilos para funcionar. Disponen de pantallas en las que aparece información enviada por la PBX (por ejemplo, el número y nombre de la persona que llama). También tienen teclas especiales con luces asociadas, las que son encendidas y apagadas por la PBX. Estas teclas especiales indican el estado de otros teléfonos (libres u ocupados), corresponden a facilidades especiales (por ejemplo: transferencia, conferencia, no molestar, etc.) e incluso pueden ser configuradas por el usuario del teléfono.

Los Teléfonos híbridos y digitales, presentan ventajas funcionales respecto a los analógicos. Los datos que se muestran en la pantalla del teléfono, así como el control de las luces de los botones, se señalizan por el par “de datos”, independiente del par “de audio”.

2.3.4.4. TECNOLOGIA ADSL

ADSL significa Línea de abonado digital asimétrica. Este sistema permite la coexistencia de un canal descendente de alta velocidad, de un canal ascendente de velocidad media y de un canal telefónico. Transmitir una señal analógica a través de estos pares de cobre tan solo utiliza una pequeña parte (4khz) del volumen total de información que podría ser transmitido en realidad. En cambio, esta tecnología elimina la transformación de la señal digital a señal analógica, por lo que la información es transferida y recibida de forma digital, utilizando así todo el ancho de banda que el cableado permite realmente.

Al tratarse de una modulación asimétrica, o sea, en la que se transmite diferente cantidad de información, en los sentidos Usuario-Red y Red-Usuario, el módem ADSL del extremo de usuario es distinto del ubicado al otro lado del lazo, en la central local. Además de los módems del usuario

(ATU-R o ADSL TERMINAL UNIT-REMOTE) y de la central (ATU-C o ADSL TERMINAL UNIT-CENTRAL); delante de cada uno de ellos se ha de colocar un dispositivo denominado "splitter" (divisor). [20]

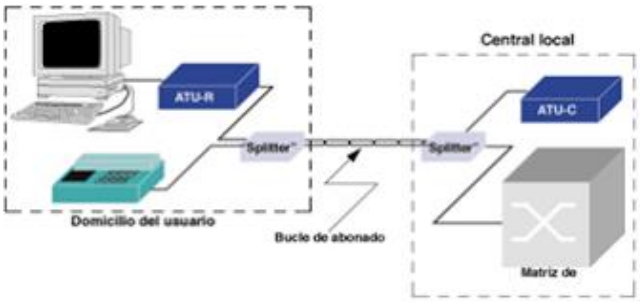


FIGURA 31. ESQUEMA DE CONEXIONES PARA UNA LINEA ADSL

FUENTE: http://www.enterate.unam.mx/Articulos/2005/junio/adsl.htm

2.3.4.5. HWSP 166 ADSL SPLITTER

Este equipo es un dispositivo de HUAWEI. Consiste en un conjunto de dos filtros, que separa la señal de voz, que se encaminarán al teléfono; de la señal de datos, que se enviarán al módem ADSL; para ser transportadas ambas por vía telefónica, sin que se causen interferencias de la una en la otra. Un filtro es de paso alto y otro de paso bajo, para separar las señales de baja frecuencia (telefonía, 300 Hz a 3400 Hz) y las de alta frecuencia (ADSL, 24KHz a 1.100KHz aproximadamente). Este es un equipo diplexor pasivo que, en recepción, tendrá una entrada de línea y dos salidas, en una de las cuales, mediante filtrado se obtendrá la señal telefónica y en la otra el espectro completo presente en la línea (telefonía y banda ancha). En la transmisión se realizará la función inversa.

La señal telefónica está comprendida entre los 0 y los 4 kHz, por lo que el filtro deberá ser capaz de rechazar todas las señales que se encuentren por encima de esta frecuencia, al momento de ser enviadas al teléfono. Un filtro pasa-bajos en la banda de frecuencias desde 0 hasta los 17 kHz, siendo compatible con todos los servicios que utilicen la citada banda, como:

~ Telefonía vocal ~ Servicio de identificación de llamadas.

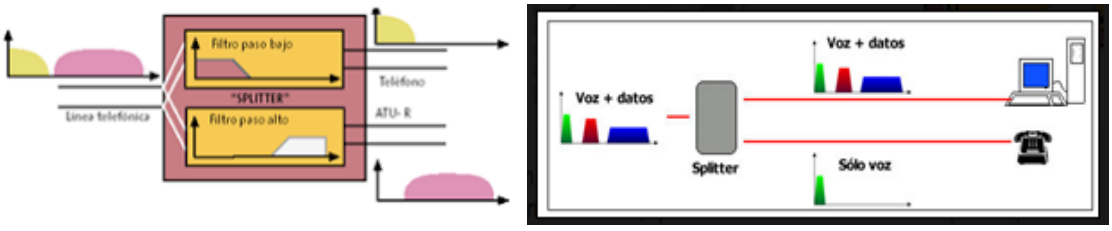


FIGURA 32. FUNCIONAMIENTO DEL SPLITER

FUENTE: http://redesaccesomichelle.blogspot.com.co/2011/04/funcionamiento-de-los-splitters.html

[20] http://www.enterate.unam.mx/Articulos/2005/junio/adsl.htm

CAPITULO 3

3. SISTEMAS DE CAMARAS

3.1. COMPONENTES DE LOS SISTEMAS DE CAMARAS

Para llevar a cabo el trabajo desarrollado con la empresa SERVIBOY LTDA, fue necesario conocer a profundidad los sistemas de vigilancia con cámaras. Detallar los componentes que los conforman, y así, tener claro la manera cómo se comportan dichos sistemas, con el objeto de aplicar este conocimiento en la realización de mantenimiento de equipos e instalación en nuevos proyectos.

Los principales componentes de los Sistemas de vigilancia por Cámaras, pueden agruparse en:

3.1.1. MEDIOS DE ADQUISICIÓN DE LA IMAGEN

La finalidad de las cámaras, es captar señales ópticas y transformarlas en señales eléctricas, enviándolas a los monitores a través de las líneas de transmisión. Sus elementos básicos son:

A) ÓPTICOS: capta la imagen y la enfoca hacia el tubo captador. Está formado por el objetivo (conjunto de lentes convexas y cóncavas) y el diafragma (láminas que regulan las dimensiones del orificio del objetivo). Existen parámetros del sistema óptico, como: distancia focal, apertura o luminosidad, profundidad de campo, tamaño de la imagen y ángulo visual.
B) TUBO CAPTADOR: Transforma la imagen luminosa captada en señal electrónica. Las características que influyen en los tubos, son: tamaño, resolución, sensibilidad, entrelazado...
C) CIRCUITOS DE TRATAMIENTO DE IMAGEN: Reciben la señal eléctrica procedente del tubo y proporcionan los impulsos de sincronismo, transformándola en señal de vídeo transportable.
D) ELEMENTOS AUXILIARES DE LAS CTV: Son accesorios que se pueden incorporar a una cámara, para facilitar su tarea. No son imprescindibles y su empleo está condicionado por la aplicación. Hay una amplia gama de elementos auxiliares: carcasas, soportes, iluminación.

FIGURA 33. CAMARA DE SEGURIDAD- SERVIBOY LTDA

FUENTE: AUTOR

3.1.2. MEDIOS DE TRANSMISIÓN DE LA IMAGEN

Son los empleados para la transmisión de las señales de vídeo desde las cámaras hasta los monitores, receptores de las mismas. Se puede realizar en tiempo real o en diferido y los componentes empleados, son: cable coaxial, par trenzado, red telefónica, fibra óptica, enlace por radiofrecuencia, enlace por microondas, enlace láser.

3.1.3. MEDIOS DE VISUALIZACIÓN: MONITORES

El monitor es un equipo cuya finalidad principal es la de presentar en su pantalla la imagen captada por la cámara, en las mejores condiciones. Para ello necesita recibir la señal de vídeo emitida por la cámara y separar las señales de imagen y sincronismo. La amplificación de la señal de imagen separada produce una iluminación en la pantalla que es proporcional a la señal que recibió. La señal de sincronismo permite el barrido del haz correspondiente a la imagen, en forma vertical y horizontal.

FIGURA 34. MONITOR - SERVIBOY

FUENTE: AUTOR

3.1.4. MEDIOS DE REPRODUCCIÓN: VIDEOGRABADORES

Su función es la de reproducir y almacenar las imágenes captadas, cuando pueda ser conveniente, o necesario, su uso posterior. Ofrecen un amplio campo de aplicaciones en el mundo de la seguridad, por sus numerosas posibilidades de empleo en todas las áreas de la demanda. A las conocidas y tradicionales funciones de manejo del vídeo casero, su unen los avances tecnológicos e informáticos, que permiten la grabación en discos compactos, con el aumento de las horas de imagen, la calidad de reproducción, etc.

FIGURA 35. DVR - SERVIBOY LTDA

FUENTE: AUTOR

3.1.5. MEDIOS DE TRATAMIENTO DE LA IMAGEN

La observación de varias cámaras en uno o varios monitores, según la finalidad que se tenga, pueden ser manuales, secuenciales o automáticos en alarma. Otros medios de tratamiento de la imagen son los elementos de mando, integrados por telemandos y teclados de control y los elementos auxiliares de monitorización, generadores de fecha y hora, identificadores de cámaras, generadores de texto.

3.2. DESARROLLO DEL TRABAJO

3.2.1. CONOCIMIENTO DE LOS TIPOS DE DISPOSITIVOS

Además del estudio realizado sobre la estructura general de sistema de vigilancia con cámaras, fue necesario llevar a cabo una ardua investigación sobre cada uno de ellos, y también de los programas (software) que se emplean. En el caso de una instalación nueva, contando con este conocimiento, se realizan estudios de seguridad y se puede orientar a los clientes sobre lo que se debe implementar y cómo implementarlo dependiendo de las necesidades de cada quien.

3.2.2. VISITAS REALIZADAS A LOS USUARIOS: APLICACIÓN DEL CONOCIMIENTO ADQUIRIDO

Día a día, las operadoras del Command center informan al departamento de ingeniería sobre fallas que se estén presentando en algunas de las unidades monitoreadas. Con esta información, el ingeniero de mantenimiento en compañía del personal técnico, deben dirigirse a diferentes lugares, para atender los requerimientos, a que haya lugar. Por un lado, siendo apoyo para el trabajo que se genera en la empresa en el área de la vigilancia electrónica y posteriormente, dirigiendo y supervisando el desarrollo de estas actividades.

En las visitas técnicas de mantenimiento, realizar diferentes pruebas para detectar aquello que este ocasionando la falla en el sistema: revisión de cableado, comprobación de los niveles de voltaje y corriente, revisión de condiciones del sistema por si ha sido violentado o alterado, entre otros estudios; para luego proceder a dar solución a la problemática según sea el caso.

3.2.3. OBJETIVOS DE LA VIGILANCIA CON SISTEMA DE CAMARAS

- Tener conocimiento en tiempo real de lo que está sucediendo en determinada unidad: residencia o establecimiento; para reaccionar en caso de presentarse alguna eventualidad.
- Contar con una evidencia que se pueda hacer efectiva, si se tiene algún proceso que requiera posterior revisión.

3.3. EVOLUCION DE LA TECNOLOGIA DE SEGURIDAD POR CAMARAS

La primera referencia sobre el Circuito Cerrado de Televisión fue en 1942 y desarrollado por la empresa Siemens AG para el ejército alemán. La finalidad era poder monitorizar el lanzamiento de los misiles V2. También durante los años 40 el ejército americano utilizó este sistema para poder desarrollar y testear las armas atómicas desde un área segura.

FIGURA 36. SISTEMA ANTIGUO DE VIGILANCIA POR VIDEO

FUENTE: http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/

La primera comercialización de este tipo de sistemas fue en 1949 a través de la empresa VERICON, por aquel entonces, al no disponer de sistemas de grabación de imagen, la monitorización se hacía

de forma continuada. Y no fue hasta 1951 que apareció el primer sistema para poder almacenar las imágenes en una cinta de vídeo VTR.

En los años siguientes los sistemas de CCTV ya no solo eran utilizados por las entidades públicas o militares, empresas privadas empezaron a añadir estos sistemas como medidas de seguridad, como en bancos, gasolineras, etc. Nunca se demostró por aquel entonces que estos sistemas pudieran bajar la ratio de criminalidad, pero sí que ayudo bastante a la hora de poder capturar a los delincuentes. Uno de los primeros Gobiernos que utilizó estos sistemas de monitorización para controlar el tráfico y manifestaciones fue el Gobierno Británico, debido al potencial de estos sistemas también empezaron a utilizarlo con otros fines y a instalarlo en más áreas.

Al principio todos estos sistemas eran analógicos y funcionaban a través de un cable coaxial (cobre) con una señal sinusoidal entre + 0,5 y -0,5 voltios, las cámaras enviaban la señal al monitor o a la matriz a través de este cable, que era muy susceptible a interferencias y provocaba que las imágenes no fueran de calidad. La calidad de la imagen se medía en líneas de televisión (LTV) y en vez de grabadores digitales había video-grabadores con cintas de video: VHS o VTR.

Los sistemas analógicos perduraron muchos años, hasta que llegamos al año 1996 donde se desarrolló la primera cámara IP la NETEYE 200 desarrollada por Axis. Desde entonces hasta nuestros días, la transformación de los sistemas de seguridad ha tenido un avance increíble, la intrusión de la informática en estos sistemas ha producido que el salto de analógico a digital fuera más que rápido. Aunque aún en el mercado hay más de un 30% de los sistemas CCTV analógicos, el restante lo reparten el cupo de Sistemas IP y Sistemas Híbridos.

FIGURA 37. FOTO CAMARA IP

FUENTE: AUTOR

Las mejoras aportadas por la informática en estos sistemas han sido increíbles, desde la grabación digital de gran calidad, control de las cámaras a través de la red, el VMD (VIDEO MOTION DETECTION), agilidad a la hora de buscar eventos en las grabaciones, sistemas que interactúan con el entorno o activación de relés, etc.[21]

[21] http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/

3.4. TIPOS DE SISTEMAS DE CAMARAS

La empresa SERVICIOS DE VIGILANCIA DE BOYACA LTDA, cuenta con sistemas de seguridad que constan de componentes de software, hardware, dispositivos y equipo de control, que son controlados desde el COMMAND CENTER. Se tienen cámaras análogas, cámaras HD y cámaras IP.

Dentro de los servicios que presta la empresa, están los sistemas de cámaras, que comprenden: CIRCUITO CERRADO DE TELEVISION y VIDEO- VIGILANCIA. Se hace esta diferenciación, porque no todas las cámaras que están instaladas en las unidades se monitorean desde la central. En algunos casos, el cliente requiere de cámaras y el monitoreo del sistema se realiza en el sitio donde estén instaladas (localmente). En otras ocasiones, es solicitado que solo se instale el servicio, pero sin que se monitoree. Para los casos en los que hay monitoreo, por lo general, los videos que se generan en la parte interna de las unidades, como los pasillos, se tienen como para apoyo a la labor del guarda de seguridad.

En la central de la empresa SERVIBOY S.A., se monitorean aproximadamente 100 cámaras, que abarcan todos los proyectos; estas corresponden a los puntos más vulnerables del conjunto, edificio o centro comercial; que casi siempre se refieren a las porterías, los puntos de accesos tanto peatonales como vehiculares, las zonas correspondientes a los parqueaderos, donde se presente el caso, en los linderos con muros o lotes baldíos, así como rejas y en general, toda la parte que bordea el sitio al cual, se le presta el servicio de vigilancia.

3.4.1. CIRCUITO CERRADO DE TELEVISION

Cuando se habla de los CCTV, se refiere al hecho de instalación de un determinado número de cámaras en el espacio a vigilar. Esto con la intensión de tener un registro visual de lo sucede en el sitio. Registro que queda localmente en el lugar de la instalación, pero no queda en la central.

En la prestación de este servicio, no se incluye el trabajo de análisis, diseño e implementación de equipos de red, ya que la señal de video no se envía hasta la central de monitoreo. La tarea de supervisar las cámaras, les corresponde a los guardas que presten servicio de vigilancia, en dichos sitios o en su defecto, esta responsabilidad recae en el dueño del sitio.

3.4.2. VIDEO- VIGILANCIA

Para que se pueda brindar este servicio, es necesario: lógicamente, tener instaladas una o varias cámaras en determinado lugar, tener un equipo grabador de video, que guarde información captada por las cámaras. Se hace necesario el envío de datos de manera inalámbrica desde un punto: casa, conjunto o centro comercial; hasta la central para la transmisión de las señales de video y así poder monitorear 24 horas el sistema.

3.5. EQUIPOS PARA LA VIGILANCIA CON SISTEMAS DE CAMARAS

Para la implementación de Sistemas de vigilancia por Cámaras, los elementos son:

- CAMARAS
- DVR
- Video BALUN, Cable
- SOFTWARE DE MONITOREO DE CÁMARAS
- Monitores: locales y remotos.

FIGURA 38. ESQUEMA GENERAL DE LA VIGILANCIA BASADA EN CAMARAS

FUENTE: https://plus.google.com/+Serviboyltda/photos

3.5.1. DESCRIPCION DE EQUIPOS PARA VIGILANCIA CON SISTEMAS DE CAMARAS

Anteriormente se habló sobre los componentes de los sistemas de cámaras. En esta parte, se describen detalladamente los equipos presentes en los sistemas de cámaras con los que se trabaja en SERVIBOY S.A., además que se relacionan con el componente que le corresponda.

3.5.1.1. CAMARAS

Son el componente principal de un CCTV. Las cámaras de seguridad son cámaras de video de características profesionales que, además de dar una alta calidad de imagen, son robustas y fiables. Para sus instalaciones, SERVIBOY LTDA dispone de una amplia gama de cámaras con diversas características, según diferentes atribuciones. Pueden ser, según la ubicación: interiores o exteriores; según la calidad de la cámara: análoga, AHD o Digital IP y dentro de estas, se subdividen con otras tantas especificaciones, enfocadas en numerosas aplicaciones. Independientemente de la cámara que se use, estos dispositivos corresponden al medio de adquisición de las imágenes, dentro de la estructura de funcionamiento de los CCTV.

En cámaras análogas la resolución se mide en líneas (TVL), son las más económicas, pero se sacrifica calidad de imagen. La tecnología análoga se está dejando de usar, pues con los años, la industria ha venido trabajando en mejorar la propiedad de los equipos, con lo que se mejora en general este servicio de vigilancia. Un nuevo estándar de imágenes para cámaras y grabadoras de video, es AHD (ANALOGIC HIGH DEFINITION), (720p-1080p). El número indica la cantidad de líneas horizontales de píxeles que forman una imagen, y la letra p significa PROGRESSIVE SCAN. La tecnología AHD brinda calidad de imagen en alta definición. Otro de estos avances, es la tecnología IP, la resolución de las cámaras IP es de HD (HIGH DEFINITION) y se mide en Mega-Pixeles teniendo en cuenta también la velocidad de cuadros por segundos (FPS). El procesamiento avanzado de imágenes, garantiza que cada detalle es reproducido con el máximo realismo, colores vivos y detalles nítidos, asegurando calidad total.

3.5.1.2. DVR

Son los encargados de digitalizar y grabar las imágenes y audios que llegan desde las cámaras de seguridad. Además de la grabación, nos permiten ver en una pantalla los videos captados. Algunos de estos dispositivos de grabación y control, cuentan además con la posibilidad de acceso remoto, es decir que, por ejemplo, se pueden ver las cámaras de seguridad desde una computadora conectada a la red, desde una computadora en otro lugar físico a través de Internet o desde un celular. Unos DVR cuentan con un estándar de comunicación de bus en serie llamado RS485 o EIA-485, este sistema es utilizado para mover cámaras de seguridad (PTZ). Los hay para 4, 8, 16, 32, 64 cámaras. Una de las ventajas de estos equipos, es que pueden ser interconectados con alarmas para dispararla en caso de que la cámara de seguridad detecte a un intruso mediante la detección de movimiento o de forma manual. Internamente poseen un disco duro en el cual se harán las grabaciones de las cámaras.

Igual que el caso de las cámaras, la empresa trabaja con diferentes DVR que se acoplan a las necesidades de cada usuario. El avance tecnológico actual, se ve representado en los DVR TRIBIDOS, que registran y reproducen una calidad de imagen de alta definición, en tiempo real, tienen la característica única tríbrido que acepta cámaras AHD, cámaras análogas e IP, con el mismo equipo, adaptándose fácilmente a cualquier tipo de proyecto CCTV.

Dentro de los componentes de CCTV, el DVR se clasifica en los medios de reproducción de imágenes: video-grabadores.

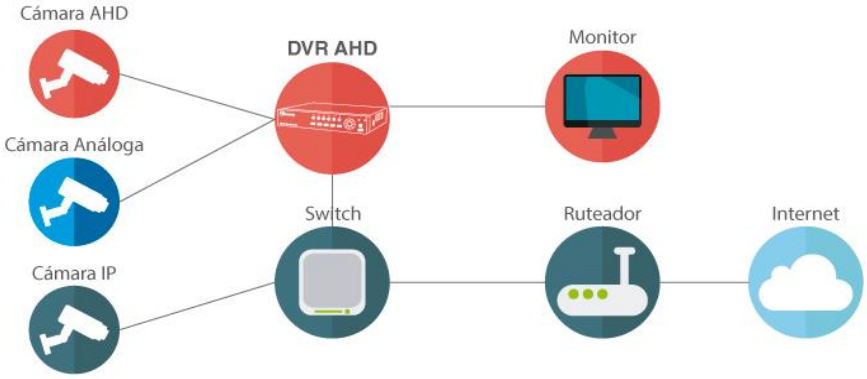


FIGURA 39. DVR

FUENTE: http://www.gsabogal.com/paginaahd/indexahd.html

3.5.1.3. VIDEO BALUN

Un VIDEO BALUN es un transformador que permite conectar dos cosas diferentes con un cable y no comprometer la integridad de la señal. Existen dos clases de VIDEO BALUN: activo y pasivo, la diferencia radica en que el activo necesita ser energizado y el de tipo pasivo, no lo necesita.

