DISEÑO DE SISTEMA DE SEGURIDAD ELECTRÓNICO PARA EL REGISTRO, AVISO Y CONTROL EN TIEMPO REAL DE INCIDENTES DE SEGURIDAD COMUNITARIA PARA LA EMPRESA DARPA CEROS Y UNOS DE COLOMBIA SAS. (FSE - FRENTE DE SEGURIDAD ELECTRÓNICO)

VÍCTOR MANUEL ZAMBRANO HERNÁNDEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

FACATATIVÁ, CUNDINAMARCA

2021

DISEÑO DE SISTEMA DE SEGURIDAD ELECTRÓNICO PARA EL REGISTRO, AVISO Y CONTROL EN TIEMPO REAL DE INCIDENTES DE SEGURIDAD COMUNITARIA PARA LA EMPRESA DARPA CEROS Y UNOS DE COLOMBIA SAS. (FSE - FRENTE DE SEGURIDAD ELECTRÓNICO)

VÍCTOR MANUEL ZAMBRANO HERNÁNDEZ

Proyecto de Grado para optar el título de

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

Docente

Mg. JOEL CARROL

UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

FACATATIVÁ, CUNDINAMARCA

2021

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Facatativá, Marzo de 2021

DEDICATORIA

Doy gracias a Dios y la vida, el haberme dado la oportunidad de poder cumplir y culminar un sueño más… agradezco de manera especial a mi familia mi madre, mis hermanos, quienes han estado incondicionalmente para brindarme el apoyo en el momento en el que más he requerido. A mis hijos Luisa Fernanda y Manuel Francisco, quienes son el motor de mi vida y mi razón de ser y de luchar cada día, por ellos los sacrificios valen la pena, pues su amor y presencia en mi vida son una plenitud. De igual manera una vez más gracias señores tutores, porque sin el conocimiento y apoyo que recibí de ustedes no habría sido posible avanzar. Hoy puedo decir con total franqueza que los sueños se cumplen y hoy mí se convierte en realidad.

Víctor Manuel Zambrano Hernández

AGRADECIMIENTOS

Quiero agradecer primero a Dios que me ha brindado la oportunidad de adelantar esta especialización, de igual manera agradezco a todos y cada uno de los tutores de la UNAD universidad Abierta y a Distancia por su acompañamiento y paciencia para conmigo, por el tiempo dedicado para construir el mejor resultado y por supuesto por sus aportes valiosos que sumaron para perfeccionar y enriquecer el fin. A mi familia por su apoyo e incondicional amor y apoyo en realidad hoy me siento honrado por el tiempo que me dieron, la confianza y mejor ambiente para un feliz desarrollo.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: Información o sistema que se relaciona con el tratamiento de esta y que tiene valor para una organización.

ADMINISTRACION ELECTRÓNICA: Se relaciona con la prestación de servicios haciendo uso de medios telemáticos que se fundamenta en el decreto 1413 de 2017.

AMENAZA: Evento que en el momento de ocurrir puede presentar un impacto negativo sobre un activo de información.

ALARMA: Mecanismo de alerta.

CONFIDENCIALIDAD: Es una propiedad que tiene la información, la cual garantiza que esta sea accedida solamente por las personas que estén autorizadas.

DISPONIBILIDAD: Suficiencia que debe tener la información o un servicio para ser accedida y usada por los usuarios que estén autorizados.

INCIDENTE DE SEGURIDAD: Evento que puede afectar la Disponibilidad, confidencialidad e integridad de la información de una organización.

INTEGRIDAD: Garantiza la exactitud de los datos, teniendo presente el aseguramiento de la información de tal forma que no se presente perdida o alteración de esta.

MICROCONTROLADOR: Circuito integrado que se compone de varios bloques.

SEGURIDAD ELECTRÓNICA: Es el mecanismo que permite brindar seguridad a un sector determinado a través de la tecnología.

SEGURIDAD: Se entiende por la confianza y tranquilidad que brinda algo o alguien.

SISTEMA: Es la agrupación de normas o reglas para realizar una actividad determinada.

TARJETA: Objeto rectangular en el cual se logran diseñar sistemas.

TECNOLOGÍA: Es la agrupación de diferentes recursos e instrumentos que son utilizados para realiza un sector determinado.

INTRODUCCIÓN

Este proyecto tiene como finalidad desarrollar un Sistema Electrónico de seguridad el cual permita brindar a los beneficiarios y comunidades seguridad y tranquilidad teniendo en cuenta que se realizará a través del sistema un trabajo mancomunado con la Policía Nacional, donde se busca mitigar y lograr una reacción de la policía más eficiente frente a los delitos más frecuentes como los son lesiones personales, hurtos, piratería terrestre, hurto a entidades financieras y abigeato, los cuales son conductas criminosas en donde la fechoría o delincuencia es causada por dos tipos de victimarios, los Individuales quienes son los que actúan como delincuencia común, y victimarios grupales, denominados como delincuencia organizada.

Así mismo, es de resaltar que, con este Sistema Electrónico de Seguridad, se brindará muchos beneficios a la sociedad dentro de los cuales encontramos brindar confianza y seguridad, disminución de hurtos, preservación de la integridad de las personas en el municipio de Facatativá, atenúa la violencia, reduce el índice de criminalidad y finalmente contribuye al bienestar social.

Es de anotar que en términos de ciberseguridad y visto desde la Norma ISO 27001:2013, este proyecto contribuye en dar respuesta a los dominios A.9. de control de acceso, A.11. de seguridad física y del entorno, A.12. de seguridad de la información. A.16 de gestión de incidentes de seguridad de la información y el A.18. de cumplimiento, teniendo presente estos apuntan en brindar: requisitos del negocio para el control de acceso en una comunidad, organización pública o privada o cualquier zona o espacio que deba ser monitoreado, la gestión de los accesos a usuario ya que desde la generación de las alertas del sistema se puede en tiempo

real detectar accesos no deseados o irregulares. En conjunto con el uso de la tecnología de las organizaciones a partir de sistemas de circuito cerrado, permite proteger áreas seguras; donde el sistema genera información que aporta en la generación de reportes de eventos de seguridad y en el dar cumplimiento a los requisitos legales y contractuales que emanen de la información recolectada en el sistema FSE.

ABSTRACT

The purpose of this project is to develop an Electronic Security System which allows to provide the beneficiaries and communities with security and tranquility, taking into account that joint work with the National Police will be carried out through the system, which seeks to mitigate and achieve a reaction of the most efficient police in the face of the most frequent crimes such as personal injury, theft, land piracy, theft from financial entities and cattle rustling, which are criminal behaviors where the wrongdoing or delinquency is caused by two types of perpetrators, the Individuals who they are those who act as common criminals, and group perpetrators, known as organized crime.

Likewise, it is noteworthy that, with this Electronic Security System, many benefits will be provided to society, within which we find providing trust and security, reduction of thefts, preservation of the integrity of people in the municipality of Facatativá, attenuates violence reduces the crime rate and ultimately contributes to social welfare.

It should be noted that in terms of cybersecurity and seen from the ISO 27001: 2013 Standard, this project contributes in responding to the A.9 domains. access control, A.11. of physical and environmental security, A.12. information security. A.16 on information security incident management and A.18. of compliance, bearing in mind these aim to provide: business requirements for access control in a community, public or private organization or any area or space that must be monitored, the management of user access since from the generation of the System alerts can in real time detect unwanted or irregular accesses. Together with the use of the organizations' technology from closed circuit systems, it allows to protect safe areas; where the system generates information that contributes in the generation of reports of security events and in complying with the legal and contractual requirements that emanate from the information collected in the FSE system.

Palabras Claves

Confidencialidad, Controles, Red de apoyo, Seguridad Física, Seguridad Perimetral.

Confidentiality, Controls, Support Network, Physical Security, Perimeter Security.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 PRESENTACIÓN

Debido a la inseguridad ciudadana, Colombia es denominado como el país más conflictivo de Latinoamérica, así lo afirman las conclusiones del índice de paz elaborado por el Institute for Economics and Peace, donde afirma que Colombia ocupa el puesto 150[1] entre 162 naciones que compara el índice global de paz (IGP) y que mide adicionalmente otros 23 indicadores entre los cuales se encuentran la seguridad interna, la participación del país en conflictos y el grado de militarización que tiene.[2]

Para el año 2015 se presentó un aumento de 1,5%, respecto al año anterior, donde las personas mayores de 15 fueron víctimas de por lo menos un delito, según estudio que se realizó en 28 ciudades, por lo anterior la tasa de Victimización fue de 17,3%.