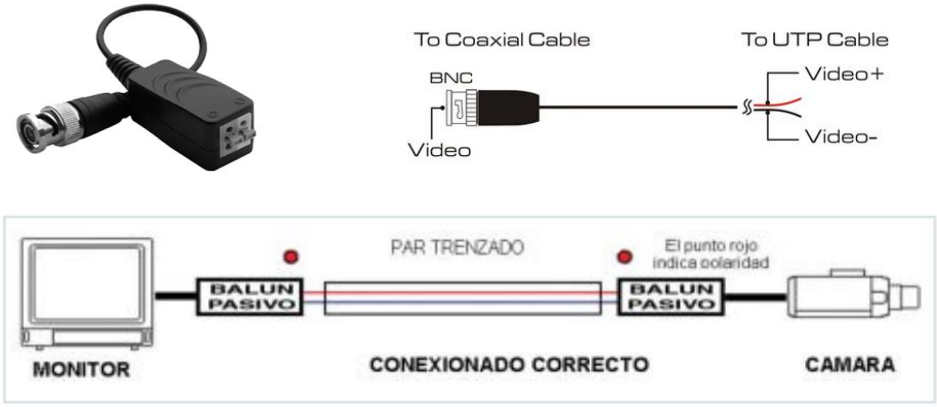


FIGURA 40. VIDEO- BALUN

FUENTE: http://www.rnds.com.ar/articulos/030/RNDS_134W.pdf

3.5.1.4. CABLE NEXXT CATEGORIA 6

La empresa cuenta con conductor NEXXT categoría 6, que es un cable diseñado para la máxima velocidad de transmisión de datos que consta de 4 pares de cable de cobre, calibre 23 AWG. Está elaborado de conformidad con los más altos estándares de transmisión de datos para redes LAN, la categoría 6 de pares trenzados, garantiza las cualidades técnicas que cumplen con todos los estándares internacionales eléctricos y de telecomunicaciones, incluyendo ANSI/ TIA/ EIA-568 C.2, además de ISO/ IEC 11801.

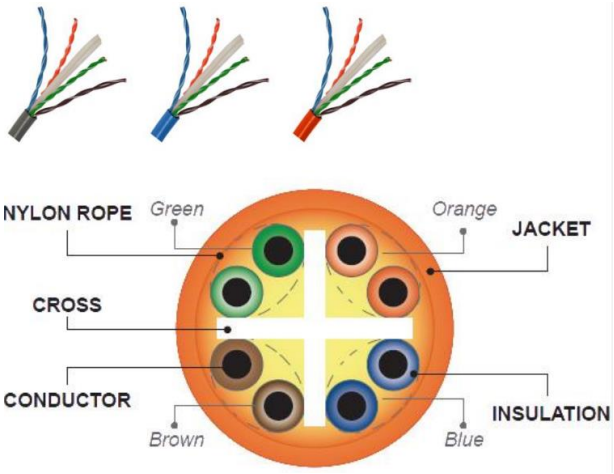


FIGURA 41. CABLE NEXT

FUENTE: HOJA TECNICA CABLE NEXXT CAT 6

Tanto el VIDEO- BALUN como el CABLE, dentro del CCTV, están dados como los medios de transmisión de imágenes. Aunque no son los únicos medios de transmisión con los que cuenta la empresa, si son dispositivos que necesariamente deben estar en cualquier instalación CCTV.

Para los sistemas con cámaras, con los medios de transmisión de la imagen, sucede lo siguiente: cuando solo se necesita enviar video desde las cámaras hasta el DVR, este recorrido se hace de manera cableada y utilizando una pareja de video balun: uno ubicado en medio de la cámara y el cable UTP, y el segundo, en el otro extremo cable, antes del DVR. En el caso de que se realice el monitoreo remoto, desde la central de la empresa, además de instalar necesariamente lo que se describió anteriormente, se instalan otros equipos para la transmisión de la imagen de manera inalámbrica, desde las unidades monitoreadas hasta la central.

3.5.1.5. SOFTWARE DE MONITOREO

Para ver en una pantalla las cámaras de seguridad monitoreadas de los diferentes puntos, SERVIBOY LTDA posee dos versiones de Software para monitoreo de cámaras, en los cuales se puede gestionar cual o cuales cámaras tienen visualización a la vez, ajustar los tamaños de las imágenes, mover las cámaras, configuración y grabación de los videos generados en cada cámara,

permitiendo grabar de manera continua, o realizar las grabaciones en determinados periodos de tiempo: programando horarios de grabación, o por detección de movimiento; configurar la calidad de las imágenes y reproducción de los videos grabados.

Software: SIERA PANTHER 3.0 Para las cámaras de calidad media.
CMS Se maneja este programa para las cámaras de alta calidad.

Estas plataformas de monitoreo tienen la posibilidad de ver diferentes divisiones en la pantalla: una sola cámara, 2x2, 3x3, 4x4, 5x5, 6x6 o 7x7; dependiendo de lo que se quiera observar.

FIGURA 42. SOFTWARE SIERA PANTHER

FUENTE: http://www.sieraelectronics.com/es/component/content/article/602

Uno de los retos más grandes a la hora de monitorear remotamente un establecimiento, es la compresión de los datos, pues el video ocupa una cantidad de espacio considerable, es decir, no es factible el envío de video, sin algún tipo de compresión. Por esto que la empresa adquiere equipos con características de compresión de video, siendo el formato H.264, el utilizado. Los medios de tratamiento de la imagen, son los encargados de las tareas de control y configuración; por lo tanto, en esta clasificación se encuentra el software de monitoreo.

3.6. INSTALACION DE SISTEMAS DE CAMARAS

El procedimiento a seguir para implementar un sistema, independientemente si el nuevo sistema de cámaras se tratara de CCTV o fuera un sistema con monitoreo remoto, se tendrá en cuenta en ambos casos, el siguiente orden:

- ✓ Estudio de seguridad
- ✓ Diseño del Sistema
- ✓ Asesoría al cliente sobre los equipos
- ✓ Determinar el software y hardware que se adecue a las necesidades del cliente.
- ✓ Cierre del acuerdo con el cliente y firma del contrato.

- ✓ Instalación de los equipos.
- ✓ Configuración de equipos.
- ✓ Entrega del sistema en funcionamiento y a satisfacción del cliente.

En las salidas con el PERSONAL TECNICO, no solo se trabajaba en mantenimientos sino también se iba a los lugares en que posiblemente se implementaría algún sistema de seguridad con SERVIBOY, cumpliendo con el procedimiento anteriormente señalado:

- ✓ ESTUDIO DE SEGURIDAD: Cuando la empresa se dispone a adquirir un proyecto, lo primero que se hace es la inspección del lugar. Así se conoce la ubicación y se observa el perímetro, con el fin de determinar los puntos susceptibles de riesgos o daños.
- ✓ DISEÑO DEL SISTEMA: Se le comenta con el cliente las conclusiones del estudio de seguridad y se determina el número y la forma como serán ubicadas las cámaras del servicio de vigilancia. Este diseño depende mucho del cliente, pues la empresa sugiere una distribución y el, es quien finalmente decide los puntos a vigilar, según sus necesidades.
- ✓ ASESORIA AL CLIENTE SOBRE LOS EQUIPOS: Este punto está muy relacionado con el diseño del sistema, pues cuando el cliente comenta cuales son los lugares dentro de la unidad que necesita monitorear constantemente, se les indica el equipo más favorable a sus necesidades.
- ✓ DETERMINAR EL SOFTWARE Y HARDWARE QUE SE ADECUE A LAS NECESIDADES DEL CLIENTE: En esta parte del proceso, se toma un tiempo para realizar la cotización de los equipos que cumplen las especificaciones, para su posterior aprobación por parte del usuario.
- ✓ CIERRE DEL ACUERDO CON EL CLIENTE Y FIRMA DEL CONTRATO: Se aprueba la cotización, se firma contrato, se acuerda forma de pago y fecha de instalación de equipos.
- ✓ INSTALACIÓN Y CONFIGURACIÓN DE EQUIPOS: Dependiendo de la extensión del proyecto, esto puede tomar varios días. Antes de llevar a cabo la instalación como tal, se disponen los equipos a instalar. Lo primero, es realizar un diagnóstico del funcionamiento adecuado de los dispositivos en los laboratorios de la empresa; de estar todo en condiciones óptimas, se dirige el personal técnico al lugar de la instalación, a quienes se les brinda a supervisión y apoyo, por parte del personal de ingenieros. Por último, como líder el proyecto, se realiza la configuración de los equipos instalados, para el funcionamiento del sistema, como: establecer la forma de grabación, programar el recorrido de las cámaras PTZ, alarmas de la cámara, y verificación de la calidad de las imágenes grabadas.
- ✓ ENTREGA DEL SISTEMA EN FUNCIONAMIENTO Y A SATISFACCIÓN DEL CLIENTE: Cuando la instalación y su respectiva configuración es concluida, se le muestra el sistema en funcionamiento al cliente para su visto bueno. Para evidenciar la instalación del nuevo proyecto, se firma un acta de entrega, por parte tanto del ingeniero como del cliente.

3.7. MODIFICACIONES EN LA DOCUMENTACION

3.7.1. IMPLEMENTACION DEL FORMATO PARA REPORTAR MANTENIMIENTOS

Para mejorar los procedimientos los que se realizaban mediante un reporte verbal, se procedió a elaborar formatos en los cuales se consignaba las novedades del servicio en forma escrita. Se creó un documento en Excel, donde se relacionan las unidades, citando cuales requieren mantenimiento o presentan novedades y cuales están en óptimas condiciones.

3.7.2. REALIZACION DE MANUALES

Cada unidad cuenta con un manual, el cual es un documento que consiste en la descripción del sistema de cámaras, según el sitio: número de cámaras y la ubicación de cada una de estas.

PROYECTOS CON LOS QUE ACTUALMENTE CUENTA LA EMPRESA (ABRIL 2016)

NOMBRE	# CAMARAS	MANUAL
❖ Santa Helena	16	LISTO- IMPRESO
❖ Torres de Oriente	4	LISTO- IMPRESO
❖ Concesionario CARRAZOS	8	NO EXISTE- DEBE REALIZARSE
❖ Rincón de la Pradera (HD)	16	PARA MODIFICAR
❖ Edificio Mónaco	13	PARA REVISAR
❖ Constructora BTS	4	LISTO- IMPRESO
❖ Plaza Real	16	NO EXISTE- DEBE REALIZARSE
❖ Institución Educativa INEM	8	NO EXISTE- DEBE REALIZARSE
❖ Conjunto Alameda	16	HECHO- PARA REVISION
❖ INNOVO -Duitama-.	16	LISTO- IMPRESO
❖ Colegio Galileo Galilei	8	NO EXISTE- DEBE REALIZARSE
❖ Quinta Santana	16	LISTO- IMPRESO
❖ Mirador de la Colina	16	PARA REVISAR
❖ Conjunto Acarigua	8	NO EXISTE- DEBE REALIZARSE
❖ Balcones del Bosque	8	NO EXISTE- DEBE REALIZARSE
❖ María Fernanda	16	NO EXISTE- DEBE REALIZARSE

Para la elaboración de los manuales, fue necesario hacer una inspección de cada uno de los lugares de montaje, teniendo cuidado de anotar los detalles ubicación y cubrimiento, que posteriormente fueron consignados en el respectivo manual. Elaboración, con ayuda de las operadoras de los manuales completos: con especificaciones del número de cámaras total, de esas cámaras cuantas se monitorean, datos generales del sitio, labores de la operadora, así como las acciones que toma el guarda, respecto de los avisos, alertas, o llamados que la operadora realice en el desarrollo de sus funciones.

3.8. CAPACITACION

Se llevó a cabo capacitaciones a algunos guardas de seguridad, a cerca del funcionamiento del sistema de cámaras que se encuentra instalado en la unidad.

Las cámaras tipo domos PTZ, permiten un amplio rango de visualización del área monitoreada, gracias a sus propiedades de movimiento y enfoque de las imágenes. En algunas ocasiones, este tipo de cámaras se programan para que tengan un recorrido especifico y repetitivo.

Cuando no se realiza la programación de recorrido en el domo PTZ, la cámara queda vigilando y grabando de manera fija hacia el punto en el que quedo direccionada físicamente. En estos casos, es en los que se capacita al personal de vigilancia humana, para que tenga conocimiento sobre cuales cámaras dentro de la unidad que monitorea, son PTZ y cuál es el manejo que puede dársele, de acuerdo a novedades que puedan presentarse y requieran de las cualidades de movimiento de la cámara y acercamiento, para mejor detección de imagen.

3.9. ATENCION A LAS NECESIDADES DE LOS USUARIOS

Cuando se presenta alguna novedad en las unidades monitoreadas y el cliente considere la revisión de videos, el procedimiento es el siguiente:

- Solicitud por escrito de la descarga y entrega de videos de una fecha y hora dada.
- Proceder a realizar la búsqueda del video con ayuda del software de monitoreo.
- Realizar un informe correspondiente a la información revisada en los videos.
- Reunión con el usuario, para finalizar el tratamiento de la novedad.

CAPITULO 4

4. RED DE TELECOMUNICACIONES

4.1. ESTRUCTURA

Una vez las cámaras son instaladas, se complementa el sistema con parámetros de red para enviar la información que está siendo capturada. SERVIBOY LTDA tiene una estructura con la que se hace posible el envío de señales de video desde las unidades en las que se presta el servicio de video-vigilancia, hasta la Central de monitoreo de la empresa. El almacenamiento y transporte de video, requiere de gran espacio informático, para esto se tienen las soluciones: por un lado, el DVR comprime la información y en cuanto a la red, se trabaja Giga Ethernet. El servidor que posee la empresa, es de alta capacidad para soportar este tráfico de información.

Con base en las características de extensión, SERVIBOY tiene una red WAN –Red de Área Extensa- ya que los puntos a conectar, se encuentran geográficamente distantes. Como las unidades que se monitorean están distribuidas a lo largo de la ciudad de Tunja, es prácticamente imposible tener una red cableada; así que, en cuanto a la manera de transmisión de los datos, se trabaja con redes inalámbricas. Esta estructura es una red privada: se tienen antenas propias.

4.2. REDES INALAMBRICAS

Las redes inalámbricas son aquellas que posibilitan la interconexión de dos o más equipos entre sí sin que intervengan cables, constituyendo un eficaz medio para la transmisión de cualquier tipo de datos. Se basan en enlaces establecidos con ondas electromagnéticas, que viajan a través del espacio llevando información de un lugar a otro, en lugar de cableado estándar. Las redes inalámbricas constituyen la solución para la operación de la video-vigilancia de SERVIBOY.

Desde los años 2000, se ha expandido la tecnología que hace uso de las frecuencias libres de licencia: redes inalámbricas. Utilizan básicamente longitudes de onda correspondientes a las microondas (2,4 GHz y 5 GHz) y permiten tener anchos de banda apreciables (desde 1 MB/s en las primeras versiones hasta llegar a los 54 MB/s de los últimos estándares).

Las redes inalámbricas se diferencian de las convencionales principalmente en la Capa Física y la Capa de Enlace de Datos, según el modelo de referencia OSI. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos, se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, router o compuertas para conectarse. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja. La función principal de las redes inalámbricas, es proporcionar conectividad y acceso a las tradicionales redes cableadas (Ethernet, Token Ring...), como si se tratara de una extensión de éstas.

4.2.1. TOPOLOGIAS

Existen dos modos diferentes de operación para los dispositivos 802.11: Ad Hoc (Juego de Servicios Independientes Básicos- INDEPENDENT BASIC SERVICE SET, IBSS) o Infraestructura (Juego de Servicios Extendidos- EXTENDING SERVICE SET, ESS). No siempre los modos se ven reflejados directamente en la topología. El modo puede ser visto como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de todo un diseño de red.

4.2.1.1. MODO AD HOC:

Es usualmente aquella que existe por un tiempo limitado entre dos o más dispositivos inalámbricos que no están conectados a través de un punto de acceso (Access Point - AP) a una red cableada. Por ejemplo, dos usuarios de laptop que deseen compartir archivos podrían poner una red ad hoc usando NIC compatibles con 802.11 y compartir archivos a través del medio inalámbrico (WM) sin la necesidad de usar medios externos (por ejemplo: discos, tarjetas flash).

FIGURA 43. RED INALAMBRICA EN MODO AD HOC

http://ieeestandards.galeon.com/aficiones1573328.html

4.2.1.2. MODO INFRAESTRUCTURA:

Asume la dirección de uno o más Puntos de Acceso (AP), puenteando el medio inalámbrico al medio cableado. El AP maneja la autentificación de la estación y la asociación con la red inalámbrica. Múltiples AP conectados por un sistema de distribución (DS) puede extender el alcance de la red inalámbrica a un área mucho mayor de la que puede ser cubierta por un solo AP. En instalaciones típicas, el DS es simplemente la infraestructura de la red IP existente. Para propósitos de seguridad, (VLAN) son usadas con frecuencia para segregar el tráfico inalámbrico de otro tráfico en el DS. Aunque 802.11 permite que las estaciones inalámbricas conmuten de forma dinámica la asociación de un punto de acceso a otro (tal sería el caso de un usuario de un PDA

caminando a través de un campus), no gobierna como esto deberá ser logrado. Como resultado de esto, las implementaciones de los diferentes vendedores son incompatibles en este sentido.[22]

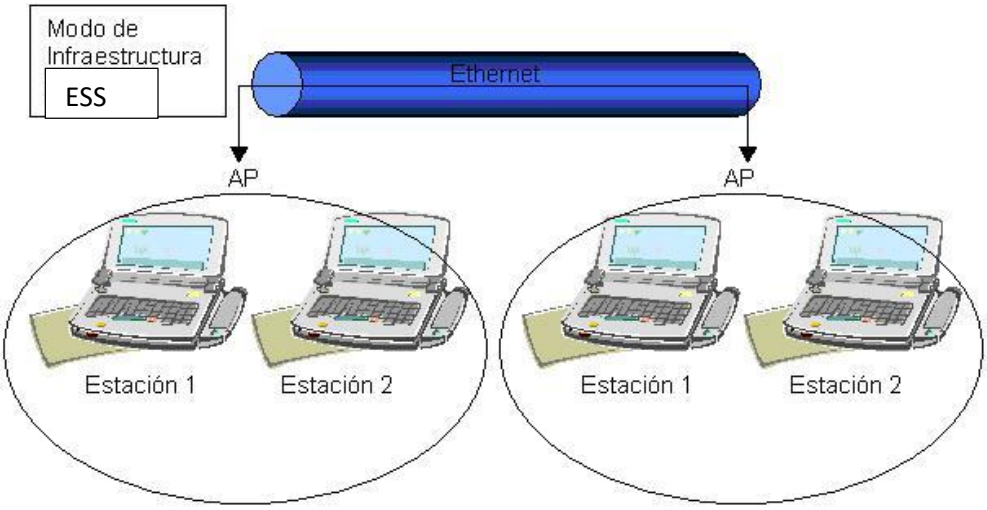


FIGURA 44. RED INALAMBRICA EN MODO INFRAESTRUCTURA

Fuente: http://ieeestandards.galeon.com/aficiones1573328.html

4.3. IEEE 802.11

En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes (Wireless) INALAMBRICAS. El momento decisivo para la consolidación de estos sistemas fue la conclusión del estándar IEEE 802.11 el pasado mes de junio de 1997.

IEEE 802, es una familia de estándares referentes a redes de área local (LAN) y metropolitanas (MAN). Por definición los estándares IEEE 802 se restringen a redes que transportan paquetes de tamaño variable (en contraste con las redes basadas en celdas de tamaño uniforme como ATM "ASYNCHRONOUS TRANSFER MODE").

El protocolo IEEE 802.11 o WI-FI es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas: física y de enlace de datos). Al no estar interconectados físicamente mediante un cable, las redes inalámbricas utilizan ondas de radio para este fin. Esto es posible, en gran parte, a que los organismos internacionales que establecen el reparto de las frecuencias han dejado libres varias franjas para uso personal o privado. Estas frecuencias son usadas, por ejemplo, por teléfonos fijos inalámbricos, walkie-talkies etc. En

[22] http://ieeestandards.galeon.com/aficiones1573328.html

cambio, y en contra de lo que se piensa comúnmente, los radio- aficionados cuentan con unas frecuencias, por las que tienen que abonar unos cánones.

La familia 802.11 actualmente incluye seis técnicas de transmisión por modulación que utilizan todas, los mismos protocolos. El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. El término IEEE 802.11 se utiliza también para referirse a este protocolo al que ahora se conoce como "802.11legacy." La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizó una especificación sobre una frecuencia de 5 GHz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la 802.11b y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporó un estándar a esa velocidad y compatible con la 802.11b que recibiría el nombre de 802.11g. En la actualidad la mayoría de productos son de la especificación 802.11b y de la 802.11g (Actualmente se está desarrollando la 802.11n, que se espera que alcance los 500 Mbps). La seguridad forma parte del protocolo desde el principio y fue mejorada en la revisión 802.11i. Otros estándares de esta familia (c–f, h–j, n) son mejoras de servicio y extensiones o correcciones a especificaciones anteriores. El primer estándar de esta familia que tuvo una amplia aceptación fue el 802.11b. En 2005, la mayoría de los productos que se comercializan siguen el estándar 802.11g con compatibilidad hacia el 802.11b.

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)
Legacy	1997	2.4 -2.5 GHz	1 Mbit/s	2 Mbit/s	?
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~30 meters (~100 feet)
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~30 meters (~100 feet)
802.11n	2008 (projected)	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters (~160 ft)

TABLA 1. ESTANDARES IEEE 802.11

FUENTE: http://ieeestandards.galeon.com/aficiones1573579.html

La banda sin licencia de los 2.4 GHz se volvió últimamente muy ruidosa en áreas urbanas, debido a la alta penetración de las redes Wireless y otros dispositivos que utilizan el mismo rango de frecuencia, tal como hornos de microondas, teléfonos inalámbricos y dispositivos Bluetooth. La banda de los 5 GHz tiene la ventaja de tener menos interferencia, pero presenta otros problemas debido a su naturaleza. Las ondas de alta frecuencia son más sensibles a la absorción que las ondas de baja frecuencia. Las ondas en el rango de los 5 GHz son especialmente sensibles al agua, a los edificios circundantes u otros objetos, debido a la alta absorción en este rango.[23]

[23] http://ieeestandards.galeon.com/aficiones1573579.html

4.4. CARACTERIZACION DE LA RED

La red inalámbrica de transmisión por radio frecuencia, es la utilizada en SERVIBOY. Esta tecnología está definida por una familia de estándares: 802.11 del IEEE. Una red 802.11 está basada en una arquitectura celular donde el sistema está dividido en células, denominadas Conjunto de Servicios Básicos (BSS), y cada una de estas células está controlada por una estación base denominada Punto de Acceso (AP).

Aunque una red wireless puede estar formada por una única célula (incluso sin utilizar un punto de acceso), normalmente se utilizan varias células, donde los puntos de accesos estarán conectados a través de un Sistema de Distribución, generalmente Ethernet y en algunos casos sin usar cables. La red wireless completa, incluyendo las diferentes células, sus puntos de acceso y el sistema de distribución, puede verse en las capas superiores del modelo OSI como una red clásica, y es denominada en el estándar, como Conjunto Extendido de Servicios (ESS).