Ahora bien, al preguntar sobre el hurto a residencias en la misma muestra se evidencia un aumento del 0.5%, donde el año anterior presentó un porcentaje equivalente al que el 3,1% reporta haber sufrido este hecho, generando un aumento de 0,5 puntos porcentuales con respecto al año anterior 2,7%.

---

[1] LA REPÚBLICA. [Sitio web]. Bogotá. [Consulta: 31 de julio 2019]. Disponible en: https://www.larepublica.co/globoeconomia/la-inseguridad-ciudadana-hace-de-colombia-el-pais-mas-conflictivo-de-america-latina-2136581

[2] EL TIEMPO. [Sitio web]. Bogotá. [Consulta: 28 de julio 2019]. Disponible en Obtenido de http://www.eltiempo.com/archivo/documento/CMS-15965877

Si observamos las estadísticas respecto al delito de hurto, se evidencia el aumento, por tal razón la creación de un Sistema Electrónico de Seguridad que tenga comunicación directa con la Estación de Policía del municipio permitirá una acción inmediata, rápida y eficaz, brindando confianza y seguridad en los diferentes sectores.

De la misma forma se observa que el 12, 6 % del total de personas propietarias de algún vehículo denunció haber sufrido un hurto del vehículo o de alguna a parte o accesorio de este; referente al factor de peleas y riñas el 2,1% de las personas mayores a 15 años declaran haber estado implicados en este acto durante 2015.

Para finalizar, se realiza el análisis para el delito de extorsión o intento de extorsión, en la cual se evidencia que se presenta un aumento equivalente al 0.3 respecto al año inmediatamente anterior, es decir en el 2014 la tasa fue de 1,0%, mientras que para el año 2015 la tasa se ubicó en 1,3%.[3], de esta manera se demuestra que este delito va en crecimiento para lo cual las autoridades competentes deben realizar los ajustes y programas preventivos que permitan la reducción de los índices anteriores.

Ahora bien, esta problemática social está afectando a todo el territorio nacional aunque su mayor aumento es reflejado en las ciudades principales, lo cual afecta de manera directa la calidad de vida de la ciudadanía, en la parte social y económica, teniendo en cuenta que las personas pierden la tranquilidad, así como la armonía; es por tal razón, que el diseño, creación e implementación de un Sistema Electrónico de Seguridad podría ayudar a disminuir estos porcentajes

[3] DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. [Sitio web]. Bogotá: DANE. [Consulta: 8 de agosto 2019]. Disponible en : http://www.dane.gov.co/files/investigaciones/poblacion/convivencia/2016/Bol_ECSC_2016.pdf

generando mayor seguridad en los diferentes sectores, brindando de esta manera una armonía y mejoramiento continuo de la calidad de vida de los beneficiarios y sus sectores aledaños. De igual manera desde la Ingeniería, es un aporte a la seguridad de los territorios, pues se demuestra con los Sistemas Electrónicos una forma inteligente de comunicación que permite agilidad y eficacia en los procesos de Seguridad Ciudadana.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo garantizar la eficiencia en los canales de comunicación que la comunidad tiene con los entes de seguridad a través de un adecuado diseño de un sistema de seguridad electrónico que brinde información de eventos en tiempo real, con el fin de poder dar respuesta a estos?

2. JUSTIFICACIÓN

"Los derechos, las garantías y los deberes de los derechos fundamentales" [4], que incluye la carta magna son el derecho a la vida, a la igualdad, a la libertad y a la intimidad. Teniendo en cuenta esto, la inseguridad atenta y vulnera de manera directa estos derechos, para contrarrestar este fenómeno, el estado ha implementado un modelo nacional de vigilancia comunitaria, el cual está dirigido por la Policía Nacional de Colombia y estipulado por la ley "1453 de 2011"[5] , pero esto no es suficiente, pues el delito y las contravenciones que se generan día tras día, presentan índices muy altos, esto afecta negativamente el desarrollo de las personas y la comunidad en general.