FIGURA 45. RED INALAMBRICA QUE INTEGRA LOS DOS MODOS: AD HOC E INFRESTUCTURA

FUENTE: http://ieeestandards.galeon.com/aficiones1573328.html

4.5. SISTEMA DE COMUNICACIONES DE LA EMPRESA

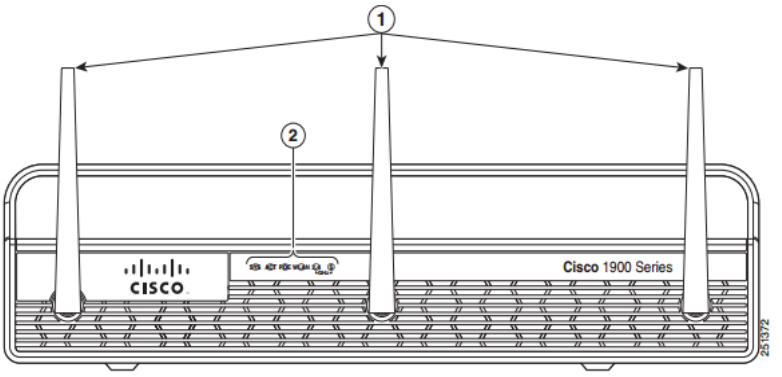
Los equipos que conforman el sistema de comunicaciones de la empresa SERVIBOY LTDA, son:

- ROUTER MARCA CISCO
- PATCH PANEL MARCA AMP NETCONNECT
- ROUTER INALAMBRICO MARCA TP- LINK
- CZ4530-000 FOWB-T MARCA TE CONNECTIVITY
- MODEM MARCA HUAWEI
- ANTENAS MARCA UBIQUITI

4.5.1. ROUTER CISCO

La empresa cuenta con un router Cisco de la serie 1900. El modelo de dicho router es el 1941W. La serie de Router de Servicios Integrados de Cisco 1900, tienen conexiones de LAN y WAN, que se pueden configurar a través de tarjetas de interfaz intercambiables y módulos internos de servicio. El 1941W es un router WI-FI CERTIFIED y compatible con 802.11 a/ b/ g/ n. El diseño modular de los router proporciona flexibilidad, lo que permite configurar el router dependiendo las necesidades. Esta serie tiene nuevas ranuras que apoyan WAN de alta velocidad, tarjetas de próxima generación de interfaz mejorada, módulos de servicios internos y 2 tarjetas Compact Flash (solamente el MODELO 1941). Los puertos universal serial bus están disponibles para dispositivos USB y una consola serial de puerto mini USB tipo B, además del conector de la consola RJ-45.

En esta imagen, se observa el esquema de esta serie de router. El que se tiene en la empresa no es la versión general, sino el router 1941W, que es una mejora del anterior, es inalámbrico y viene sin antenas. Este router provee de internet a la empresa, en cuanto a la red cableada



1	Antenna mounts[1]	2	LEDs[2]

FIGURA 46. ROUTER CISCO DE LA SERIE 1900

FUENTE: DATASHEET ROUTER CISCO 1900

4.5.2. PATCH PANEL - PANEL DE CONEXIONES

Este dispositivo de la marca AMP NETCONNECT, está localizado en el Rack del Command Center de la empresa. El PATCH PANEL cuenta en su parte frontal con un número de 48 conectores RJ45 y en la parte trasera diversas conexiones para acoplar cables de red UTP procedentes de los conectores de pared Jack RJ45. En este equipo, se concentran señales de voz y datos.

Este equipo se encarga de recibir la señal del router y enviarla a todos los puntos de red cableados de la empresa, que corresponden a las oficinas de los diferentes empleados y a las mesas de trabajo de las operadoras de medios tecnológicos en el Command center.

FIGURA 47. PANEL DE CONEXIONES AMP NETCONNECT

FUENTE: AUTOR

4.5.3. ROUTER INALAMBRICO TP- LINK N750

Este dispositivo, es un router de banda dual; se llama así porque efectivamente viene con dos bandas de transmisión: maneja una banda de 2.4 GHz y otra de 5GHz, esto le brinda una alta productividad al equipo, ya que, recibe y transmite por las dos bandas de manera simultánea, permitiendo tener una banda ancha total, como si se tuviera dos router en uno.

La idea de funcionamiento con este elemento, es que mientras se usa la banda de 2.4GHz en aplicaciones básicas como correo electrónico también se pueda ejecutar tareas más robustas como la transmisión de video de alta velocidad utilizando la banda de 5GHz.

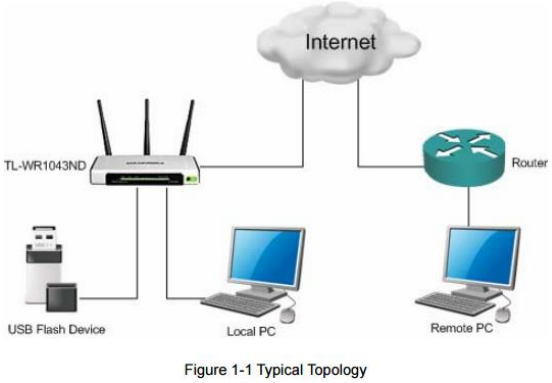


Figure 1-1 Typical Topology

FIGURA 48. TOPOLOGIA TIPICA

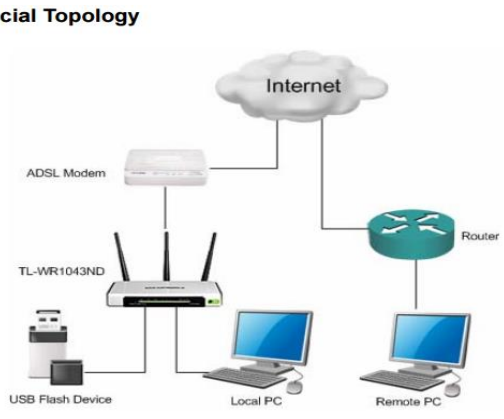


FIGURA 49. TOPOLOGIA ESPECIAL

FUENTE: APPLICATION GUIDE TP- LINK

4.5.4. CAJA CZ4530-000 FOWB-T

Es una caja terminal óptica de exteriores para 8 fibras.

El servicio de internet con el que cuenta la empresa es de alta velocidad y por eso, el proveedor de servicios hace que este llegue con una conexión de fibra óptica, la cual es recibida en la empresa a través de este equipo.

FIGURA 50. CAJA DE CONEXIÓN DE FIBRA OPTICA

FUENTE: http://pdf.directindustry.com/pdf/te-connectivity-fiber-optics/fiber-optic-product/26736-184396.html

4.5.5. MODEM MARCA HUAWEI

La empresa cuenta con dos conexiones de internet, una trabaja únicamente la parte de la red cableada que está dispuesta principalmente para los puestos de trabajo de las operadoras de los servicios de seguridad electrónica y otra red para los servicios generales.

FIGURA 51. MODEM MARCA HUAWEI

FUENTE: AUTOR

Este modem se encuentra ubicado en el rack y está asociado a una de las líneas de internet contratadas por la empresa. No hace parte de los equipos de la red cableada, sino que tiene la función de conectar equipos finales inalámbricamente, de manera local. Se encarga de dotar de

wifi a los equipos que lleguen a la empresa y requiera el uso de internet: pc portátiles, celulares, tabletas o similares.

4.5.6. ANTENAS

SERVIBOY utiliza equipos de la marca UBIQUITI (NANOBRIDGE- NANOSTATION- MICROTIK) que actualmente es la que mejor está posicionada en el mercado, en cuando a soluciones wifi.

Las antenas, son los equipos encargados de la extensión de la red de SERVIBOY. Cuando se realizó el análisis de los diferentes componentes que se tienen a la hora de implementar la vigilancia con sistemas de cámaras, se hizo la descripción de los medios de transmisión de la imagen. En primer lugar, las cámaras van conectadas a un DVR, esto se hace por medio de un par de VIDEO BALUN y con Cable UTP categoría 6; con esto, se obtiene visualización local de las cámaras instaladas. Realizada esta conexión, se lleva a cabo la configuración e implementación de las antenas, para tener ahora el monitoreo remoto de las cámaras.

FIGURA 52. ANTENA NANOBEAM

FUENTE: CATALOGO PRODUCTOS UBIQUITI

Para la vigilancia remota, la mayoría de los DVR con los que se trabaja en SERVIBOY, cuentan con un puerto LAN para conexiones de red, como se observa en la siguiente imagen, donde se relaciona: 1) Línea de tierra; 2) Conector audio/video; 3) Interface VGA; 4) interface RJ45, 5) 2 puertos USB, 6) led indicador de encendido, 7) interface RS 485 y 8) Switch para encender el equipo.

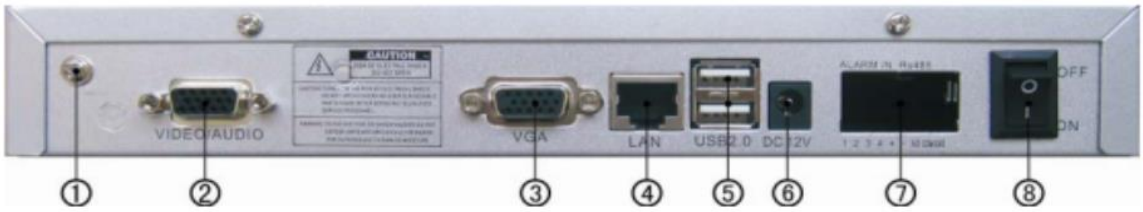


FIGURA 53. CONEXIONES DVR- SERVIBOY

FUENTE: DATASHEET DVR SDR 1004

Para más claridad se elaboró la tabla RELACION DE ANTENAS DE SERVIBOY, donde se especifica el equipo instalado y características básicas de operación del equipo.

RELACION DE LAS ANTENAS DE SERVIBOY			
EQUIPO	**ESTACION**	FRECUENCIA	ESTANDAR
Nano Bridge M5	COMMAND CENTER	5 GHz	802.11a
Nano Station M5	COMMAND CENTER BTS	5 GHz	802.11a
Nano Station M5	TORRES DE ORIENTE	5 GHz	802.11a
Nano Station M5	QUINTA SANTANA TORRE 3	5 GHz	802.11a
Nano Station M5	QUINTA SANTANA TORRE 2	5 GHz	802.11a
Nano Station M5	BTS POSTES	5 GHz	802.11a
Nano Station M5	RINCON DE LA PRADERA	5 GHz	802.11a
Nano Station M5	BTS SALTO	5 GHz	802.11a
Nano Station M5	BTS OFICINAS	5 GHz	802.11a
NanoBeamM5 16	MONACO_ALAMEDA	5 GHz	a/n mixed
NanoBeamM5 16	ALAMEDA	5 GHz	a/n mixed
Nano Bridge M900	PLAZA REAL	900 MHz	802.11n
Nano Station LocoM900	MARIA FERNANDA	900 MHz	AIRMAX
Nano Bridge M900	MIRADOR DE LA COLINA	900 MHz	802.11n
Nano Station LocoM900	SANTA HELENA	900 MHz	AIRMAX
MikroTik Sextant 5HnD	MONACO CLIENTE	5 GHz	802.11n
MikroTik Sextant 5HnD	MONACO CENTRAL	5 GHz	802.11n
Nano Station M5	ACARIGUA	5 GHz	802.11ª
NanoBeamM5 16	INEM PRINCIPAL	5 GHz	a/n mixed
NanoBeamM5 16	PLAZA REAL SUR	5 GHz	a/n mixed
Nano Bridge M5	BALCONES	5 GHz	802.11a

TABLA 2. RELACION DE LAS ANTENAS DE SERVIBOY

FUENTE: AUTOR

4.6. FORMAS EN QUE SERVIBOY ESTABLECE LA COMUNICACIÓN

4.6.1. ENLACES PUNTO A PUNTO

Este tipo de enlace es empleado, cuando se necesitan comunicar dos puntos específicamente. Es ampliamente usado por la empresa. Las unidades que se encuentran cercanas a la empresa, y además cuentan con línea de vista, están configuradas para establecer una comunicación punto a punto.

FIGURA 54. ENLACE PUNTO A PUNTO

FUENTE: https://www.telcoantennas.com.au/site/ubiquiti-nanobridge-m-point-point-wifi-bridge

4.6.2. ENLACES PUNTO A MULTIPUNTO

Cuando es necesario establecer comunicación entre varias unidades con un punto central, se utilizan los enlaces punto a multipunto. Las dos formas de comunicación son utilizadas por la empresa, ya que se tienen diferentes necesidades en los puntos a monitorear.

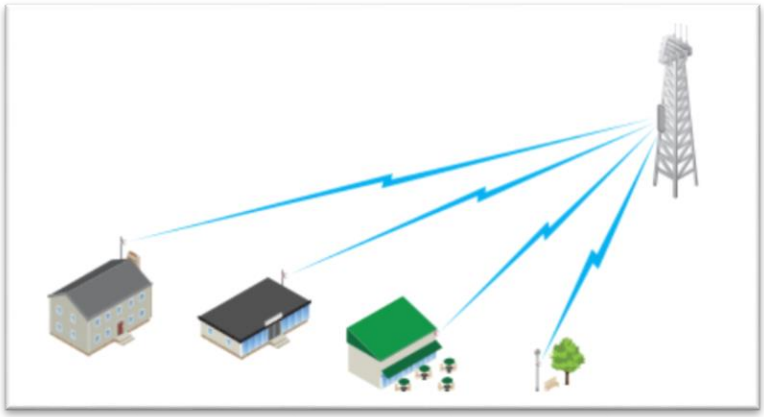


FIGURA 55. ENLACE PUNTO A MULTIPUNTO

FUENTE: DATASHEET NANOBRIDGE M5

4.6.3. PROTOCOLO DE TÚNELES PUNTO A PUNTO

Protocolo que permite a las empresas extender su propia red corporativa a través de túneles privados en la red pública Internet. De esta forma, una empresa puede usar de forma efectiva una WAN (red de área extensa) como una gran LAN (Local Área Network, red de área local) única. Este tipo de interconexión se denomina red privada virtual (VPN).

VPN (VIRTUAL PRIVATE NETWORK, RED PRIVADA VIRTUAL): Crea un túnel seguro entre los puntos de la VPN. Únicamente los dispositivos con la clave correcta serán capaces de funcionar dentro de la VPN. Una red VPN puede encontrarse dentro de una LAN (Local Área Network, Red de área local) de una empresa, pero también pueden conectarse distintas ubicaciones a través de Internet de forma segura. Un uso habitual de las VPN es la conexión de un ordenador remoto a la red corporativa, por ejemplo, a través de una línea telefónica directa o a través de Internet.[24]

FIGURA 56. ESQUEMA DEL ENVIO DE SEÑAL AL COMMAND CENTER

FUENTE: https://plus.google.com/+Serviboyltda/photos

En la empresa SERVIBOY LTDA, se realiza la configuración de equipos, de manera que la red WAN se comporta como una LAN extendida y se hace autenticación por medio de claves, con el fin garantizar que solo exista conexión entre los equipos requeridos, comportándose como una VPN.

[24] http://www.axis.com/cl/es/glossary/network-video

4.7. MODELAMIENTO DE LA RED

Para llevar a cabo el modelamiento de la red de la empresa SERVIBOY LTDA, fue necesario programar un plan de acciones, con el fin de tener un procedimiento ordenado de los elementos que se deben tener en cuenta, en el desarrollo de esta actividad.

- Ubicación en GOOGLE MAPS, de los lugares monitoreados
- Ayuda con el programa RADIO MOBILE, para los enlaces
- Estudio concienzudo de los datasheet de las antenas.
- Inspección de la configuración de las antenas, para recopilar datos
- Creación de tablas con la información revisada.
- Diseñar la red, en un software de modelamiento de redes de comunicaciones.

4.7.1. UBICACIÓN DE LOS LUGARES MONITOREADOS

Gracias a la realización de los manuales de cada unidad monitoreada, se pudo contar con la información de cada uno de estos sitios. Uno de los datos es la dirección, con la dirección y la ayuda de GOOGLE MAPS, se pudo establecer la ubicación exacta de todos los lugares vigilados.

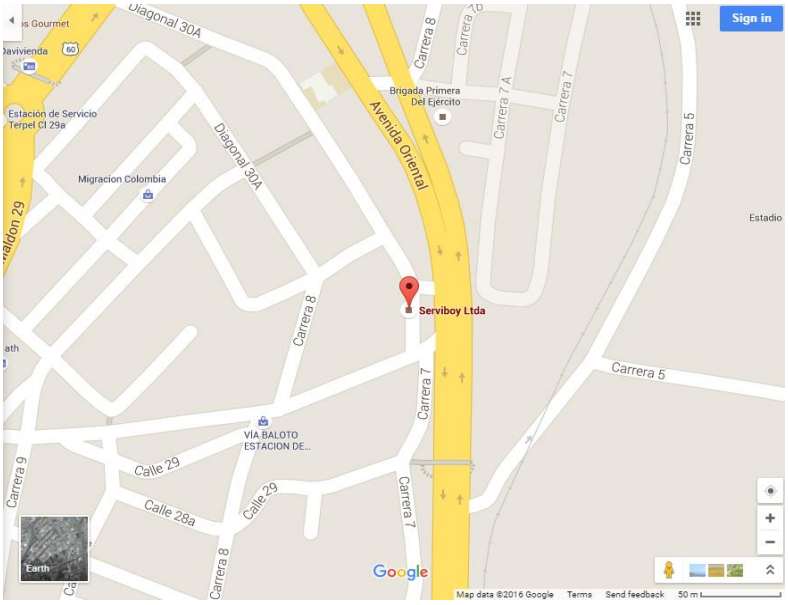


FIGURA 57. UBICACIÓN DE SERVIBOY LTDA EN GOOGLE MAPS

FUENTE: AUTOR

4.7.2. INFORMACION DE LA RED DE LA EMPRESA SERVIBOY LTDA

Para poder visualizar y evaluar el estado de los enlaces, se usó el software RADIO MOBILE. Este programa necesita que se especifiquen puntos dentro del mapa del lugar que se va a estudiar, información con la que no se contaba de manera estructurada.

Por eso fue necesaria la creación de archivos, para documentar la información de manera que cuando se necesite, no se presenten contratiempos. Lo primero que se llevó a cabo, fue recopilar y organizar datos sobre los equipos que componen la red, ubicar la dirección correspondiente y con ayuda de GOOGLE MAPS, se obtuvo las coordenadas de los diferentes lugares.

UBICACIÓN ANTENAS SERVIBOY LTDA		
NOMBRE DE LA ESTACION	DIRECCION	COORDENADAS
COMMAND CENTER	CRA 7ª # 28-27	5.5416173,-73.3569464
COMMAND CENTER BTS	CRA 7ª # 28-27	5.541633, -73.356632
TORRES DE ORIENTE	CRA 4ª N° 35-66	5.545589, -73.353910
QUINTA SANTANA TORRE 3	CRA 2ª N° 32- 49	5.5439039,-73.353403
QUINTA SANTANA TORRE 2	CRA 2ª N° 32- 49	5.543955, -73.353537
BTS POSTES	VIA TOCA. KM 1.5	5.5327873,-73.3442325
RINCON DE LA PRADERA	CRA 4ª N° 35-73	5.545748, -73.353990
BTS SALTO	VIA TOCA. KM 1.5	5.5327873,-73.3442325
BTS OFICINAS	VIA TOCA. KM 2	5.533456, -73.343797
MONACO_ALAMEDA	CALLE 28 N° 8- 28	5.5399724,-73.3580169
ALAMEDA	CALLE 36 N° 8- 66	5.5488904,-73.357431
PLAZA REAL	CALLE 20 N° 12-84	5.534796, -73.364791
MARIA FERNANDA	CALLE 45 N°4-79	5.5523336,-73.3504978
MIRADOR DE LA COLINA	AV.UNIVTARIA N°41-50	5.5469236,-73.3472152
SANTA HELENA	CALLE 59 N° 2E- 58	5.560293, -73.337263
MONACO CLIENTE	CALLE 28 N° 8- 28	5.540536, -73.357797
MONACO CENTRAL	CRA 7ª # 28-27	5.541641, -73.356662
ACARIGUA	CRA 3ª N° 32-25	5.5440143,-73.3542903
INEM PRINCIPAL	CRA 15 N° 9- 72	5.5254398,-73.3697274
PLAZA REAL SUR	CALLE 20 N° 12-84	5.5349297,-73.3657138
BALCONES DEL BOSQUE	CALLE 12 N° 10- 84	5.525180, -73.362943

TABLA 3. UBICACIÓN DE LAS ANTENAS DE SERVIBOY LTDA

FUENTE: AUTOR

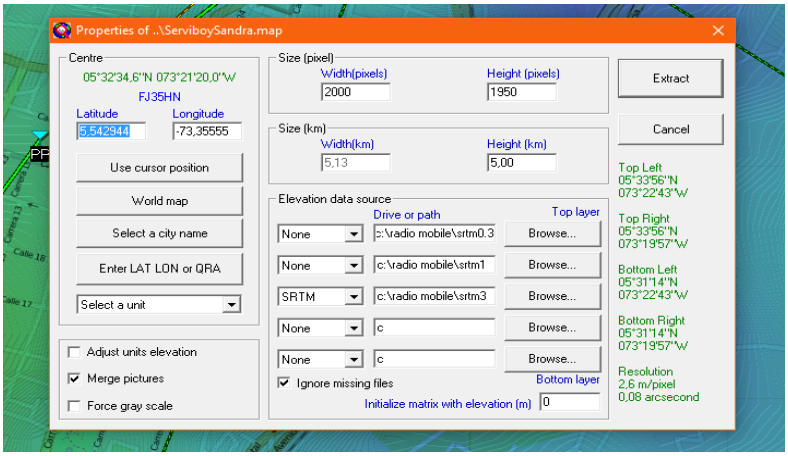


FIGURA 58. SOFTWARE RADIO MOBILE: PROPIEDADES DEL MAPA

FUENTE: AUTOR

Una vez se tienen los datos de ubicación, se pasa al programa RADIO MOBILE para configurar como primera medida, las propiedades del mapa que es objeto de estudio, situando la coordenada 5,542944 y -73,35555, que es un punto ubicado en la ciudad de Tunja y será el centro del mapa.

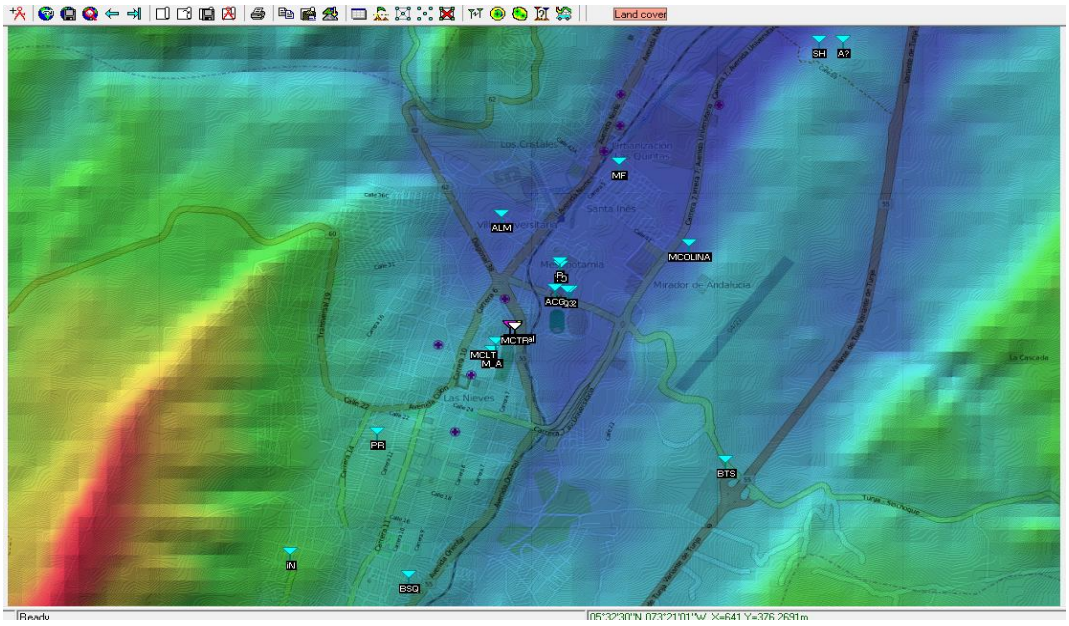


FIGURA 59. MAPA DE TUNJA CON LA UBICACIÓN DE LAS ANTENAS DE SERVIBOY LTDA

FUENTE: AUTOR

En la figura 59, los puntos señalados con triangulo azul corresponden a las antenas instaladas.

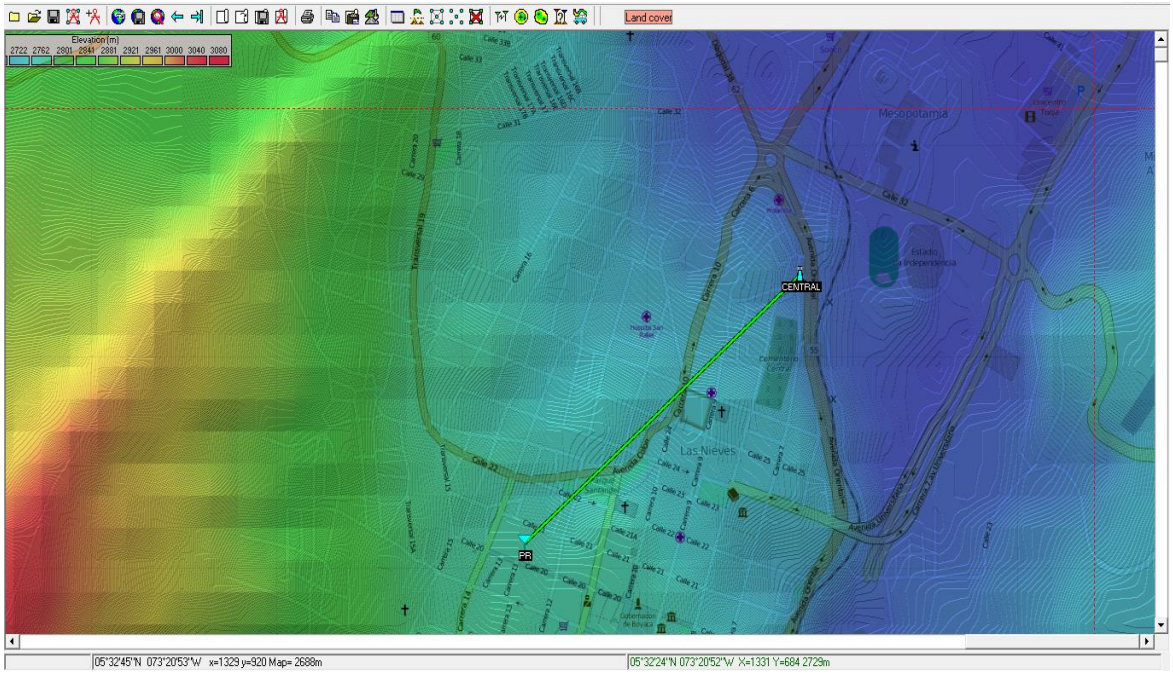


FIGURA 60. MAPA DE TUNJA EN EL PROGRAMA RADIO MOBILE

FUENTE: AUTOR

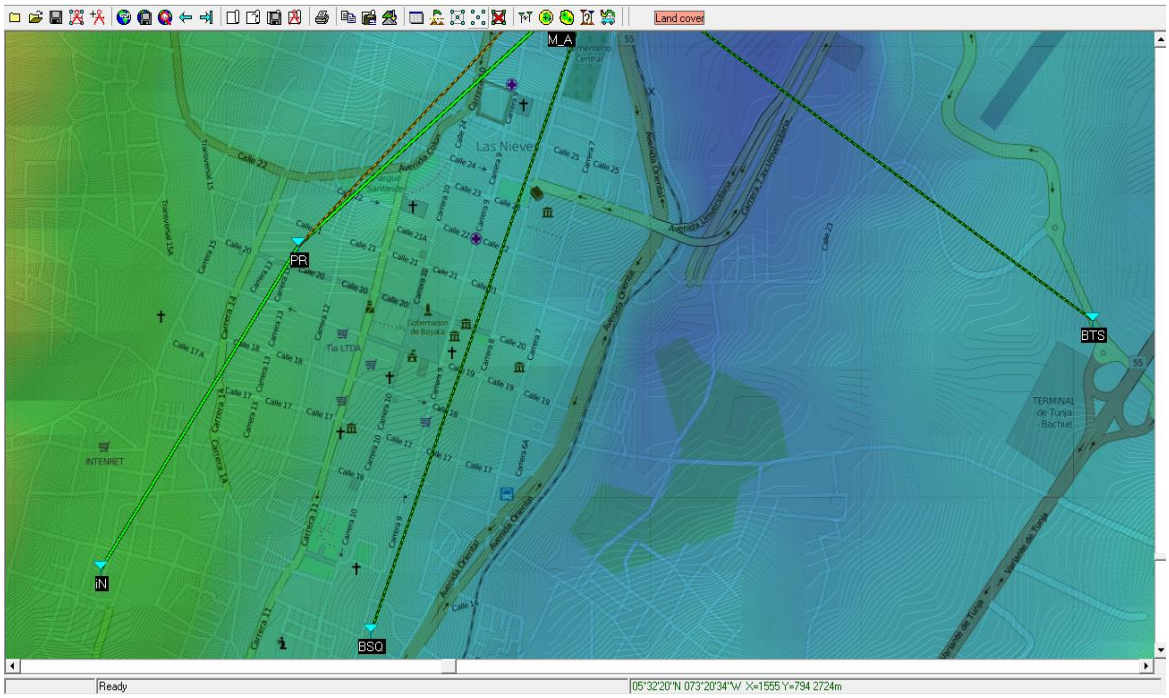


FIGURA 61. MAPA DE TUNJA EN EL PROGRAMA RADIO MOBILE

FUENTE: AUTOR

Dado que los puntos a ubicar están distribuidos a lo largo y ancho de Tunja, es muy difícil concentrar todo el mapa en una sola imagen, sin que se superpongan algunas unidades, por la cercanía existente entre ellas. Las figuras 60 y 61, permiten visualizar diferentes puntos. En la figura 60 se tiene el noroccidente de la ciudad y en la figura 61, se observa el sur de Tunja.

Para continuar con el trabajo en el software RADIO MOBILE, es necesario tener los datos de operación de los equipos. Se elaboró esta tabla con información recopilada de las hojas técnicas correspondientes.

INFORMACION ANTENAS		
NANOBRIDGE M5	22 dBi	5180- 5805
NANOSTATION M5	16 dBi	5170- 5875
NANOBRIDGE M900	11 dBi	902- 928
NSTATION LOCOM9	8 dBi	902- 928
MikroTik Sextant 5HnD	17 dBi	5180- 5805
NANOBEAM M5	19 dBi	5150- 5875

TABLA 4. DATOS ANTENAS USADAS EN SERVIBOY LTDA

FUENTE: AUTOR

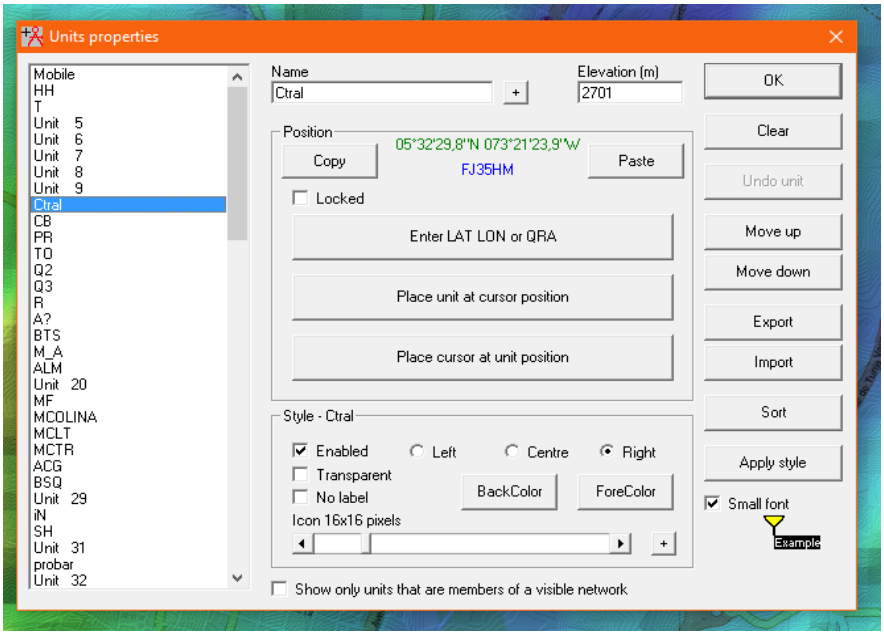


FIGURA 62. SOFTWARE RADIO MOBILE: PROPIEDADES DE LAS UNIDADES

FUENTE: AUTOR

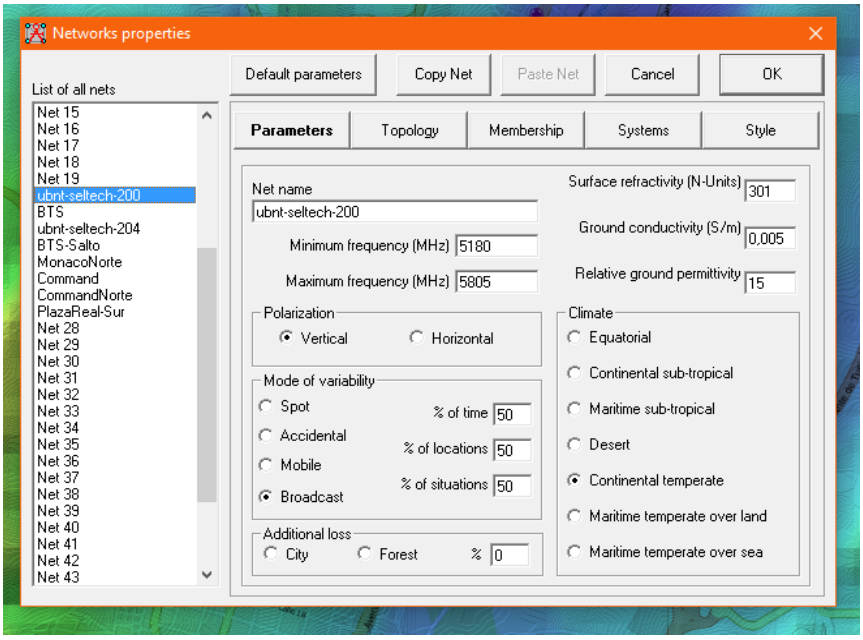


FIGURA 63. SOFTWARE RADIO MOBILE: PROPIEDADES DE LAS REDES

FUENTE: AUTOR

En las figuras 62 y 63, se puede observar que en el programa RADIO MOBILE se configuran todos los datos necesarios: En propiedades de las unidades, nombre y ubicación de estas; y en propiedades de las redes, se detalla nombre de las redes, frecuencia de operación, potencia de transmisión y la ganancia del dispositivo.

Una vez son ingresados todos los datos de configuración en el programa, se procede a realizar el análisis de cada uno de los enlaces.

4.7.3. SOFTWARE

La empresa UBIQUITI, que elabora y distribuye equipos de tecnología para comunicaciones inalámbricas, proporciona una plataforma de configuración propia de la marca, llamado AIR OS.

En esta plataforma se puede observar que configuración tiene cada una de las antenas, se revisó la información de los cada uno de los equipos y se consignaron los datos.

FIGURA 64. INTERFACE DEL SOFTWATE AIR OS

FUENTE: AUTOR

4.7.4. ESQUEMAS DE RED

Para llevar a cabo el modelamiento de la red, se pensó utilizar el programa CISCO PACKET TRACER, en las figuras 65 y 66, se tiene el mapa de red; pero no todos los equipos en la simulación, corresponden a los equipos instalados.

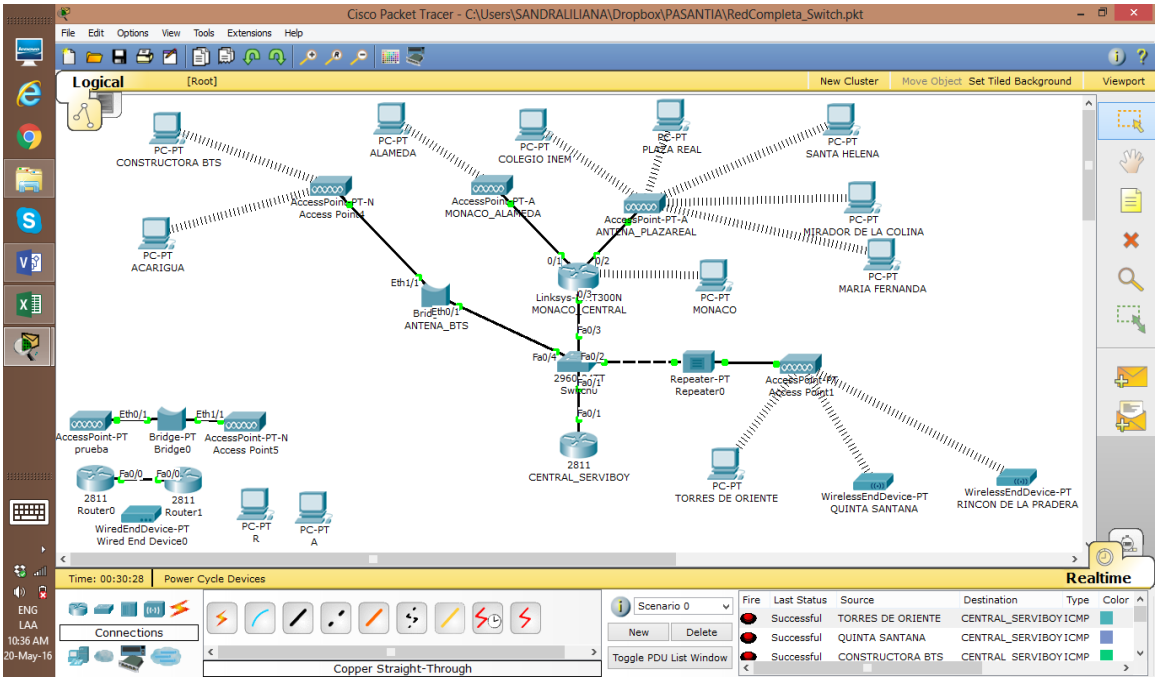


FIGURA 65. MAPA DE RED EN EL PROGRAMA CISCO PACKET TRACER

FUENTE: AUTOR

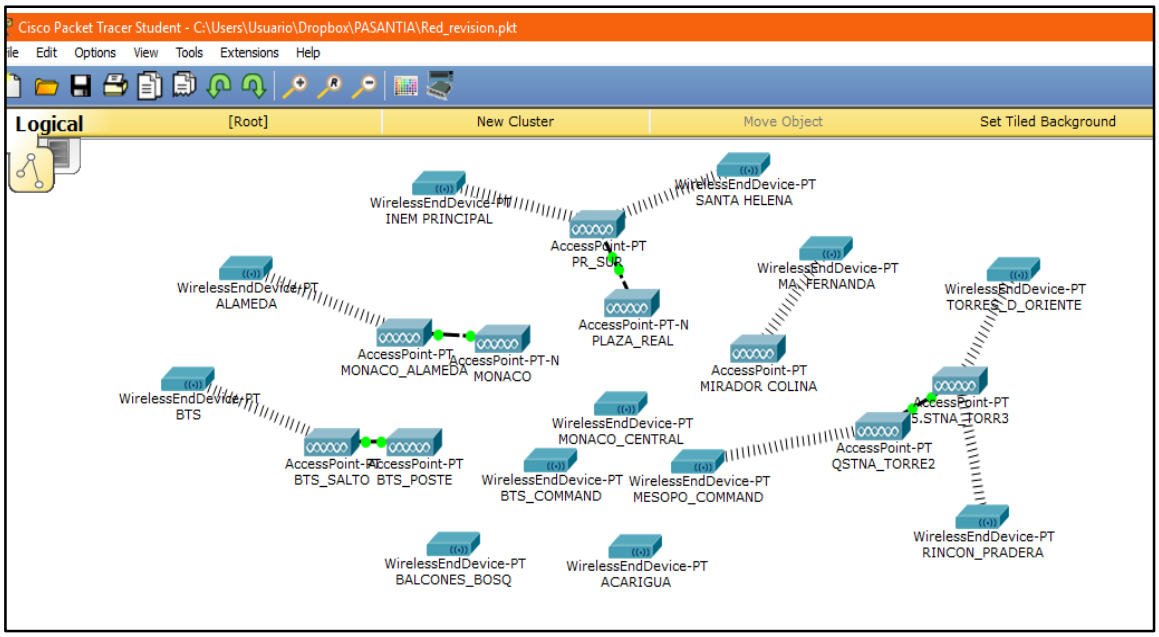


FIGURA 66. MAPA DE RED EN EL PROGRAMA CISCO PACKET TRACER

FUENTE: AUTOR

También se planteó la posibilidad de utilizar el simulador de redes GNESE3, pero no presentaba ninguna ventaja con respecto a CISCO PACKET TRACER dado que, aunque se podía hacer una representación de la red, no todos los equipos de la simulación correspondían a los equipos instalados.

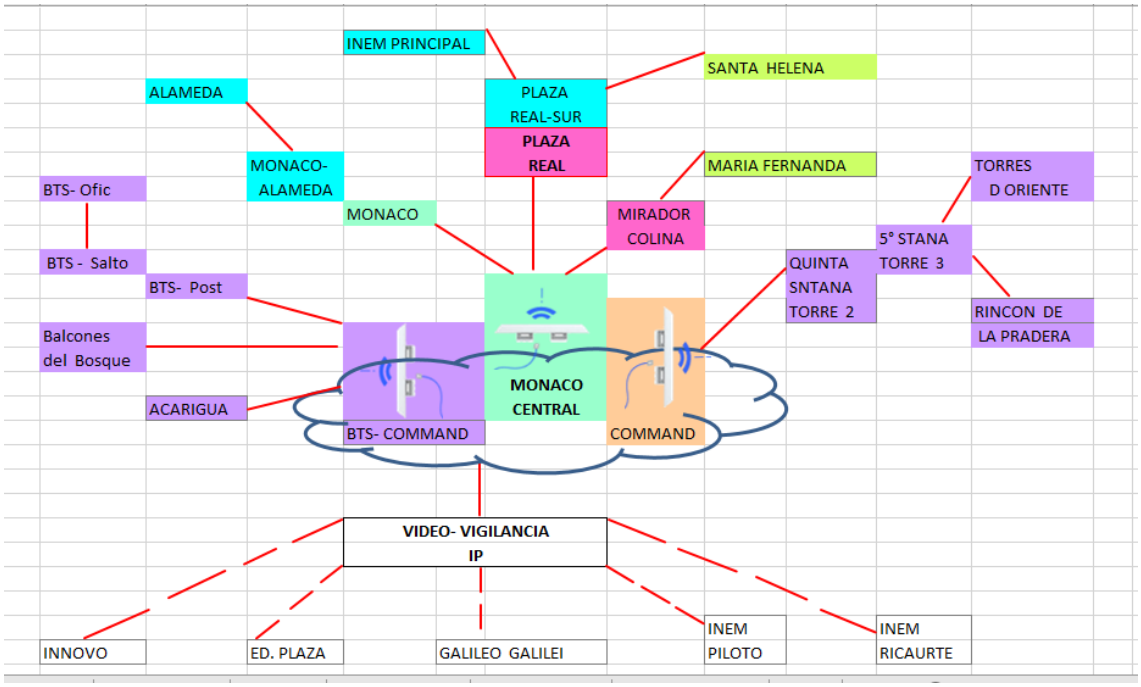


FIGURA 67. ESQUEMA DEL MAPA DE RED

FUENTE: AUTOR

Después de realizar el análisis de los datos que están configurados en la plataforma AIR OS de UBIQUITI, las tablas y documentos generados como los archivos producto de esta pasantía para el departamento de ingeniería de SERVIBOY LTDA, se elaboró el esquema de red que se observa en la figura 67. Aunque no se encuentra dentro de un programa de simulación de redes, si establece todas las conexiones con las que se cuenta en la empresa, para su funcionamiento.

Con el ánimo de consignar esta información, en un programa que efectivamente sea para el modelamiento de redes de telecomunicaciones, se elaboró el mapa de red de SERVIBOY LTDA en el programa VISIO, como se puede observar en la figura 68.

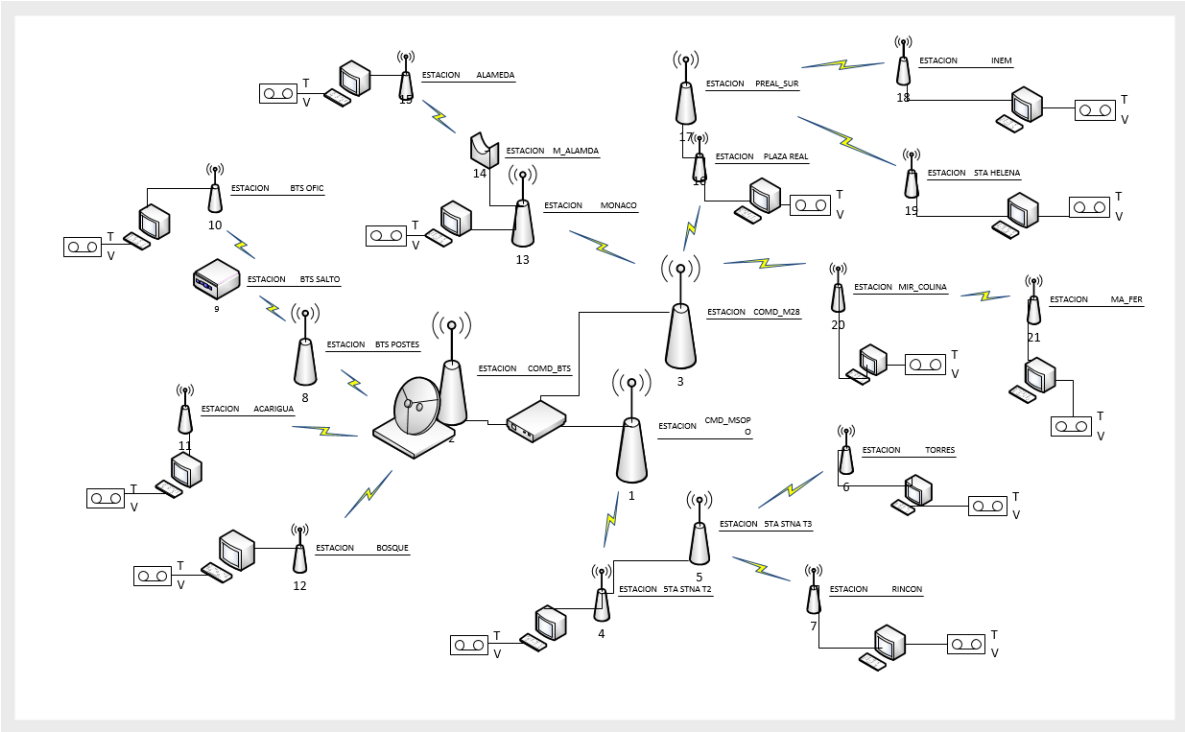


FIGURA 68. MAPA DE RED DE SERVIBOY LTDA

FUENTE: AUTOR

CAPITULO 5

5. OTRAS LABORES

Durante la práctica profesional en SERVIBOY LTDA, se llevó a cabo una amplia investigación sobre la vigilancia con sistemas de alarmas y control de accesos; sus componentes y su funcionamiento. Así como con los sistemas de cámaras, este conocimiento es fundamental tanto para realizar labores de mantenimiento de equipos, como para la implementación de estos, en nuevas instalaciones.