Teniendo en cuenta lo anteriormente expuesto, las personas en busca de lograr una tranquilidad y seguridad han buscado otro tipo de herramientas donde los Sistemas Electrónicos juegan un papel importante teniendo en cuenta que la tecnología en estos casos logrará ayudar a mitigar y disminuir los riesgos que se vienen presentando frente al tema de inseguridad para la comunidad por lo que permiten una comunicación acertada con las autoridades quienes a su vez tendrán una reacción inmediata a los actos delictivos como lo son el hurto, el consumo de sustancias psicoactivas, los homicidios, feminicidios entre otros.

[4] COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1453 (24, Junio, 2011). Por lo cual se reforma el Código Penal el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. En: Diario oficial. Junio, 2011. Nro. 48.110 .p.1-15.

[5] COLOMBIA, CORTE CONSTITUCIONAL. CONSTITUCIÓN POLÍTICA DE COLOMBIA. (1991). En: Constitución Colombia

Por tal razón, este proyecto también permite la inclusión y a su vez contribuye a la alfabetización digital de las personas involucradas en los frentes de seguridad y a su vez al manejo de esta herramienta

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de seguridad electrónico haciendo uso de tecnologías GSM y GPRS y PCB que registre y comunique incidentes de seguridad comunitaria para la empresa DARPA CEROS Y UNOS DE COLOMBIA.

3.2 OBJETIVOS ESPECÍFICOS

- Diseñar el Sistema de Seguridad Electrónico FSE (Frente de Seguridad Electrónico).

- Presentar de manera funcional el sistema de seguridad electrónico FSE (Frente de Seguridad Electrónico).

- Realizar pruebas de funcionalidad del prototipo con el fin de proteger la integridad de las personas y de los bienes físicos y tecnológicos de las mismas.

4. MARCO REFERENCIAL

4.1 MARCO CONCEPTUAL

En este apartado del documento se realizará una compilación de diferentes conceptos y términos relacionados con los sistemas de seguridad electrónica y sus componentes.

4.1.1 Sistemas de Seguridad Electrónica Un sistema es una combinación de componentes (recursos) que operan colectivamente con el fin de alcanzar el cumplimiento de un objetivo específico. Por lo tanto, está compuesto por diferentes partes que llevan a cumplir el objetivo principal del sistema seguridad. Ahora bien, cuando un componente o parte de un sistema alcanza un nivel de complejidad se puede convertir también un sistema en sí; es decir, que de ser un componente o parte pasa a ser sistema a su vez estos sistemas que se denominan o llaman subsistemas, establecen una relación entre sí la cual constituye el funcionamiento global del sistema principal[6].

Por lo tanto, se puede decir que un sistema de seguridad electrónica es una interconexión de redes, dispositivos y recursos donde su objetivo es garantizar la seguridad de las personas y su entorno advirtiéndolas de los diferentes peligros y presiones externas.[7]

[6] SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA. [Sitio web]. Bogotá [Consulta: 13 de agosto 2019]. Disponible en Obtenido de http://www.supervigilancia.gov.co

[7] Ibid.,

4.1.2 Clasificación de los sistemas de seguridad electrónica Para realizar la clasificación de los sistemas de seguridad electrónica (SSE) se tienen en cuenta dos criterios, el primero la totalidad de lugares a proteger y el segundo la ejecución del sistema.[8]

Respecto al primer criterio se puede decir que se divide en dos Sistemas locales y los sistemas distribuidos, donde un SSE local es aquel proyectado para brindar seguridad a un lugar específico, teniendo en cuenta las características del mismo; mientras que un SSE distribuido es la unión de varios SSE locales adaptados a cada lugar protegido y que además trabajan unidos a través de un sistema de Telecomunicación.[9]

4.1.3 GPRS que significa General Packet Radio Service y es una versión mejorada del GSM, que permite que exista y se dé la mensajería instantánea, de igual manera los servicios de mensajes cortos (SMS) y los mensajes multimedia (MMS) y así como el acceso al correo electrónico generando conectividad constante.[10]

4.1.4 WAP dispositivos inalámbricos, como lo son los teléfonos celulares y transceptores de radio, puedan tener acceso a Internet, y los diferentes servicios