5.1. SISTEMAS DE ALARMAS

La caracterización básica de un sistema considera las variables (entradas, recursos, etc.) que ingresan al mismo, y los productos o respuestas obtenidos. En el caso de un sistema de alarma, tendría como entrada o estímulo el impulso eléctrico generado por uno de sus sensores, diseñados para emitir una señal de alarma ante la presencia o actuaciones de un intruso, mediante la captación de cambios causados en los elementos de seguridad; y como respuesta o salida, tendría la activación de una sirena, la llamada a la central de monitoreo o el bloqueo de accesos. Su función, es la de producir una alerta desde el momento en el que se desencadena la amenaza.

5.1.1. EVOLUCION DE LOS SISTEMAS DE ALARMA

La primera alarma electromagnética del mundo la patentó el 21 de junio de 1853, AUGUSTUS RUSSELL POPE de Boston, EEUU. Hasta entonces la gente confiaba en que los ruidosos graznidos de los gansos, la fidelidad de sus perros guardianes o las campanillas mecánicas sirvieran para detectar la presencia de ladrones.

FIGURA 69. ALARMA ANTIGUA

FUENTE: http://www.abus.com/es/Guia/Proteccion-antirrobo/Sistemas-de-alarma/Historia-de-los-sistemas-de-alarma

El siglo veinte trajo importantes desarrollos al mundo de la tecnología de alarmas. En la década de 1970, los técnicos integraron los primeros detectores de movimiento en los sistemas de alarmas. Los años 1980 y 1990 estuvieron caracterizados por una creciente estandarización, lo cual a su vez redundó en un uso cada vez más extendido para la protección de edificios. Finalmente llegaron los primeros sistemas de alarma inalámbricos al mercado, que revolucionaron la tecnología de alarmas. [25]

5.1.2. COMPONENTES DE LOS SISTEMA DE ALARMAS

Su estructura básica, está dado por: central de monitoreo de alarmas, teclado, detectores, comunicador, salida de alarma y el panel de control.

FIGURA 70. ESQUEMA GENERAL DE LA VIGILANCIA CON ALARMAS

FUENTE: http://xn--peaslom-5za.com/2.html

[25] http://www.abus.com/es/Guia/Proteccion-antirrobo/Sistemas-de-alarma/Historia-de-los-sistemas-de-alarma

Los componentes de los sistemas de alarma con los que SERVIBOY lleva a cabo sus proyectos de seguridad y monitoreo, trabajan dos líneas: la cableada y la inalámbrica. El funcionamiento en ambos casos, es igual. La diferencia consiste en que los sensores, contactos y elementos de salida de la alarma poseen o no, la capacidad de enviar algún cambio hasta el panel de alarma sin necesidad de cableado, lo que significa un aporte más en cuanto a lo estético que a lo funcional. Para el caso de los sistemas de alarma inalámbrica, la configuración tendrá como primera medida, el reconocimiento de cada uno de los componentes por parte del panel.

5.1.2.1. SENSORES INFRARROJOS

Su operación se fundamenta en la propiedad que tienen todos los cuerpos, de presentar radiaciones térmicas, en razón de su temperatura. En consecuencia, se utiliza la posibilidad de realizar la captación permanente de un entorno fijo y detectar la aparición de un intruso en el mismo, por la variación de temperatura que el movimiento del cuerpo provoca. Según las características del lugar a monitorear, pueden ser interiores o exteriores.

FIGURA 71. SENSOR INFRARROJO E INTRUSO

FUENTE: http://www.sdsseguridad.com/sds/index.php/robo.html

5.1.2.2. BARRAS FOTOELECTRICAS

Es un sistema sensible a las condiciones meteorológicas. El fundamento de la barrera de infrarrojos está dado por un haz de rayos, o luz infrarroja, invisible y permanente entre el emisor y el receptor, y cuya interrupción se transforma en señal de alarma.

5.1.2.3. CONTACTOS DE APERTURA

Son mecanismos que detectan la apertura y cierre de puertas o ventanas y generan una acción. Ejemplo: la luz que se enciende en la nevera, cuando se abre la puerta. El contacto se mantiene en posición de no alarma, cuando la puerta o ventana está cerrada, tal manera que cuando se abre la puerta o ventana, el imán se aleja del interruptor de contacto, activándose la alarma.

FIGURA 72. FOTO MAGNETICO EMPRESA

FUENTE: AUTOR

5.1.2.4. DETECTORES DE ROTURA

Habitualmente son más usados en establecimiento comerciales, que en residencias. Su función es la de activar la alarma, cuando por ejemplo se rompe un vidrio, al captar la frecuencia característica de la rotura de cristal en la unidad protegida.

FIGURA 73. FOTO SENSOR EMPRESA

FUENTE: AUTOR

5.1.2.5. TECLADO

Las características específicas dependen de cada fabricante. Sin embargo, por lo general y particularmente los utilizados por SERVIBOY, corresponden a un teclado numérico con una pantalla LCD incorporada, algunas teclas de función y dos o tres leds, que a la vez constituyen la interfaz para la interacción del ingeniero (durante la instalación y configuración) o los usuarios, con el dispositivo. Su función es la de activar o desactivar el sistema, mediante la digitación de una clave. Previamente se carga una lista de usuarios con el fin de que cuando alguien ingrese a la zona monitoreada, permita identificar que en el lugar se encuentra una persona autorizada para estar allí. En caso de que el usuario presente una situación de riesgo, ya sea por intrusión, incendio o

emergencia médica, dispone de las teclas de función, para enviar la señal de alerta al Command Center.

FIGURA 74. FOTO TECLADO DE ALARMA SERVIBOY

FUENTE: AUTOR

5.1.2.6. SALIDA DE ALARMA

Son aquellas que reaccionan ante una situación de alerta. La llamada a la central de monitoreo, para avisar de cualquier evento que se presente, ya sea por el funcionamiento normal de la alarma, como: test automático o apertura y cierre del lugar; o también por una señal de alerta o peligro. Otros dispositivos de salida de las alarmas, son de carácter disuasivo, como la sirena o luz estroboscópica, que se activan en caso de que el sistema detecte que un intruso a ingresado al lugar.

5.1.2.7. COMUNICADOR

Al detectarse cualquier evento en la alarma, este es enviado al Command Center. El dispositivo que envía dicha señal hasta la central de monitoreo es el comunicador. Dependiendo de la manera en que se configure la comunicación, será la naturaleza del equipo. FORMAS DE COMUNICACIÓN DE LAS ALARMAS DE SERVIBOY: Radio, Teléfono y GPRS.

5.1.2.8. PANEL DE CONTROL

Se refiere a una caja metálica, en la que se tiene una tarjeta de control a la cual, están conectados todos los demás elementos del sistema. Además, cuenta con una batería de respaldo, por si se llega a presentar una falla en el servicio de energía eléctrica, se pueda seguir contando con la protección de la alarma.

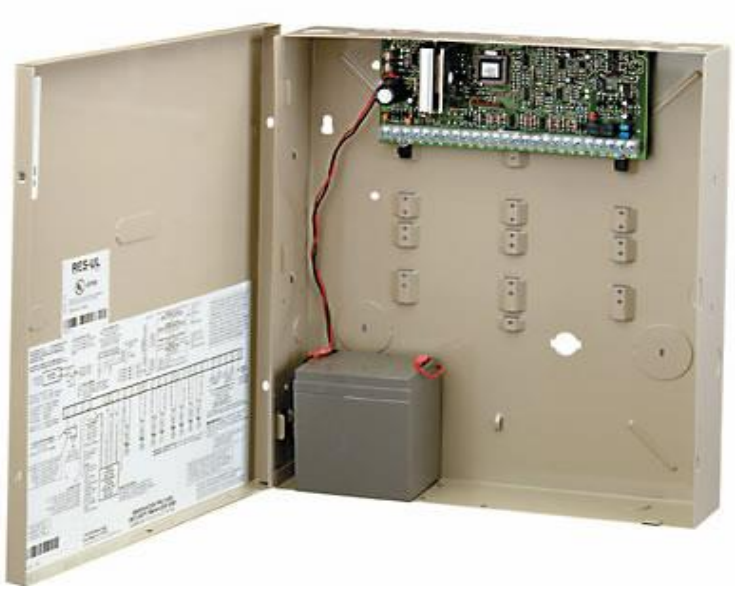


FIGURA 75. PANEL DE CONTROL DE ALARMA HONEYWELL

FUENTE: CATALOGO DE PRODUCTOS AGM

5.1.3. EQUIPOS PARA EL MONITOREO DE LAS ALARMAS

Además de los equipos que se instalan en un hogar o establecimiento, para la seguridad electrónica con sistema de alarma (sensores, sirena, teclado, sirena, comunicador y por supuesto, el panel); para el servicio de monitoreo de la alarma desde el Command Center de SERVIBOY, es necesario contar con el componente adecuado para recibir las señales correspondientes a los eventos generados en los sistemas instalados.

SERVIBOY cuenta con tres opciones para la comunicación de los paneles de alarma de los usuarios con la central, por lo tanto, en los equipos de los que dispone para este servicio, corresponden a los elementos que reciben los diferentes tipos de señal y finalmente, se tiene un software que administra todas las señales provenientes de las receptoras, con el fin de concentrar toda la información. Dicha información es con la que trabajan las operadoras del Command Center, para la seguridad de los usuarios.

5.1.3.1. CENTRAL Y RECEPTOR DIGITAL MULTI LINEA SG-DRL2A SG-CPM2

La empresa cuenta con este equipo, que consta de dos partes: SG-DRL2A, que es un receptor digital de múltiples formatos; y SG-CPM2, que es un módulo central de proceso.

El SG-DRL2A es un elemento diseñado para interpretar una variedad de formatos de comunicación para tener lo más actualizado en versatilidad y conveniencia. Adicionalmente, varios reguladores y la unidad de memoria no volátil aseguran que ninguna información se pierda o sea eliminada debido a un fallo en la red de energía eléctrica, o si la unidad debe ser apagada por mantenimiento. El CPM2 también tiene una memoria que mantiene un registro de los últimos 128 eventos los cuales pueden ser examinados en una pantalla LCD o pueden ser impresos. En caso que la impresora o un computador falle o si el modulo debe ser apagado por mantenimiento, el CPM2 guarda los últimos 128 eventos y envía automáticamente los eventos almacenados a un computador opcional o los imprime cuando el modulo sea puesto en línea.

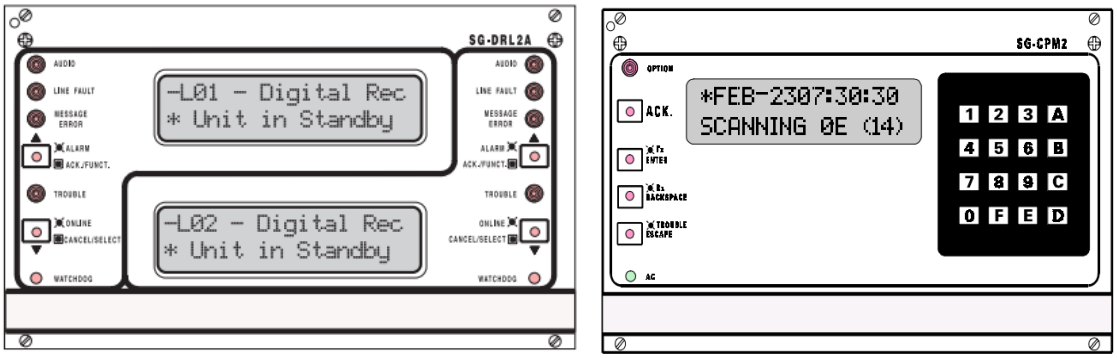


FIGURA 76. RECEPTORA SG-DRL2A SG-CPM2

FUENTE: DATASHEET SG-DRL2A SG-CPM2

La prestación de identificador de llamadas (pantalla de llamadas) está incorporado y el número telefónico reportado puede ser mostrado en pantalla, imprimirse y almacenado en la memoria; además la memoria del identificador de llamadas puede ser impresa en cualquier momento.

El equipo es energizado con 16V AC 50/60 Hz, por un transformador reductor externo. La unidad está equipada con conexiones para batería recargable de 12V y un cargador automático de batería como soporte, si se presenta alguna falla de la red AC. El bajo consumo de corriente hace posible que se tengan 24 horas de operación del equipo.

El CPM2 tiene 3 salidas programables (conmutado negativo), con una de las salidas siendo anunciada en la placa frontal de la unidad con un led. Las otras salidas están previstas para los leds y el reconocimiento de problemas. Una interfaz de teclado IBM compatible, se proporciona en la parte posterior de la unidad para usar con versiones futuras de software.

Este equipo recibe las señales de las alarmas que comunican por vía telefónica.

5.1.3.2. RECEPTORA DIGITAL PARA MONITOREO DE ALARMAS SENTRY PIMA

Para la recepción de las señales de alarma que comunican vía radio, SERVIBOY dispone de un completo sistema compuesto por hardware y software, que realiza el monitoreo y repite eventos vía radio, de los sistemas de alarma de los clientes.

El hardware de este equipo, consiste en un Receptor / Decodificador /Repetidor de Radio & Teléfono. El Receptor (SENTINEL CMS) y la Estación Repetidora de Monitoreo Inteligente (SENTINEL RMS) se diferencian por el software que corre en la tarjeta. El hardware de la SENTINEL se integra con la aplicación multilingüe de Gestión de Monitoreo1 ANDROMEDA de PIMA.

FIGURA 77. RECEPTORA SENTRY PIMA

Fuente: DATASHEET SENTRY PIMA

5.1.3.3. RECEPTORA VIRTUAL PARA MONITOREO DE ALARMAS OSM

Para los sistemas de alarma que se comunican por GPRS, SERVIBOY cuenta con una solución que no constituye hardware, sino que se trata de una receptora virtual: OSM.

FIGURA 78. ESTRUCTURA DE LAS ALARMAS QUE COMUNICAN POR GPRS

FUENTE: MANUAL DE CONFIGURACION DEL COMUNICADOR LX20

Los transmisores utilizados en este tipo de sistemas emplean la red de telefonía celular para la transmisión de eventos de paneles de alarma, desde la ubicación del cliente hasta la central de monitoreo. El software receptor OSM recibe los datos en la central, vía internet y los entrega al software de monitoreo. El OSM almacena todos los eventos o sucesos del sistema y los GPRS.

5.1.3.4. SOFTWARE DE MONITOREO DE ALARMAS: BYKOM

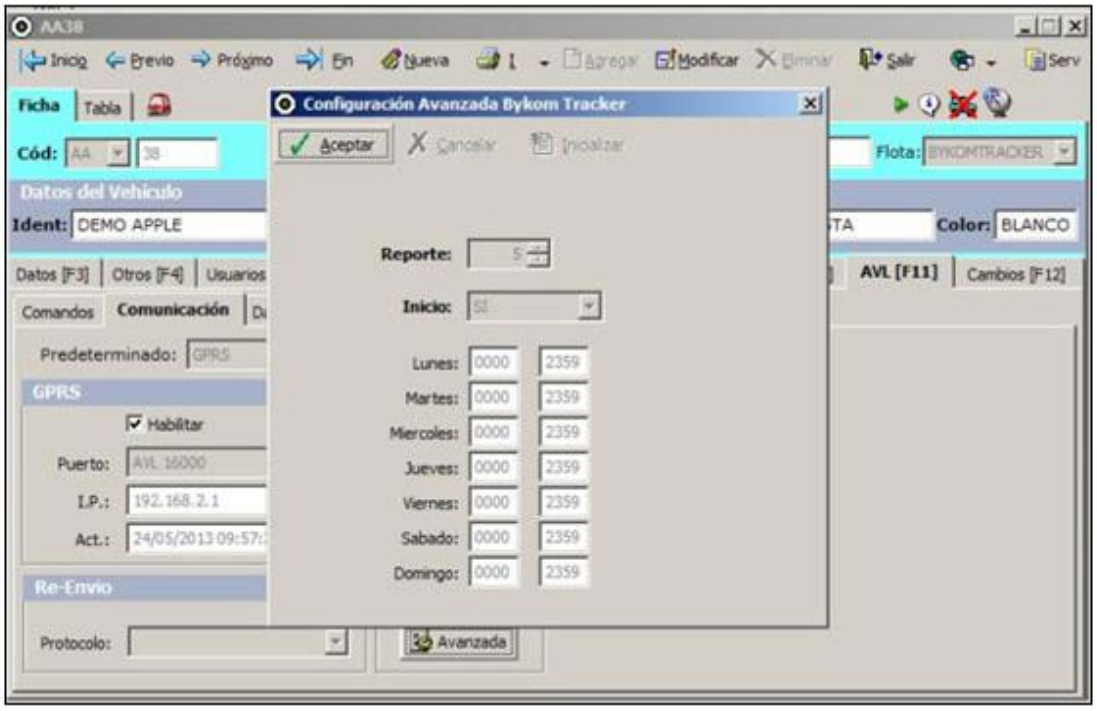


FIGURA 79. INTERFAZ DEL SOFTWARE BYKOM

FUENTE: AUTOR

Después de que los eventos se transmiten desde el panel de alarma hasta la respectiva receptora del Command Center; toda esta información se concentra en un programa.

Las receptoras envían estos datos a un PC- Servidor, donde está instalado dicho software para la recepción y procesamiento de señales compatible con todos los formatos, entregando a la central las herramientas necesarias para la administración simultánea de las señales recibidas vía radial, telefónica e IP/GPRS.

5.1.4. MANTENIMIENTOS E INSTALACIONES

Las labores de mantenimiento implican un conocimiento adecuado de los equipos y de las instalaciones, por ello, para trabajar con los diferentes sistemas de alarma, además de la investigación relacionada, se realizó una lectura juiciosa de cada uno de los manuales para conocer el funcionamiento de los sistemas de alarma usados por SERVIBOY LTDA.

En el caso de una instalación nueva, contando con este conocimiento, se realizan estudios de seguridad y se puede orientar a los clientes sobre lo que se debe implementar y cómo implementarlo dependiendo de las necesidades. El trabajo del personal de ingeniería, consiste principalmente en la configuración: tanto del sistema, como del comunicador que se instala.

5.1.4.1. MANTENIMIENTOS

Además del estudio realizado sobre la estructura general de sistema de vigilancia, fue necesario llevar a cabo una ardua investigación sobre los demás dispositivos, y también de los programas (software) que se emplean.

Los mantenimientos a los sistemas de alarma, incluye revisión y arreglo o cambio de sensores detectores de movimiento, detectores de humo, contactos magnéticos para la protección de puertas y ventanas, tarjeta de control de la alarma, programación y configuración del dispositivo; tanto en la línea cableada como inalámbrica.

5.1.4.2. INSTALACIONES

Se lleva a cabo la disposición de los equipos: ubicación estratégica de los sensores exteriores e interiores y los contactos magnéticos. En cuanto al teclado, este debe ser colocado a una distancia corta de la entrada principal, pues el usuario ingresa al lugar monitoreado y lo primero que debe hacer, es digitar la clave, para que se registre una apertura normal en la central, de lo contrario la alarma se activa, como si se tratara del ingreso de un intruso. Por último, se instala el panel de alarma; por lo general, este no debe estar a la vista, pues no debe ser manipulado por nadie, excepto el personal técnico y de ingeniería de SERVIBOY.

5.1.5. SISTEMAS DE COMUNICACION DE LAS ALARMAS EN SERVIBOY

La parte final en la instalación de alarmas, corresponde a la configuración de panel como tal: programando la cantidad de usuarios que estarán habilitados para activar o desactivar la alarma, claves para cada uno de los usuarios y se establece el tiempo que el usuario tendrá mientras abre la puerta de la unidad y digita la clave correspondiente, antes de que se genera una alerta en la central de monitoreo.

ALARMAS POR RADIO: se usan a nivel local (solo Tunja). Este sistema tiene asociadas varias alarmas, pero ya casi no se implementa en las nuevas instalaciones. Para estas alarmas, se usa un radio de la marca PIMA, compatible con la receptora SENTRY PIMA. La receptora viene con un software de configuración, en el que se ingresan los nuevos usuarios, para establecer la correcta comunicación con la central.

ALARMAS POR TELEFONO: se usan, siempre y cuando el cliente cuente con línea telefónica. En este caso, la comunicación se establece solo a nivel de hardware, no es necesario ningún programa, sino que el panel de alarma dispone de salidas para la conexión de un adaptador que ira conectado a la línea telefónica del cliente.

ALARMAS POR GPRS: es la solución de comunicación de alarma que más se utiliza actualmente en la empresa. Tiene un muy buen alcance, además de eliminar los límites geográficos, gracias a que su trabajo se soporta en las antenas que se usan para la comunicación celular. Para su funcionamiento, tiene una SIMCARD, se trabaja con las empresas proveedoras de estos servicios: claro y movistar, mayoritariamente movistar.

Los transmisores pueden ser programados localmente usando el cable de programación LXPROG RS232, estableciendo los parámetros de funcionamiento del GPRS en la plantilla de configuración. También es posible la configuración vía GPRS, para este último caso el servidor OSM debe estar operando y el equipo GPRS conectado.

5.2. CONTROL DE ACCESO

FIGURA 80. TIPOS DE CONTROL DE ACCESO

FUENTE: CATALOGOS PROVEEDORES SERVIBOY

El Control de Acceso es uno de los apartados de mayor relevancia en seguridad privada. La intrusión, por sí sola, no es un riesgo, dado que nadie comete intrusión por el mero hecho de penetrar en un recinto, sin ninguna intención de llevar a cabo amenazas posteriores: actos antisociales, delictivos, provocación de accidentes. En la actualidad, el mercado presenta sistemas de control de accesos de alto nivel de sofisticación y de gran fiabilidad, destinados a discriminar la entrada sin demasiadas complicaciones ni demoras.