[8] CEVALLOS, Gabriel. En: SEGURIDAD ELECTRÓNICA. [Sitio web]. Quito: Clasificación de los sistemas de seguridad electrónica. [Consulta: 2 de diciembre 2019]. Disponible en: https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-2-clasificacion-de-los-sistemas-de-seguridad-electronica

[9] Ibid.,

[10] BBC NEWS. [Sitio web]. Reino Unido. [Consulta: 21 de diciembre 2019]. Disponible en http://www.bbc.com/mundo/noticias-37247130

que brinda la conectividad en el cual está incluido el correo electrónico, la World Wide Web, grupos de noticias, y mensajería instantánea.[11]

De esta forma se logra evidenciar que este estándar técnico permite obtener información a través de la conectividad a internet.

4.1.5 THT Es una clase de tecnología donde se utilizan los agujeros que están impresos en las placas de los circuitos con el fin de llevar a cabo el ensamble de los diferentes elementos electrónicos y así diseñar puentes eléctricos entre una de las caras de la placa de montaje hacia la otra, por medio de un tubo conductor que generalmente es una combinación de zinc, cobre y plata, para impedir su oxidación y lograr su soldadura.[12]

4.1.6 Vigilancia electrónica Es la seguridad que se brinda a través de los medios tecnológicos, en las áreas residenciales, empresas, establecimientos comerciales, financieros, e industriales.[13]

Así mismo también se realiza vigilancia a través de Monitoreo de Alarmas, debido a que estas emiten información recibida y atendida por una Central de Monitoreo."[14] Y permite en tiempo real tener conocimiento de las diferentes

[11] TECHTARGET. [Sitio web]. Massachusetts. [Consulta: 11 de octubre 2019]. Disponible en: http://searchmobilecomputing.techtarget.com/definition/WAP

[12] PREZI. [Sitio web].Budapest. [Consulta: 23 de octubre 2019]. Disponible en: https://prezi.com/8ih96ob-bqh0/tecnologia-de-agujeros-pasantes-through-hole/

[13] Ibid.;

[14] Ibid.;

circunstancias o anomalías que se presenten y de esta manera lograr una reacción inmediata ante los hechos.

4.1.7 Sistema de alarma Es el mecanismo mediante el cual se informa a la comunidad en general o específica que algo anormal está pasando, que puede generar amenaza.

4.1.8 Alarma Es una señal o un aviso de alerta que sugiere y avisa sobre la ocurrencia real o inminente de un hecho que genera amenaza o de una circunstancia que denota peligro."[15]

4.1.9 Panel de Alarma Es el lugar donde se realiza la conexión de cada uno de los dispositivos y elementos que conforman la electrónica precisa mediante el cual se realiza el proceso de información del Sistema de alarma, de igual manera es donde se da la comunicación con la central de monitoreo o centro de control, convirtiéndolo en la parte principal de la alarma.[16]

4.2 MARCO CONTEXTUAL

En esta sección se pretende mostrar una visión general del sector de la seguridad en el municipio de Mesitas del Colegio, específicamente en lo que se refiere a la seguridad electrónica que es el tema de este proyecto.

[15] Ibid.;

[16] Ibid.;

El Municipio de El Colegio, es popularmente denominado o llamado Mesitas del Colegio, hace parte del departamento de Cundinamarca, debido a su cálido clima es un sector turístico.[17] Sus límites son: La Mesa, San Antonio del Tequendama, Anapoima, Tena, Viotá y Granada.[18]

La jurisdicción del municipio El Colegio está conformada por tres El Triunfo, Pradilla y La Victoria, los cuales presentan categoría de inspección de Policía.

Ahora bien, El municipio de El Colegio, como es reconocido así como otros sectores de Colombia, se han visto afectados por la Inseguridad que se vive actualmente, por las diversas razones dentro de las cuales encontramos la delincuencia común y la delincuencia Organizada, así como también el flagelo social del desempleo y los migrantes de Venezuela son algunos factores que en definitiva no se han logrado controlar y que por el contrario aumentan generando pánico entre la sociedad, debido a que el pie de fuerza que cubre el municipio parece insuficiente ante la inseguridad que se percibe. Es por tal razón que el Sistema Electrónico de Seguridad permite que se organicen las comunidades y la Policía realizando un trabajo mancomunado aprovechando las herramientas y beneficios que brinda este sistema donde se puede lograr una tranquilidad al saber y sentir que tanto la familia, el entorno y los bienes se encuentran protegidos por un sistema en línea con comunicación directa a la Policía Nacional.