Se define el control de accesos como la comprobación, inspección y fiscalización, del paso o circulación de personas, vehículos u objetos a una zona clasificada como área protegida. Es el primer eslabón de la seguridad. La canalización arquitectónica, las barreras naturales, es el medio más elemental de asegurar y controlar el acceso de personas.

Es muy relevante el tipo de instalación en el que se implante, la lógica marca que habrá de ser mucho más significativo en aquellos lugares en los que exista un mayor nivel de riesgo, como pueden ser centros oficiales e instituciones públicas. Se trata, en definitiva, del empleo de medios que obliguen físicamente a seguir un itinerario determinado y pasar por una o más puertas concretas, donde estarán ubicados, medios de control.[26]

5.2.1. COMPONENTES DE LOS SISTEMAS DE CONTROL DE ACCESO

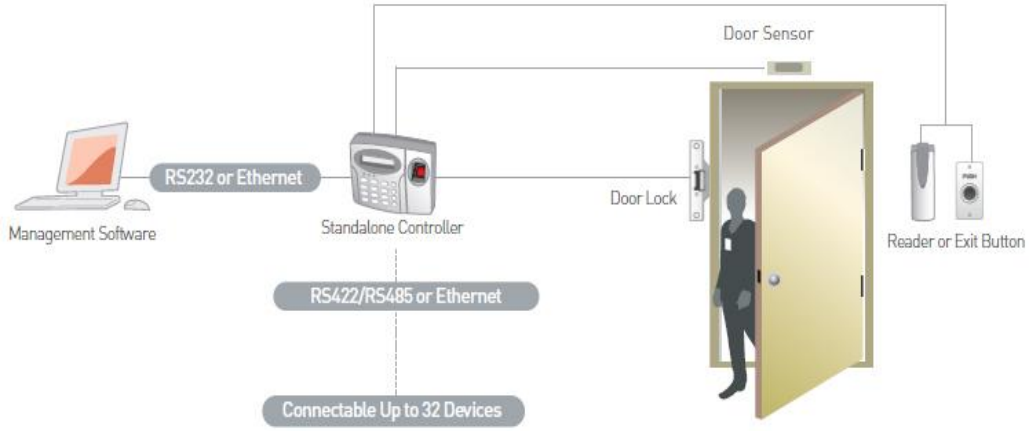


FIGURA 81. ESQUEMA DE UN SISTEMA DE CONTROL DE ACCESO

FUENTE: CATALOGO DE PRODUCTOS ZKSOFTWARE

Las funciones específicas serán las de control de:

- ENTRADAS: Selección de todo lo que puede entrar. Impedir la entrada a lo que no esté autorizado. Detección de entradas no autorizadas. Neutralización de riesgos.
- SALIDAS: Detectar y evitar la salida de todo lo que no esté autorizado.

[26] http://losvigilantesdeseguridad.org/vigilantes.html

- ❖ CIRCULACIÓN: Evitar la circulación de todo lo que no esté autorizado.
- ❖ PERMANENCIAS: Detectar y evitar la permanencia de todo lo que no esté autorizado en áreas para las que no presenta autorización.

5.2.1.1. CABINA DE CONTROL O CONTROLADORA

Es el elemento que concentra la información y toma las decisiones, en consecuencia. Todos los demás dispositivos solo generan información o ejecutan acciones. También es función de la controladora, la tarea de comunicarse con el programa central que centraliza toda la información del sistema en general, tanto la información de configuración y programación como la de eventos producidos.

FIGURA 82. CONTROLADORA DE ACCESOS ROSSLARE

FUENTE: CATALOGO DE PRODUCTOS ROSSLARE

5.2.1.2. DISPOSITIVOS DE IDENTIFICACIÓN

Son aquellos que tienen por objeto identificar a la persona que desea el acceso. Existen diferentes tipos de dispositivos, cada uno con sus propias características. Se utilizan tarjetas maestras, teclado o dispositivos de identificación biométrica. Algunos permiten el acceso más rápido, como las tarjetas de proximidad, y otros identifican al sujeto con más precisión, como los lectores biométricos.

5.2.1.3. DISPOSITIVOS DE ENTRADA

Estos dispositivos comunican a la controladora el estado de las variables del sistema, tales como si la puerta está abierta o no, si se pulsó el botón de salida, etc., y le permiten tomar decisiones con mayor precisión.

5.2.1.4. DISPOSITIVOS DE SALIDA

Son aquellos que ejecutan las acciones ordenadas por la controladora como las de liberar cerraduras, accionar barreras, accionar alarmas, etc.

5.2.1.5. RED DE COMUNICACIONES

Es la red utilizada para que la controladora se comunique con otros de los demás elementos del sistema y con una o más estaciones centrales.

5.2.1.6. SOFTWARE DE CONFIGURACION Y CONTROL

En ocasiones, el software solo es de configuración. Y para otros proyectos, el software se usa en la configuración, pero también se instala en un PC del lugar, con el fin de tener un registro de las acciones que se lleven a cabo, con el sistema de control de acceso.

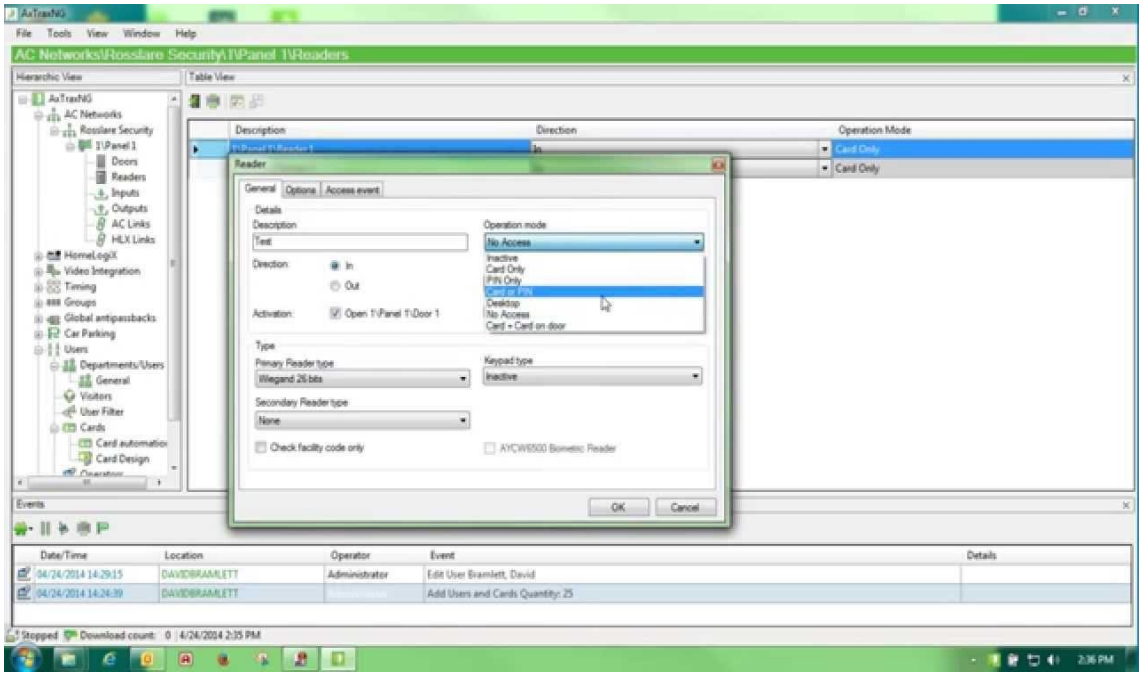


FIGURA 83. SOFTWARE CONTROL DE ACCESO

FUENTE: AUTOR

Cuando no es necesario tener un registro detallado de los accesos dados en determinado lugar, el software es solo de configuración y se usa al instalar el sistema para cargar la información de los usuarios en la controladora, o cuando se necesite registrar nuevas tarjetas. En otras instalaciones, el cliente necesita no solo permitir el acceso a los usuarios inscritos en la controladora, sino que además la controladora guarde el registro del número de tarjeta, usuario que ingresa y fecha y hora tanto de entrada como de salida del lugar; en este caso, es necesario contar con un PC en el que se instala el software para que allí se pueda observar todos los eventos producidos, para su revisión.

5.2.2. INTERVENCIONES EN LOS CONTROLES DE ACCESO

En el área de control de acceso, con el estudio de los manuales del software y de los componentes, se pudo conocer el mecanismo que hace posible un control de acceso sistematizado, con el fin de aportar ideas en la implementación de nuevos sistemas y colaborar en las configuraciones que se requieran.

5.2.2.1. CONTROL DE ACCESO EDIFICIOS MONACO Y ALTOS DE VALIZA

La estructura del edificio Mónaco, es un sistema de control de acceso totalmente automatizado, ya que cuando el usuario hace uso de su tarjeta en el ascensor, este se dirige directamente al piso correspondiente.

Los mencionados edificios corresponden a dos unidades independientes, que poseen el mismo software de configuración. Estos sistemas disponen solo de la capacidad de permitir o denegar el acceso, sin ejercer control sobre los datos. Los administradores de los conjuntos respectivamente, solicitan visita del personal del departamento de ingeniería de SERVIBOY. Se hace presencia en la unidad y se registraron nuevas tarjetas para el ingreso de los usuarios.

5.2.2.2. CONTROL DE ACCESO VILLA TOSCANA

El conjunto cerrado VILLA TOSCANA ubicado en el municipio de Jenesano, cuenta con una controladora de acceso para cuatro puertas peatonales. El sistema de control de acceso en esta unidad, permite tener un registro de las entradas y salidas de los usuarios, estableciendo fecha y hora de los mismos, así como la especificación de la puerta en la que se admite el ingreso. Adicionalmente, está en estudio la posibilidad de instalar un control de acceso de tipo vehicular.

Servicio de mantenimiento: Revisión del programa de control de acceso. Se reportó una falla en la puerta para acceder a una de las manzanas del conjunto, se realizaron pruebas con las tarjetas de usuario. Se revisó el sistema y algunas tarjetas de usuarios para acceso al conjunto, que estaban fallando. En cuanto al programa, fue necesario repasar y actualizar las características del software.

Dicha actualización, permitió que la información de las tarjetas que no se encontraban funcionando, se volviera a cargar en la controladora, para que los usuarios puedan ingresar normalmente, de nuevo. Se realiza una inspección general del sistema y se lleva a cabo el mantenimiento correspondiente.

5.2.3. INSTALACIONES

Cuando la empresa SERVIBOY proyecta la implementación un sistema de control de acceso, evalúa los riesgos, tenido en cuenta puntos como:

- NIVELES DE ACCESO PERMITIDOS: establecer los controles seleccionando a las personas, vehículos y objetos que podrán acceder por un control determinado.
- ZONAS: De acceso permitido, o libre, y de acceso restringido.
- FRONTERAS: Son los espacios que separan dos zonas contiguas.
- ITINERARIOS: De entrada, de salida o de interiores.

5.2.4. IMPLEMENTACION DEL CONTROL DE ACCESO EN EL CONJUNTO MARIA FERNANDA

En este conjunto se instaló el control de acceso para los vehículos. En este caso, que el sistema es para uso residencial, mediante la evaluación previa, se determinó: no se estipulan itinerarios de entrada o salida o de interiores, ya que los propietarios tienen la libertar de entrar y salir del conjunto sin restricción de horarios. Se establece que tendrá un nivel de acceso, que estará directamente dispuesto en la entrada principal del edificio. Lo que en seguida nos permite determinar que se tendrán dos zonas: la de acceso libre corresponderá a la calle 45 entre carreras 4ta y 5ta y la de acceso restringido es, naturalmente, el parqueadero.

Para esta instalación, se dispuso de una controladora de la marca ROSSLARE, que está integrada con el software AXTRAX. Para la autenticación de personal autorizado, se situaron dos lectoras de tarjetas (una interior y otra exterior), y finalmente, se adecuo una talanquera que será el elemento físico que impedirá la entrada al conjunto, en caso de que así corresponda o permitirá el ingreso, al tratarse de un usuario registrado.

Referente a la configuración, se instala el software AXTRAX en el PC de la portería principal, para contar con la información que se genera en el control de acceso. Posteriormente, se carga la información necesaria para habilitar las tarjetas de los usuarios. Se prueba que la configuración sea la correcta y que cuando un usuario ingrese el sistema guarde la información de fecha y hora de quien ingresa y se entrega, el sistema en funcionamiento.

5.2.5. CAPACITACIONES

Se llevaron a cabo capacitaciones para algunos guardas de seguridad y una de las operadoras de medios tecnológicos del Command Center de SERVIBOY, con el fin de poner en conocimiento de ellos, el esquema de funcionamiento general de los sistemas de control de acceso. En dichas capacitaciones, se realizaron procesos de adición de tarjetas al software, cuando la unidad así lo solicite.

5.3. LABORES ADMINISTRATIVAS

Referente al tema del desempeño de actividades administrativas, se trabajó de acuerdo a los requerimientos de SERVIBOY y tomando en cuenta lo que la Superintendencia de Vigilancia y Seguridad Privada en su normativa expone al respecto, se planteó el siguiente manual de funciones:

1. Recibir, estudiar y tramitar informes de fallas o novedades, así como respuestas de las quejas presentadas por los usuarios, y terceros sobre los servicios de vigilancia y seguridad privada.
2. Preparar para la firma del Gerente, los actos sobre los asuntos que estudia el área bajo su competencia.
3. Realizar las cotizaciones necesarias para los procesos de contratación en la entidad.
4. Realizar las entradas y salidas al almacén de elementos de la vigilancia de la empresa.
5. Actualizar y verificar los registros, formularios y procedimientos de carácter administrativo o técnico, a que dieran lugar, de acuerdo a los lineamientos sobre gestión de la información.
6. Realizar instalaciones de software esenciales para el uso cotidiano de los equipos, tales como editores de texto, antivirus, reproductores de audio y vídeo, sistemas operativos, navegadores y otras herramientas de trabajo. Brindar el soporte: Evaluar, probar e instalar hardware y software.
7. Asignar prioridades y gestionar la resolución de problemas con los usuarios, documentando procedimientos de instalación y configuración
8. Llevar y mantener actualizada la base de datos de cada uno de los trámites y archivos.
9. Promover y desarrollar la implementación, mantenimiento y mejora del Sistema de Gestión de Calidad dentro del puesto de trabajo de acuerdo con la normatividad vigente y las políticas institucionales.
10. Propender y fomentar la cultura organizacional de autocontrol y autoevaluación que contribuya al mejoramiento continuo, para el logro de la misión y objetivos institucionales.

Estas funciones, corresponden a la participación en la coordinación del Departamento de Ingeniería de SERVIBOY LTDA, tomando como base, un enfoque en el manejo de personal, siendo la líder del grupo de operadoras y técnicos del Command Center, coordinando ideas estratégicas, sobre su labor y gestionando la comunicación de las operadoras y el personal técnico, con la Gerencia.

5.3.1. INVESTIGACION SOBRE HABEAS DATA Y SU RELACION CON SERVIBOY

5.3.1.1. CONCEPTO

El derecho de hábeas data es aquel que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de naturaleza pública o privada.

5.3.1.2. ANALISIS

En una empresa como SERVIBOY LTDA; donde las personas dejan a nuestro cuidado, su cuidado y protección, siendo esto es una responsabilidad grandísima, hay que tener un especial conocimiento sobre el manejo y la seguridad de los datos que se tienen de los usuarios, ya que tenemos acceso a información personalizada y hay que conocer las normas sobre el uso de esta (HABEAS DATA). Así mismo, es importante documentarse sobre la seguridad en nuestro entorno y conocer las generalidades de las entidades del gobierno que tienen que ver con el ejercicio del trabajo en determinada entidad.

SERVIBOY tiene una relación directa con el derecho de habeas data, pues en el Command Center reposa una amplia información sobre los clientes de los servicios de vigilancia electrónica: que van desde datos generales, como: nombres completos, cedula; hasta información detallada como videos de su lugar de trabajo o residencia. El HABEAS DATA se busca proteger cualquier información vinculada a una o varias personas que puedan asociarse con una persona natural o jurídica, es decir, los datos personales, que pueden ser públicos, semiprivados o privados.

5.3.1.3. PRINCIPIO DE CONFIDENCIALIDAD

SERVIBOY está sujeto a este principio. El principio de confidencialidad en la información, consiste en que todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan carácter público, están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar el suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas.

5.3.2. CREANDO CONCIENCIA SOBRE LA COMUNICACIÓN EN LA EMPRESA

Para el departamento de ingeniería, es importante que se generen reportes de aquellas cámaras y alarmas que estén fallando; por parte de las operadoras del Command Center, pues esto permite un trabajo óptimo. Se detecta y establece la importancia de tener un registro que constituya una comunicación sólida entre los miembros de la empresa, para llevar control de las operaciones de la central y para que se trabaje de manera conjunta, buscando realizar el trabajo correctamente.

5.3.2.1. REPORTES DE FALLAS TECNICAS PARA EL DEPARTAMENTO DE INGENIERIA

Se hizo la revisión de los formatos para reportar novedades de las unidades, con el fin de enviárselas a los usuarios y se concluyó que, aunque es importante mantener informado al usuario sobre las novedades que puedan presentarse en las unidades monitoreadas a lo largo del día, está haciendo falta la existencia de un documento similar, pero que sea de manejo interno de la empresa, pues al indagar sobre la forma en la que se hacen reportes al personal técnico, se aprecia que las diferentes novedades que se presenten, se informan de manera verbal.

La idea es abrir el canal de comunicación entre el personal de ingeniería y las operadoras de medios tecnológicos, pues ellas son las que están en la central de monitoreo todo el tiempo, unas tratando el monitoreo de las alarmas y otras en la video- vigilancia, por lo tanto, son quienes observan las fallas en alguno de los sistemas de seguridad electrónica; así se puede organizar el tema, llevando reporte de los daños que se presentan y registrándolos para darles el debido tratamiento.

Por esta razón, se empieza a trabajar con las operadoras de Command Center, en la construcción de un formato en Excel, que permita relacionar los lugares que son monitoreados, documentando las fallas que se presenten. Adicionalmente, en la parte de monitoreo de cámaras, no solo se tiene que inspeccionar que la transmisión del video llegue correctamente a la central, sino que también se debe tener cuidado de verificar que las grabaciones se están realizando correctamente y así, tener certeza de estar brindando un servicio de calidad al usuario. Por lo tanto, también es importante informar del estado de las grabaciones, para contribuir a una mejor organización del trabajo del departamento de ingeniería.

5.3.2.2. IMPLEMENTACION DE LA MINUTA

Se formula la importancia de tener siempre un registro de las cosas que se hacen: hora de recibido y entrega de puesto de trabajo, o datos que sea necesario documentar para conocimiento de todas las operadoras. Además de tener siempre registro de todas las novedades que pueda generar en los lugares monitoreados. Esta documentación, también es para la comunicación interna del personal, en este caso, entre las diferentes operadoras de Command Center.

En algunas ocasiones, por la naturaleza de los turnos de trabajo, las operadoras no están reunidas en el momento del cambio de turno, por lo que es importante la importante, dejar consignadas o información general, para que, aunque no las operadoras no se encuentren en el cambio de turno,

si dejen y encuentren siempre los datos necesarios para estar actualizadas de lo que ocurre en su puesto de trabajo, generando un ambiente de mutuo entendimiento y cordialidad y se cumpla de manera satisfactoria con las labores.

5.3.3. CREACION DE CARPETAS PARA CADA UNIDAD MONITOREADA

Dentro de la generación de documentación para el departamento de ingeniería, se crean unas carpetas en las que los datos relevantes de cada unidad estén al alcance, en caso de ser necesario.

Documentos para Archivar en la Construcción de las Carpetas:

- Copia del contrato
- Formato de instalación de los equipos en la unidad
- Manual del Sitio (especificación de las cámaras),
- Graficas (Plano, Mapa): Google MAPS
- Graficas correspondiente a una foto del sitio
- Control interno de los guardas (generalidades, prohibiciones)
- Formatos: mantenimientos y reparaciones.

5.3.4. COORDINACION EN EL COMMAND CENTER

- Revisión de los turnos de trabajo de las operadoras de cámaras, analizando la viabilidad de continuar con los mismos horarios, o si es necesario hacer algunas modificaciones.

- Supervisar la distribución de cámaras en las diferentes pantallas que se tienen en el Command Center. Para responsabilizar a cada una de las operadoras por un número de unidades y un número de cámaras, procurando que el monitoreo de las operadoras, sea equitativo.

- Al ingresar una nueva operadora, capacitación en ofimática.

5.3.5. PROYECTOS LIDERADOS

Supervisar la instalación y puesta en marcha de diferentes sistemas de vigilancia electrónica.

※ VETERNARIA PET SHOP SISTEMA INSTALADO: ALARMA

Esta unidad hace referencia a una clínica veterinaria de la ciudad de Tunja. En compañía del personal técnico, se realizó la visita al lugar para realizar el estudio de seguridad. Se estableció la cantidad y ubicación de los componentes de la alarma. En un día se instaló el sistema y se tomó otro día para la configuración. Se entrega funcionando y a satisfacción.

※ MESON DE LOS VIRREYES SISTEMA INSTALADO: CCTV

El hotel Mesón de los Virreyes está ubicado en el municipio de Villa de Leyva, contando ya con el servicio de cámaras, instaladas también por SERVIBOY LTDA. El usuario ve la necesidad de realizar un cambio total en el sistema. Se llevó a cabo el desplazamiento hacia esta unidad, en compañía de uno de los técnicos. Se hizo una revisión general, encontrando que había 6 cámaras, de las cuales 1 estaba dañada. Junto con el cliente, se rediseña el sistema, determinando que ahora serán 12 cámaras y la ubicación de cada una de estas.

Del antiguo sistema se conservan las 5 cámaras que se encuentran funcionando correctamente y para las nuevas, se establece un cambio de tecnología: cámaras AHD. Es necesario cambiar de DVR, para que haya compatibilidad con todas las cámaras. Para realizar esta instalación, se contó con el trabajo de los técnicos de la empresa por seis días. Se muestra el sistema funcionando a los usuarios y se entrega a satisfacción.

※ TORRES DE SION: SISTEMA INSTALADO: CCTV Y ALARMA

Este conjunto residencial, es una obra que no está finalizada, al momento de solicitar la vigilancia electrónica. Las personas encargadas, solicitan la instalación tanto de cámaras como de un sistema de alarma, dada la gran extensión del lugar y los diversos puntos a vigilar.