[17] WIKIPEDIA CONTRIBUTORS. [Sito web]. [Consulta: 22 de octubre 2019]. Disponible en https://es.wikipedia.org/wiki/El_Colegio#Organizaci%C3%B3n_territorial

[18] Ibid.;

4.3 ANTECEDENTES

En la historia existen momentos claves que se recuerdan porque reflejan los aciertos y desaciertos que son consecuencia por hechos sucedidos a lo largo de la evolución humana, dentro de los cuales se encuentran, los inventos, las guerras, los acuerdos entre países; sin duda, todos son han sido importantes dentro la historia y evolución humana.

En este proyecto aplicado se expondrán las etapas de la nueva era en la seguridad y vigilancia electrónica de los lugares privados y públicos, en un orden cronológico.

Hacia el año 1942 una compañía norteamericana desarrolla un circuito cerrado de televisión para el ejército alemán, donde el objetivo era que este sistema de vigilancia hiciera rastreo de la expulsión de misiles V2. Mientras tanto en Norte América, el ejército de los Estados Unidos desarrollo un método similar en busca de lograr un rastreo a las pruebas nucleares desde una distancia apropiada, previniendo del riesgo de la radiación a las personas que realizaban este tipo de pruebas. Estos prototipos de sistemas fueron utilizados inicialmente solo por los gobiernos y sus ejércitos; posteriormente y después de varios años estos sistemas fueron comercializados a otras entidades con el fin de beneficiar a los ciudadanos del común y empresas privadas.

Para el año 1949 se comercializa el primer sistema de monitoreo, sin embargo, el sistema no contaba con muchos avances y hasta el año 1951 luego de varias mejoras se desarrolla una nueva tecnología la cual admitió grabar y almacenar las imágenes en una cinta de video que fue llamada VTR.

Posteriormente, la comercialización de los sistemas permitió que estos fueran utilizados en entidades públicas y militares, dándole un uso diferente al inicial y realizando monitoreo constante y permanente de los lugares creando seguridad adentro de sus instalaciones, sin embargo, las tasas de criminalidad e inseguridad no disminuyeron, pero este sistema permitía dar con el paradero de los delincuentes y por tal razón fueron de gran ayuda pues quedaba grabado el rostro o características físicas de los mismos, permitiendo su identificación y ubicación de una manera más fácil.

De igual manera el gobierno británico utilizó este tipo de sistemas para realizar el seguimiento al tráfico, así como también a algunas manifestaciones teniendo en cuenta que para esta época en la isla ocurrían muchos desordenes sociales e inseguridad, y viendo la efectividad del sistema de vigilancia le dieron utilización en otras áreas y con otros fines y por tal razón se instalan más cámaras en diferentes sectores de control[19].

Los iniciales sistemas de vigilancia electrónica operaban de manera análoga a través de un cable coaxial (cobre) el cual emitía una señal elíptica entre + 0,5 y -0,5 voltios, estas cámaras remitían una indicación al monitor de control a través de este cable pero las imágenes eran de mala calidad y distorsionadas debido que las grabadoras no eran digitales y las que se utilizaban lo hacían por medio de cintas de video VHS O VTR teniendo en cuenta que estas cintas brindaban una mejor calidad de la imagen aunque no era del todo nítida.

[19] ENTEL CHILE. S.A. [Sitio web]. Santiago de Chile. [Consulta: 2 de noviembre 2019]. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P11800567291273156038130

Hacia el año 1.996 se crea la primera cámara IP la neyete 200 por una compañía denominada Axis y desde entonces se han visto reflejadas diferentes mejoras a los sistemas electrónicos de seguridad por parte de la informática, tales como son la grabación digital de alta calidad, vigilancia de las cámaras a través de la red o internet, el VMD (Video Motion Detection), velocidad a la hora de buscar situaciones específicas en las grabaciones, así como también sistemas que interactúan con la activación de redes, candados de seguridad etc.