Para este proyecto ubicado en la ciudad de Tunja, me dirigí al conjunto con el personal técnico, hicimos el estudio de seguridad, se determinó colocar 8 cámaras y una alarma con 3 particiones: Sala de ventas, Oficina Administrativa, Cuarto de herramientas; y se hace la cotización. Dependiendo de la marca y modelo especifico de la alarma, se permiten un número determinado de particiones, por lo general, se cuenta con 8 particiones. Las particiones en una alarma sirven para que se tenga un solo sistema, pero se pueda gestionar diferentes zonas de la unidad, de manera independiente; es decir, puedo desactivar la alarma en la partición 1 y la partición 2 seguirá activa, o viceversa; en caso de presentarse alguna activación, se genera alarma del sistema normalmente. Esto permite que se preste un monitoreo eficaz, pues no es fácil tener control de todo el lugar cuando es grande. Las tres particiones de alarma en este proyecto, permite que, aunque haya personal en la sala de ventas y esa zona este desactivada, como la oficina administrativa y el cuarto de herramientas se encuentran solos, puedan tener la alarma activada, lo que

significa que se encuentra en alerta de máxima en caso de presentarse alguna novedad y se garantiza la vigilancia de toda el área del lugar monitoreado.

Una vez se aprueba la cotización, se procede a la implementación de las cámaras y la alarma. Se concluye este trabajo al cabo de tres semanas, se realizan pruebas de funcionamiento y se entrega a satisfacción.

※ ACCESO BOYACA SISTEMA INSTALADO: ALARMA

Esta unidad corresponde a unas bodegas en la ciudad de Tunja. Me desplace con uno de los técnicos, para realizar el estudio de seguridad de la unidad. Se estableció la cantidad y ubicación de los dispositivos: 8 sensores infrarrojos y 3 contactos magnéticos. Se instaló el sistema y se hizo la configuración correspondiente. Se entrega funcionando y a satisfacción.

※ CALIPSO YOPAL SISTEMA INSTALADO: ALARMA

Esta unidad corresponde a un establecimiento comercial. Esta es una sucursal localizada en la ciudad de Yopal- Casanare; la empresa presta servicios de vigilancia electrónica, a otras sedes con esta misma marca Calipso en la ciudad de Tunja. El usuario hizo llegar a la empresa, un video con el recorrido de las instalaciones del sitio, pues no se realizó desplazamiento hasta allá para el estudio de seguridad.

El personal de ingeniería recrea un plano del lugar, con información suministrada por el cliente, para determinar la cantidad de equipos a instalar, realiza la cotización, siendo esta aprobada y se procede a agendar fecha de instalación. Se determina el uso de un comunicador GPRS, pues es la mejor opción para alarmas en lugares alejados, y se configura en las instalaciones de SERVIBOY. Uno de los técnicos viaja, realiza la instalación acordada, instala el comunicador, realiza pruebas con la central de monitoreo y entrega a satisfacción.

※ PLAZA REAL SISTEMA INSTALADO: VIDEO- VIGILANCIA

El trabajo que se llevó a cabo en el centro comercial Plaza Real de la ciudad de Tunja, consistió en el cambio del sistema de cámaras. Por la cantidad de personas que a diario visitan el centro comercial, la administración considera necesario mejorar la calidad de las imágenes que el sistema obtiene. El diseño del sistema como tal, sigue igual, ya que la ubicación de las cámaras coincide con los puntos más vulnerables y donde es fundamental la vigilancia. Se estudian los tipos de cámaras apropiadas para estas instalaciones, se cotizan y se programa instalación de los nuevos equipos. Se instalan 16 cámaras AHD: 13 fijas y 3 domos y DVR compatible, en 4 días. Se entrega funcionando a satisfacción.

※ INSTITUTO BRITISH ENGLISH SISTEMA INSTALADO: CCTV

El instituto de inglés BRITISH ENGLISH, solicita a la empresa la instalación de 3 cámaras, sin monitoreo. En esta ocasión, el cliente tiene determinada la ubicación de las cámaras, para los sitios en los cuales considera prioritario que se esté observando lo que sucede. Con las especificaciones del usuario, se realiza la cotización del sistema. El cliente autoriza la instalación del sistema, realizándose en 1 día. Se entrega funcionando y a satisfacción.

※ BALCONES EL BOSQUE SISTEMA INSTALADO: VIDEO- VIGILANCIA

El conjunto residencial Balcones del Bosque, se encuentra ubicado en la ciudad de Tunja. Me dirigí a la unidad, en compañía del Gerente, para realizar el estudio de seguridad. El edificio no presenta zonas de peligro inminente, pues es una zona completamente habitada, con excelente iluminación y se encuentra totalmente encerrado. Se determina el empleo de 8 cámaras: 3 exteriores y 5 interiores. Además, este sistema requiere de monitoreo remoto, pues no cuenta con personal de vigilancia humana. Como existe línea de vista, se instala una antena estableciendo una conexión punto a punto con la central de monitoreo. Se prueba funcionamiento y se entrega a satisfacción.

CAPITULO 6

6. BASE DE DATOS

6.1. ¿EN QUE CONSISTE UNA BASE DE DATOS?

Una base de datos es un sistema informático a modo de almacén. En este almacén se guardan grandes volúmenes de información, que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación, que busca ordenarlos y clasificarlos en conjunto. Las bases de datos pueden ser estáticas, cuando sólo sirven para su lectura y almacenamiento; o dinámicas, si la información se modifica y puede ser actualizada. [27]

FIGURA 84. CARACTERIZACION DE UNA BASE DE DATOS

FUENTE:http://programacion.net/articulo/los_mejores_gestores_de_base_de_datos_para_desarrolladores_1218

6.2. COMPONENTES DE UNA BASE DE DATOS

Una base de datos requiere de varios elementos para su correcto funcionamiento: un servidor, un lenguaje de programación, un sistema de gestión de información y una plataforma en la que se ejecuten los comandos. Por esta razón, para el diseño y puesta en marcha de la base de datos de SERVIBOY LTDA, se instaló WAMP SERVER, que es un paquete de archivos que se compone de los

[27] http://www.aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=500

requisitos anteriormente mencionados. Este nombre corresponde al acrónimo usado para describir un sistema de infraestructura de internet que contiene las siguientes herramientas:

- W: porque es compatible con Windows.
- A: se refiere a APACHE, que es un servidor web.
- M: de MYSQL, que constituye el gestor de bases de datos
- P: se refiere a PHP, que es el lenguaje de programación

FIGURA 85. COMPONENTES DE UNA BASE DE DATOS

FUENTE: http://falconhive.com/host-website-wamp-server/

El uso de un WAMP permite subir páginas HTML a internet, además de poder gestionar datos en ellas.

- LAMP es el sistema análogo que corre con Linux como Sistema operativo
- MAMP es el sistema análogo que corre con Macintosh como Sistema operativo

6.2.1. APACHE

El servidor Apache HTTP, también llamado Apache, es un servidor web HTTP de código abierto para la creación de páginas y servicios web. Es un servidor multiplataforma, gratuito, muy robusto y que destaca por su seguridad y rendimiento.

Para entender mejor lo que es Apache, definiremos lo que es un servidor web. La definición más sencilla de servidor web, que es un programa especialmente diseñado para transferir datos de hipertexto, es decir, páginas web con todos sus elementos (textos, widgets, baners, etc.). Estos servidores web utilizan el protocolo http.

Los servidores web están alojados en un ordenador que cuenta con conexión a Internet. El web server, se encuentra a la espera de que algún navegador le haga alguna petición, por ejemplo:

acceder a una página web y responde a la petición, enviando código HTML mediante una transferencia de datos en red. [28]

6.2.2. MY SQL

MySQL es un sistema de administración de bases de datos (DATABASE MANAGEMENT SYSTEM, DBMS) para bases de datos relacionales. Así, MySQL no es más que una aplicación que permite gestionar archivos llamados de bases de datos. MySQL, como base de datos relacional, utiliza múltiples tablas para almacenar y organizar la información. MySQL fue escrito en C y C++ y destaca por su gran adaptación a diferentes entornos de desarrollo, permitiendo su interactuación con los lenguajes de programación más utilizados como PHP, Perl y Java y su integración en distintos sistemas operativos.

FIGURA 86. SIMBOLO MYSQL

Fuente: http://www.esepestudio.com/noticias/que-es-mysql

También es muy destacable, la condición de OPEN SOURCE de MySQL, que hace que su utilización sea gratuita e incluso se pueda modificar con total libertad, pudiendo descargar su código fuente. Esto ha favorecido muy positivamente en su desarrollo y continuas actualizaciones, para hacer de MySQL una de las herramientas más utilizadas por los programadores orientados a Internet.[29]

6.2.3. PHP

PHP (acrónimo- PHP: HYPERTEXT PREPROCESSOR) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.[30]

[28] http://www.ibrugor.com/blog/apache-http-server-que-es-como-funciona-y-para-que-sirve/
[29] http://www.esepestudio.com/noticias/que-es-mysql
[30] http://php.net/manual/es/intro-whatis.php

6.3. CREACION DE LA BASE DE DATOS DE SERVIBOY LTDA

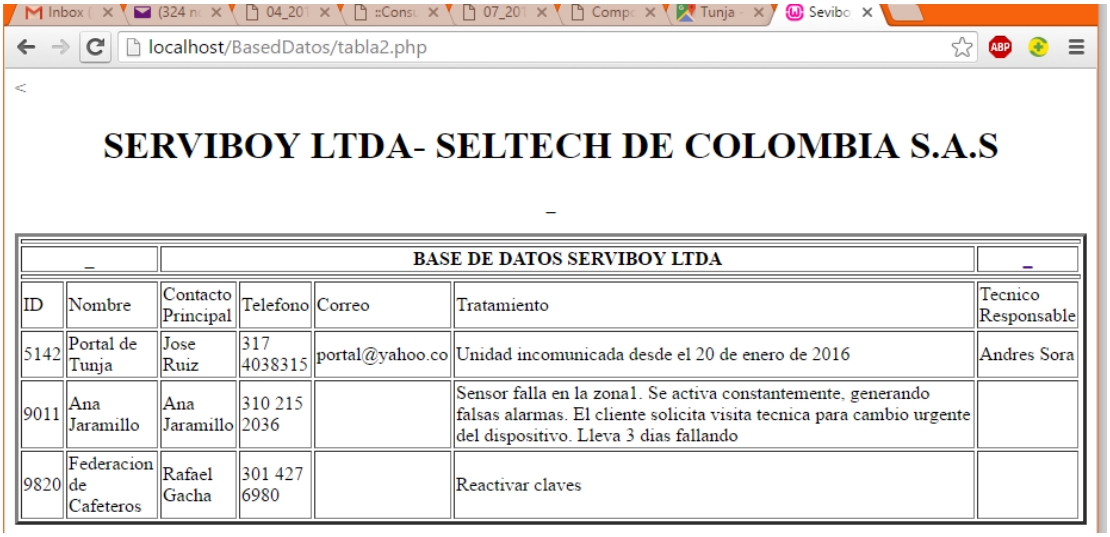
Una base de datos constituye la solución para concentrar dos cosas importantes: un registro de todos los usuarios y clientes de los diferentes servicios de seguridad electrónica e igualmente, tener un registro de los mantenimientos que se generan, para programar los que se realizan día a día, por parte de los técnicos.

6.3.1. OBJETIVOS DE LA BASE DE DATOS DE SERVIBOY

- Integrar la información de los datos de usuarios de los sistemas de vigilancia electrónica, en una sola plataforma.
- Llevar el control de mantenimientos
- Agendar efectivamente el trabajo del personal de técnicos.
- Identificación de las unidades donde las fallas son repetitivas.
- Que se le respete el tiempo al cliente
- Conocimiento por parte de las operadoras, si los mantenimientos se realizaron o no.

6.3.2. DESARROLLO

Para empezar con el diseño de la base de datos, fue necesario realizar una estructura básica y entrar en contacto con la programación web (HTML y PHP). Inicialmente se pensó en una tabla, donde se relacionarían los datos principales de usuario: nombre, teléfono y correo.



_	BASE DE DATOS SERVIBOY LTDA					_
ID	Nombre	Contacto Principal	Telefono	Correo	Tratamiento	Tecnico Responsable
5142	Portal de Tunja	Jose Ruiz	317 4038315	portal@yahoo.co	Unidad incomunicada desde el 20 de enero de 2016	Andres Sora
9011	Ana Jaramillo	Ana Jaramillo	310 215 2036		Sensor falla en la zona1. Se activa constantemente, generando falsas alarmas. El cliente solicita visita tecnica para cambio urgente del dispositivo. Lleva 3 dias fallando	
9820	Federacion de Cafeteros	Rafael Gacha	301 427 6980		Reactivar claves	

FIGURA 87. ESQUEMA BASE DE DATOS SERVIBOY LTDA

FUENTE: AUTOR

La tabla que se observa en la figura 87, fue un paso muy importante hacia la estructura de la base de datos. Cuanto se obtuvo la visualización de esta tabla, aparecieron nuevas especificaciones, pues esto es solo el primer paso y permitió observar hacia donde se dirigía este trabajo.

El programa editor de texto usado para la programación de la base de datos, fue Sublime Text.

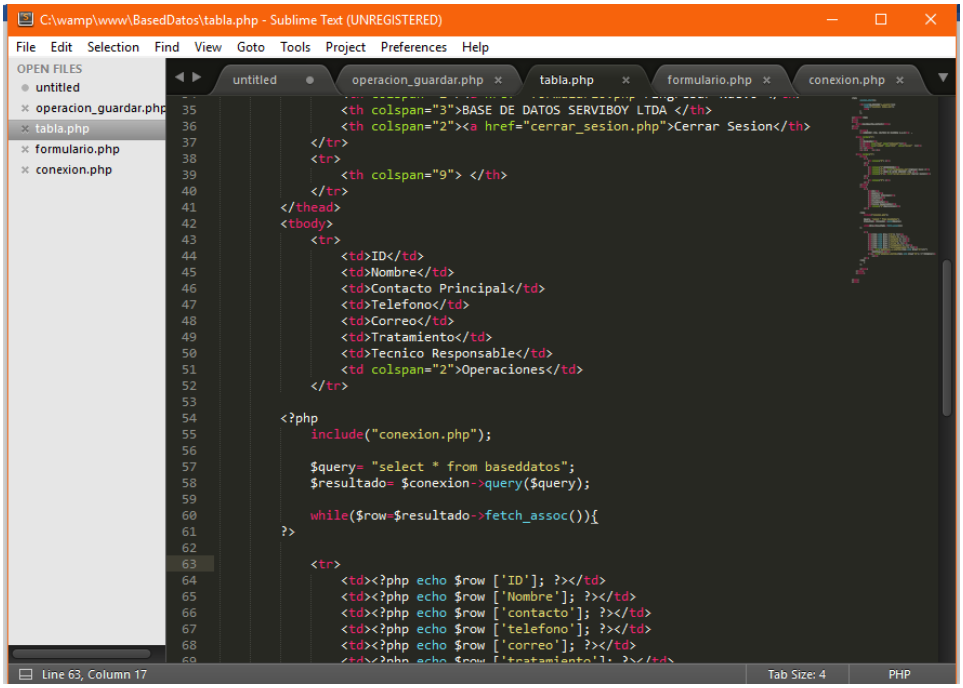


FIGURA 88. VENTALLA DEL PROGRAMA DE EDICION DE TEXTO SUBLIME TEXT

FUENTE: AUTOR

Al definir las características con las que se quiere trabajar, se diseña el sistema. La base de datos no solo debe tener la tabla en la que se encuentran los datos de los usuarios, sino que debe tratarse de una plataforma estructurada, que permita:

- Login del personal autorizado
- Adición de nuevas unidades al sistema
- Modificación de los datos de cada unidad
- Actualización de las adiciones y/o modificaciones realizadas
- Bloqueo de la muestra de datos, sin el registro del usuario
- Asignación de visitas técnicas a personal especifico
- Cierre de sesión.

Para ingresar a la base de datos, se tiene previamente una lista de usuarios, en la que están relacionadas las personas que tienen acceso a esta. Cada uno de estos usuarios, se encuentra asociado a una contraseña, para proteger la integridad de la información en la base de datos.

6.3.3. VENTANAS DE LA BASE DE DATOS DE SERVIBOY LTDA

Dadas las especificaciones anteriores, se trabaja en la programación de ventanas de presentación:

Página de inicio de sesión: Es la página de entrada y desde la cual, las personas que tengan acceso a la base de datos, ingresan un nombre de usuario y una contraseña, que serán validados para permitir o denegar el ingreso.

Página de Modificación: Corresponde a la página a la cual se programó que se direccione el usuario, cuando este necesite realizar cambios en los datos de las unidades o sus novedades.

Página de Adición: Hace referencia a un formato en el que el usuario ingresa datos de una nueva unidad.

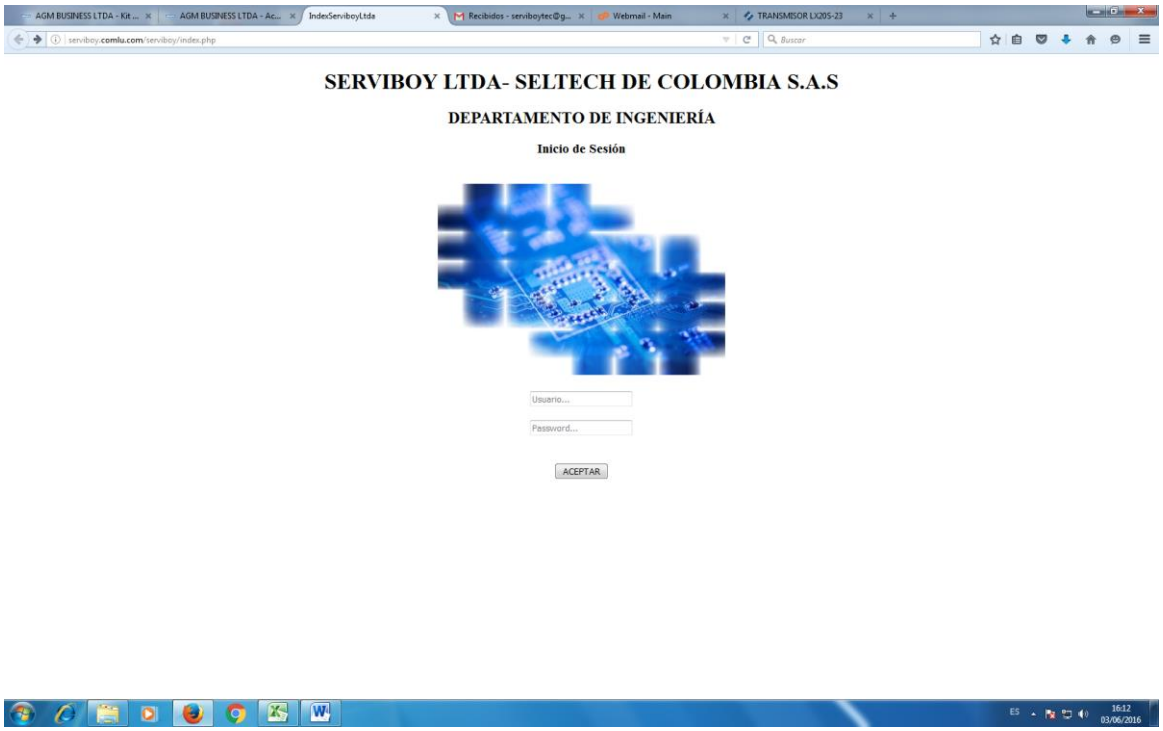


FIGURA 89. PAGINA DE INICIO DE LA BASE DE DATOS DE SERVIBOY

FUENTE: AUTOR

Al principio y para el desarrollo de la base de datos, se creó teniendo como servidor a mi computador personal, pero luego fue instalada en el servidor de la empresa, para que se empezara a hacer uso de la misma.

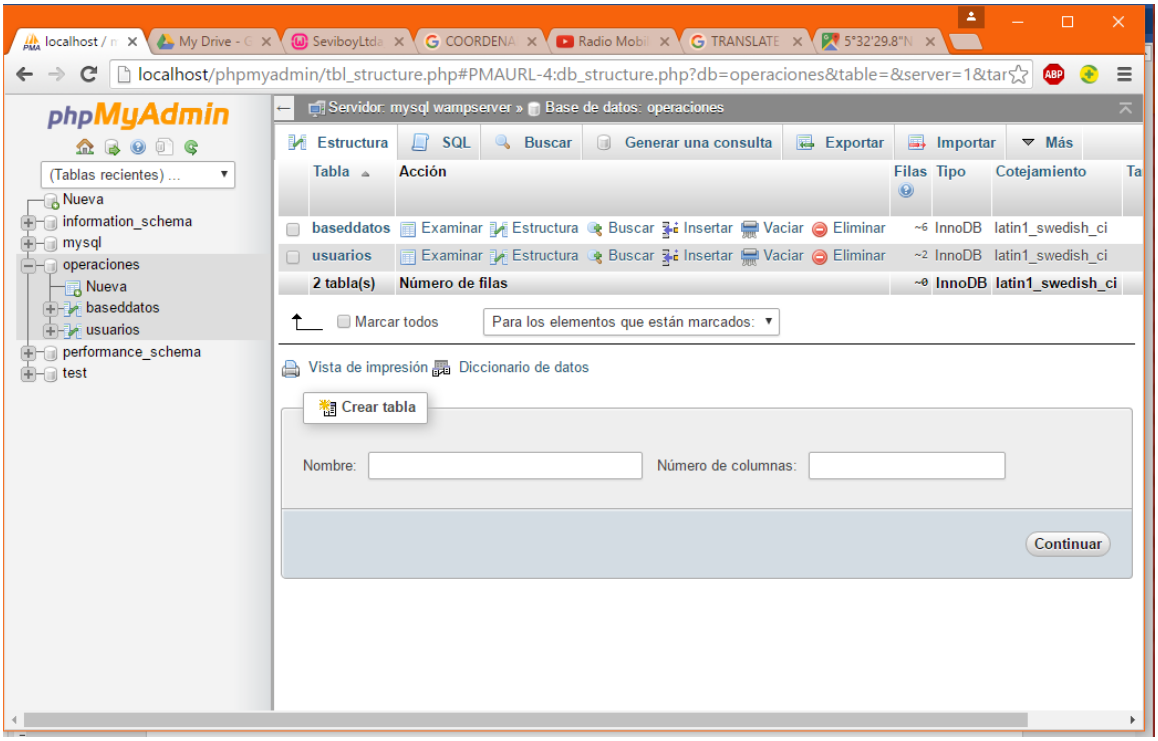


FIGURA 90. GESTOR DE LA BASE DE DATOS DE SERVIBOY

FUENTE: AUTOR

6.3.4. ANALISIS DE DATOS

El hecho de contar con la base de datos, permite observar continuamente el comportamiento que tienen los diferentes sistemas instalados de vigilancia electrónica. Si en una unidad siempre falla algo, identificar fallas comunes. Tal vez los dispositivos ya están dañados, tal vez el técnico no dio la solución exacta. La estructura que se creó, permite documentar que falla hay en la unidad, cuando se realiza el mantenimiento, se especifica el nombre de la persona encargada y así, se detalla quien y que visitas técnicas se realizan en las unidades.

Gracias a la creación de la base de datos, la empresa cuenta con un proceso más organizado para la coordinación del área de ingeniería.

CONCLUSIONES

- Poseer documentación técnica de los elementos, tecnologías y esquemas de conexiones o enlaces, que conforman un sistema, es de gran importancia para la empresa SERVIBOY LTDA, a la hora de prestar sus servicios; permitiéndole proporcionar un sistema adecuado y con un correcto funcionamiento del mismo.

- El hecho de tener dentro de la empresa SERVIBOY LTDA, un sistema de simulación de redes, significa un avance en cuanto a calidad de servicio se refiere, reduce los costos y el tiempo que se generan por realizar enlaces de unidades con el método de ensayo- error. Además, ha permitido realizar análisis de los enlaces existentes, para determinar qué tan satisfactorios son las conexiones que se han implementado hasta el momento y garantizando que futuros enlaces se realicen, con alta calidad de comunicación.

- La implementación de sistemas de seguridad, es una tarea que requiere de investigación profunda y un análisis detallado. Por medio de estas dos actividades, es posible establecer un procedimiento adecuado para llevar a cabo el desarrollo de un proyecto, y de esta forma, evitar que se presenten errores, por falta de conocimiento de las funciones, características, conexiones o parámetros, de los elementos que conforman el sistema.

- La creación de un sistema informático de almacenamiento, genera una mejora significativa para el desarrollo de las actividades del personal del departamento de ingeniería de SERVIBOY LTDA, pues por medio del uso de esta, es posible llegar a obtener un desempeño ideal, pues además de relacionar la lista de usuarios, en la base de datos se hace un seguimiento de las visitas técnicas, optimizando el rendimiento del trabajo y mejorando la relación con el cliente, que redunda en beneficio, tanto para la empresa como para el usuario.

- El reconocimiento de tecnologías, interfaces, dispositivos, componentes y demás elementos de un sistema, es de gran importancia en los procesos de desarrollo de actividades u operaciones que requieran de diseño, implementación, reparación, adaptación, etc.

RECOMENDACIONES

- Capacitar al personal técnico de la empresa SERVIBOY LTDA, sobre la configuración necesaria y el manejo de las aplicaciones que permiten visualizar las cámaras en los dispositivos celulares, teniendo en cuenta la compatibilidad aplicación- marcas de cámaras; para que brindar al cliente la posibilidad de revisar la unidad monitoreada, cuando lo requiera y desde cualquier lugar.

- Es fundamental poseer sensores de movimiento, sensores discriminadores de audio, sensores de exteriores, fuentes de alimentación de cámaras y video- balun, de repuesto; que son los dispositivos que generan más llamadas de los usuarios para solicitar visitas técnicas de mantenimiento, tanto de marca HONEYWELL como DSC, que son las más usadas por SERVIBOY LTDA en sus proyectos. Esto permitiría reducir el tiempo que tarda un sistema de vigilancia, fuera de servicio mientras se verifica el funcionamiento de estos dispositivos. Al existir esta serie de equipos de repuesto, se programaría temporalmente, mientras se revisa el equipo original.

- En el Command Center las operadoras de medios tecnológicos tienen distractores que pueden interferir con las funciones que cada una de ellas debe cumplir en su turno de trabajo. Debido a que el trabajo es de mucha responsabilidad y requiere de la absoluta atención del personal, es prudente que se restringa parcialmente el ingreso a internet, de manera que esta herramienta se utilice únicamente para actividades de carácter laboral.

- Capacitación continua, para estar actualizado sobre los productos, software o tecnologías que presentan renovaciones o mejoras, y sobre las nuevas que se lanzan al mercado.

BIBLIOGRAFIA

- JENNY PONTON Y ALFREDO SANTILLAN. (2008). Ciudad Segura 2. Quito- Ecuador
- RETIE: REGLAMENTO TECNICO DE INSTALACIONES ELECTRICAS
- RETILAP: REGLAMENTO TECNICO DE ILUMINACION Y ALUMBRADO PUBLICO
- Manual de Requerimientos frecuentes de la Superintendencia de Vigilancia y Seguridad Privada
- Decreto 356 de 1994
- Protocolo de Vigilancia Electrónica. Superintendencia de Vigilancia y Seguridad Privada
- USER MANUAL DVR
- USER MANUAL IR HIGH SPEED DOME CAMERA
- Guía de instalación y Formato de Programación ADEMCO VISTA- 12 LA, HONEYWELL
- Guía de instalación y Formato de Programación ADEMCO VISTA- 48 LA, HONEYWELL L
- Guía de instalación Sistema de alarma autónomo inalámbrico v1.0 DSC POWER SERIES
- Manual de instalación DSC Power 864 SECURITY SISTEM
- Guía de instalación y configuración Sistemas de seguridad Lynx Plus
- Manual GPRS LX
- AXTRAX NG SOFTWARE MANUAL

INFOGRAFIA

http://www.flacsoandes.edu.ec/libros/digital/49668.pdf

http://www.rnds.com.ar/articulos/037/RNDS_140W.pdf

http://www.monografias.com/trabajos/cctelevis/cctelevis.shtml

http://seguridadig.com/historia-del-circuito-cerrado-de-television-cctv/

http://www.soloseguridad.net/preguntas/las-imagenes-de-una-camara-de-seguridad-son-nitidas

http://www.gsabogal.com/paginaahd/indexahd.html

http://www.seguridadsos.com.ar/dvr/

http://www.nexxtsolutions.com/co/cable-utp-cat6-en-bobina

http://deredes.net/redes-inalambricas-principales-protocolos/

http://ieeestandards.galeon.com/aficiones1573328.html

http://ieeestandards.galeon.com/

http://datateca.unad.edu.co/contenidos/301120/2014_II_LECCION_EVALUATIVA1.pdf

http://www.axis.com/cl/es/glossary/network-video

http://www.abus.com/es/Guia/Proteccion-antirrobo/Sistemas-de-alarma/Historia-de-los-sistemas-de-alarma

http://www.luisgyg.com/blog/2013/08/22/tip-gmsi-que-son-los-contactos-magneticos/

http://losvigilantesdeseguridad.org/vigilantes.html

http://www.rnds.com.ar/articulos/045/RNDS_152W.pdf

http://www.aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=500

http://www.ibrugor.com/blog/apache-http-server-que-es-como-funciona-y-para-que-sirve/

http://www.esepestudio.com/noticias/que-es-mysql

http://php.net/manual/es/intro-whatis.php

ANEXOS


NanoBridge M | Datasheet
NanoBridge® M
High-Performance airMAX® Bridge
Models: NBM9, NB-2G18, NBM3, NBM365, NB-5G22, NB-5G25
High Performance, Long Range
Completely Integrated CPE in Antenna Feed
Easy Assembly and Installation
UBIQUITI NETWORKS

Models

NanoBridge M9

Model	Frequency	Gain
NBM9	900 MHz	10.6 - 11.3 dBi

NanoBridge M2
NanoBridge M5

Model	Frequency	Gain
NB-2G18	2.4 GHz	18 dBi
NB-5G22	5 GHz	22 dBi
NB-5G25	5 GHz	25 dBi

NanoBridge M3
NanoBridge M365

Model	Frequency	Gain
NBM3	3.3 - 3.7 GHz	21.5 - 22.5 dBi
NBM365	3.65 - 3.675 GHz	21.5 - 22.5 dBi

Specifications

System Information			
Model	NBM9	NB-2G18/NB-5G22/NB-5G25	NBM3/NBM365
Processor Specs	Atheros MIPS 24KC, 400 MHz	Atheros MIPS 24KC, 400 MHz	Atheros MIPS 24KC, 400 MHz
Memory	64 MB SDRAM, 8 MB Flash	32 MB SDRAM, 8 MB Flash	32 MB SDRAM, 8 MB Flash
Networking Interface	(1) 10/100 Ethernet Port	(1) 10/100 Ethernet Port	(2) 10/100 Ethernet Ports

Regulatory/Compliance Information				
Model	NBM9	NB-2G18/NB-5G22/ NB-5G25	NBM3	NBM365
Wireless Approvals	FCC, IC	FCC, IC, CE	–	FCC
RoHS Compliance	Yes			

Physical/Electrical/Environmental			
Model	NBM9	NB-2G18/NB-5G22/NB-5G25	NBM3/NBM365
Dimensions (mm)	543 x 440 x 725	NB-2G18: 400 diameter NB-5G22: 326 mm diameter NB-5G25: 400 mm diameter	492 x 440 x 705
Weight (Dish and Mount Included)	5.098 kg	NB-2G18: 2.346 kg NB-5G22: 1.904 kg NB-5G25: 2.304 kg	NBM3: 4.656 kg NBM365: 4.660 kg
Power Supply	24V, 1A PoE	24V, 0.5A PoE	24V, 0.5A PoE
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)	Passive PoE (Pairs 4, 5+; 7, 8 Return)	Passive PoE (Pairs 4, 5+; 7, 8 Return)
Max. Power Consumption	6.5 W	5.5 W	8 W
Gain	10.6 - 11.3 dBi	NB-2G18: 18 dBi NB-5G22: 22 dBi NB-5G25: 25 dBi	21.5 - 22.5 dBi
LEDs	(1) Power, (1) LAN, (4) WLAN	(1) Power, (1) LAN, (4) WLAN	(1) Power, (2) LAN, (4) WLAN
Wind Loading	105 lbf @ 125 mph	NB-2G18: 77 lbf @ 125 mph NB-5G22: 45 lbf @ 125 mph NB-5G25: 77 lbf @ 125 mph	105 lbf @ 125 mph
Wind Survivability	125 mph		
LEDs	(1) Power, (1) LAN, (4) WLAN		
Signal Strength LEDs	Software-Adjustable to Correspond to Custom RSSI Levels		
Enclosure	Outdoor UV Stabilized Plastic		
Mounting	Pole-Mount Kit Included		
Operating Temperature	-30 to 75° C		
Operating Humidity	5 to 95% Non-Condensing		
Shock & Vibration	ETSI300-019-1.4		

Operating Frequency Summary (MHz)					
Model	NBM9	NB-2G18	NBM3	NBM365	NB-5G22/NB-5G25
Worldwide	902 - 928	2402 - 2462	3370 - 3730	3650 - 3675	5170 - 5875
USA					5725 - 5850

GUIA DE USO

RADIO MOVIL MOTOROLA RADIUS M120

El radio móvil M120 usa una memoria no volátil para almacenar información del cliente. Si a determinada frecuencia, un código o canal local/ distancia necesita ser cambiarse, esto puede ser hecho con el uso de RADIO SERVICE SOFTWARE (RSS). La opción TIME-OUT TIMER puede ser deshabilitada o cambiada a cualquier duración desde 1 hasta 255 segundos. La configuración por defecto está en 60 segundos.

ENCENDER EL EQUIPO: La perilla de ON/ OFF es también la del volumen. Al girar la perilla media vuelta en el sentido de las manecillas del reloj, se prende sonando el tono de encendido y un led verde también se prende para indicar el último canal usado por el radio.

CONFIGURAR EL NIVEL DE VOLUMEN: Presionar el botón del monitor por dos segundos (el led indicador correspondiente se prendera). Se escuchará "ruido blanco" lo cual significa que el radio está en buenas condiciones. Ajustando la perilla de encendido se estabiliza el nivel de volumen. Al presionar nuevamente el botón del monitor, el equipo vuelve al modo receptor normal.

PARA RECIBIR: Esta la opción para escoger entre el canal 1 o 2 presionando el botón selector de canal. Los canales son mostrados por un led indicador de canal, de color verde. Para recibir una transmisión específica, la cual ha sido previamente programada con un código PL/ DPL, permanece en el canal seleccionado y espera para la transmisión (radio en modo PL/ DPL). Esto solo permite escuchar la transmisión predeterminada. Para recibir todas las transmisiones en un canal seleccionado, se presiona el boto del monitor o descolgar el micrófono enganchado. El led del monitor se encenderá y el radio ahora estará en "modo monitor". Para volver al "modo PL/ DPL", se debe presionar el botón del monitor otra vez o colocar de vuelta a su lugar, al micrófono. Esto volverá a dejar el radio para recibir solamente la transmisión predeterminada de la que se habló anteriormente.

PARA TRANSMITIR: Se puede escoger entre el canal 1 o 2, presionando el botón selector de canal. Los canales son mostrados por un led indicador de canal de color verde. Antes de la transmisión, hay que asegurarse que el canal está vacío. Visualmente, se puede verificar eso gracias al led TRANSMIT/ BUSY con lo que se ve que hay una transmisión en el canal seleccionado. También se puede escuchar una transmisión, tomando el micrófono. Una vez el canal está desocupado, mantenga presionado el botón PUSH TO TALK (PTT) a un lado del micrófono y hable despacio y claramente. El led TRANSMIT/ BUSY permanecerá en rojo hasta que PTT este suelto para indicar que ya "esta al aire".

SERVIBOY	**REGISTRO DE VISITA DE MANTENIMIENTO, SOPORTE TÉCNICO E INSTALACIÓN**

CLIENTE: _____ **Cel. _____**

Dirección: _____ **FECHA: _____**

MARCA CAMARAS: _____ **MARCA DVR: _____**

MANTENIMIENTO: _____

_____

_____

_____

INSTALACIÓN: _____

_____

_____

ASIGNACION DE USUARIOS Y CLAVES

EQUIPO_____ USUARIO_____ CONTRASEÑA_____

EQUIPO_____ USUARIO_____ CONTRASEÑA_____

EQUIPO_____ USUARIO_____ CONTRASEÑA_____

_____ _____

FIRMA TECNICO RESPONSABLE **FIRMA USUARIO**

_____

Vo Bo GERENTE OPERATIVO

SERVIBOY	**REGISTRO DE VISITA DE MANTENIMIENTO, SOPORTE TÉCNICO E INSTALACIÓN**

CLIENTE: _____ **Cel.** _____

No. Cuenta: _____ **FECHA:** _____

MARCA PANEL_____ **COMUNICACIÓN:** ◯ **RADIO** ◯ **GPRS** ◯ **TELEFONO**

MANTENIMIENTO: _____

_____

_____

_____

INSTALACIÓN: _____

_____

_____

ASIGNACION DE USUARIOS Y CLAVES

POSICION_____ **NOMBRE**_____ **CC**_____

CARGO_____ **TELEFONO**_____ **CONTRASEÑA**_____

POSICION_____ **NOMBRE**_____ **CC**_____

CARGO_____ **TELEFONO**_____ **CONTRASEÑA**_____

POSICION_____ **NOMBRE**_____ **CC**_____

CARGO_____ **TELEFONO**_____ **CONTRASEÑA**_____

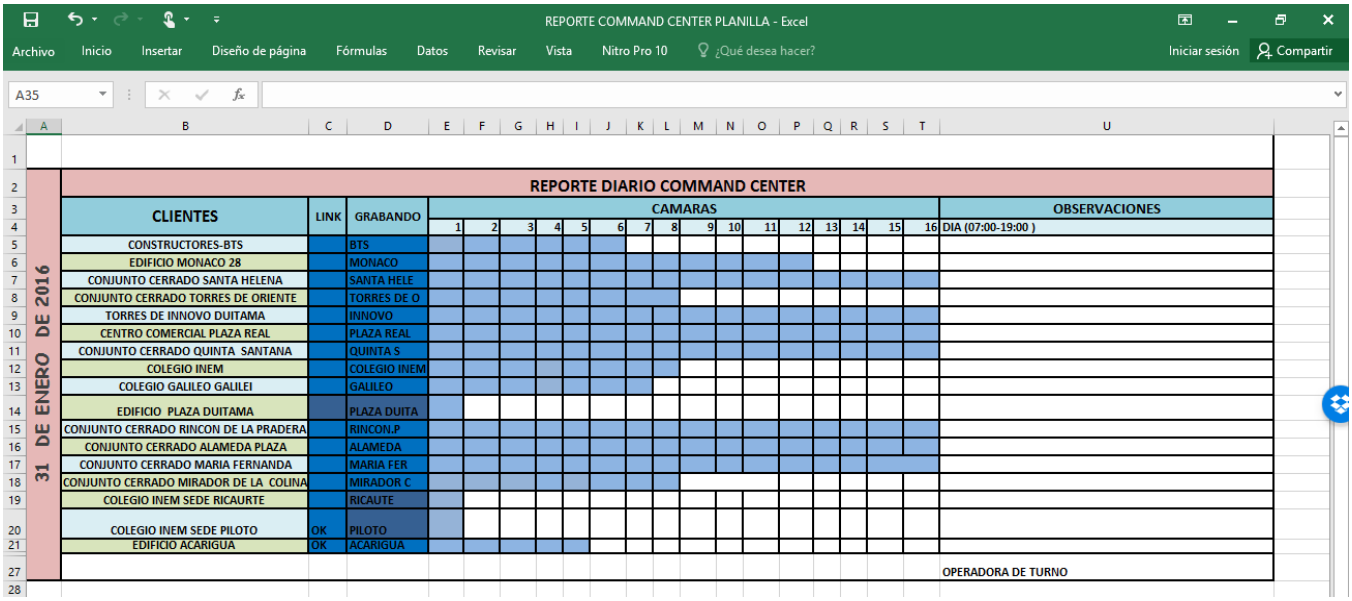
_____ _____

FIRMA TECNICO RESPONSABLE **FIRMA USUARIO**

_____

Vo Bo GERENTE OPERATIVO

PLANILLA EN DOCUMENTO DE EXCEL, CREADA PARA REALIZAR EL REPORTE DE LAS FALLAS TECNICAS DEL COMMAND CENTER, E INFORMARLAS AL DEPARTAMENTO DE INGENIERIA



REPORTE COMMAND CENTER PLANILLA - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Nitro Pro 10 ¿Qué desea hacer? Iniciar sesión Compartir

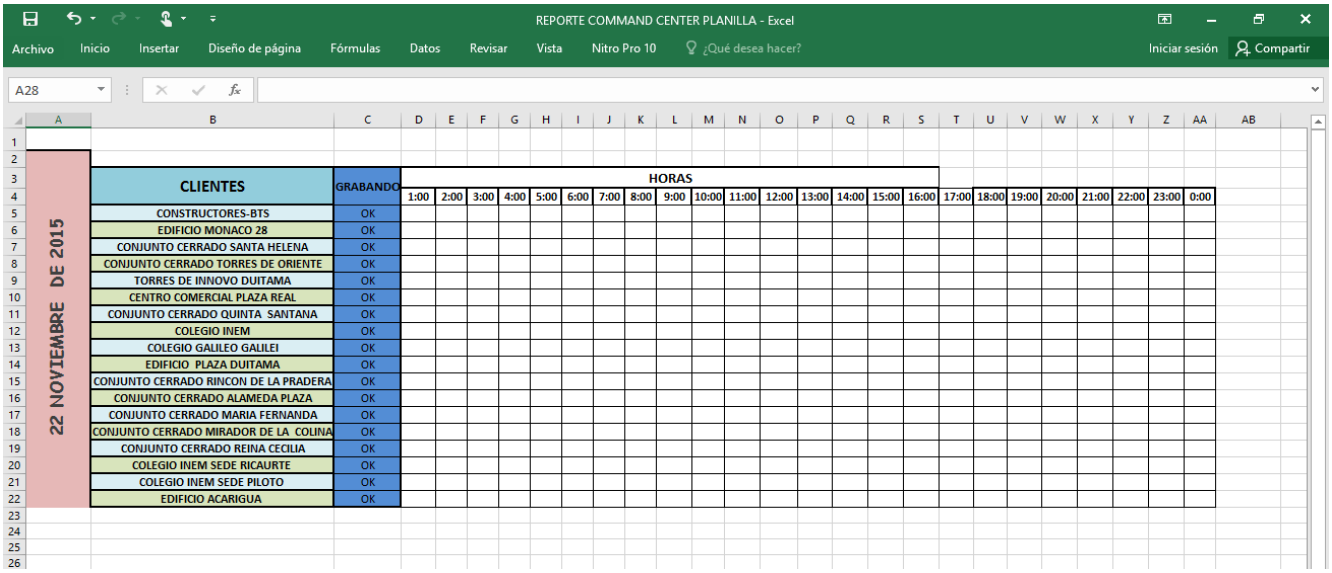
A35

REPORTE DIARIO COMMAND CENTER

31 DE ENERO DE 2016

CLIENTES	LINK	GRABANDO	CAMARAS 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	OBSERVACIONES
CONSTRUCTORES-BTS		BTS																	DIA (07:00-19:00)
EDIFICIO MONACO 28		MONACO																	
CONJUNTO CERRADO SANTA HELENA		SANTA HELE																	
CONJUNTO CERRADO TORRES DE ORIENTE		TORRES DE O																	
TORRES DE INNOVO DUITAMA		INNOVO																	
CENTRO COMERCIAL PLAZA REAL		PLAZA REAL																	
CONJUNTO CERRADO QUINTA SANTANA		QUINTA S																	
COLEGIO INEM		COLEGIO INEM																	
COLEGIO GALILEO GALILEI		GALILEO																	
EDIFICIO PLAZA DUITAMA		PLAZA DUITA																	
CONJUNTO CERRADO RINCON DE LA PRADERA		RINCON.P																	
CONJUNTO CERRADO ALAMEDA PLAZA		ALAMEDA																	
CONJUNTO CERRADO MARIA FERNANDA		MARIA FER																	
CONJUNTO CERRADO MIRADOR DE LA COLINA		MIRADOR C																	
COLEGIO INEM SEDE RICAURTE		RICAUTE																	
COLEGIO INEM SEDE PILOTO	OK	PILOTO																	
EDIFICIO ACARIGUA	OK	ACARIGUA																	

OPERADORA DE TURNO



REPORTE COMMAND CENTER PLANILLA - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Nitro Pro 10 ¿Qué desea hacer? Iniciar sesión Compartir

A28

22 NOVIEMBRE DE 2015

CLIENTES	GRABANDO	HORAS 1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	0:00
CONSTRUCTORES-BTS	OK																								
EDIFICIO MONACO 28	OK																								
CONJUNTO CERRADO SANTA HELENA	OK																								
CONJUNTO CERRADO TORRES DE ORIENTE	OK																								
TORRES DE INNOVO DUITAMA	OK																								
CENTRO COMERCIAL PLAZA REAL	OK																								
CONJUNTO CERRADO QUINTA SANTANA	OK																								
COLEGIO INEM	OK																								
COLEGIO GALILEO GALILEI	OK																								
EDIFICIO PLAZA DUITAMA	OK																								
CONJUNTO CERRADO RINCON DE LA PRADERA	OK																								
CONJUNTO CERRADO ALAMEDA PLAZA	OK																								
CONJUNTO CERRADO MARIA FERNANDA	OK																								
CONJUNTO CERRADO MIRADOR DE LA COLINA	OK																								
CONJUNTO CERRADO REINA CECILIA	OK																								
COLEGIO INEM SEDE RICAURTE	OK																								
COLEGIO INEM SEDE PILOTO	OK																								
EDIFICIO ACARIGUA	OK																								