Es de esta manera como en muchos lugares del mundo estos sistemas fueron utilizados donde la inseguridad estaba por encima de las autoridades y la ayuda de las grabaciones permitía identificar las caras o características de los facinerosos permitiendo la captura o detención de estos.

Teniendo en cuenta lo anterior, se puede evidenciar que el avance de estos sistemas de seguridad electrónicos ha sido muy acertado y cada día estos se convierten en el mejor aliado para el monitoreo y seguimiento de los espacios privados y públicos alrededor del mundo, generando seguridad a las personas que están a su alcance[20].

4.4 MARCO LEGAL

Para el presente proyecto se deben tener en cuenta las normas que en Colombia rigen el tema de Ciber seguridad las cuales se presentan a continuación:

4.4.1 Ley 1273 del 5 de enero de 2009 Ley mediante la cual se realiza una modificación al Código Penal y se incluye la protección de la información y de los

[20] Ibid.,

datos de igual manera se resguardan integralmente todos los sistemas que manejen las tecnologías de la información y las comunicaciones.[21]

Con esta ley el gobierno busca generar la protección de la información y de los datos, de igual manera estipula cuales son los delitos informáticos.

4.4.2 Ley 1341 del 30 de julio de 2009 Por medio de esta ley se conceptualizan y especifican los conceptos y principios de la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, además se crea la Agencia Nacional del Espectro.[22]

4.4.3 Artículo 269B Obstaculización ilegítima de sistema informático o red de telecomunicación.

Este artículo hace referencia a que está prohibido obstaculizar o impedir el normal funcionamiento a un sistema informático, a una red de telecomunicaciones o a las bases de datos informáticas contenidas en los sistemas informáticos, so pena prisión equivalente entre cuarenta y ocho (48) a noventa y seis (96) meses y además una sanción económica de 100 a 1000 salarios mínimos legales."[23]

[21] SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [Sitio web]. Bogotá. [Consulta: 10 de enero 2020]. Disponible en: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

[22] Ibid.;

[23] DACCACH, José. En: DELTA ASESORES. [Sitio web]. Ley de delitos informáticos en Colombia. [Consulta: 23 de enero 2020]. Disponible en https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Hace mención a las sanciones y multas que se aplican en el caso de obstaculizar el acceso a un sistema informático, además hace referencia a las diferentes multas por tener una conducta inapropiada del uso de estos sistemas.

4.4.4 Artículo 269E: uso de software malicioso Hace referencia a las sanciones y multas que se generan por el uso inadecuado del software, así como de comercialización de programas dañinos como virus, que afecten el funcionamiento normal de los equipos y sistemas, además puede ir a presión con una pena desde cuarenta y ocho (48) hasta noventa y seis (96) meses y sanción económica de 100 a 1000 salarios mínimos legales mensuales vigentes.[24]

4.4.5 CONPES 3854 – 2016 Política Nacional de Seguridad Digital Es la política Pública que protege la seguridad informática, además vigila y protege contra la explotación sexual, la pornografía, entre otros delitos cibernéticos.[25]

4.5 MARCO TEÓRICO

El presente proyecto aplicado tiene la finalidad de diseñar un sistema de seguridad electrónico que tiene como fin lograr la minimización de los delitos locales en el municipio de El Colegio.

Este sistema es una alarma digital con funciones de transmisión de datos, que funciona con tecnologías GSM y GPRS, de igual manera el sistema WAP, todo esto para que sea capaz de operar en las 4 bandas de telefonías móviles en el país. Para

[24] Ibid.;

[25] DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. [Sitio web]. Bogotá: DANE. [Consulta: 9 de marzo 2020]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

lograr la fabricación de esta alarma se desarrolló una tarjeta PCB con tecnología THT; un módulo celular de superficie que tiene como función recibir y enviar mensajes de texto, el cual, en la fase de realización de pruebas e implementación se realizó en el municipio de Mesitas del Colegio; un microcontrolador PIC16F88A, el cual es un circuito integrado que cuenta en su interior con una CPU, unidades de memoria (RAM y ROM), así como puertos de entrada y salida periféricos. La interconexión de estas partes en el interior del microcontrolador, forman en conjunto que se denomina una microcomputadora.

Por lo anterior, se puede confirmar que el microcontrolador, es una microcomputadora completa encapsulada en un circuito integrado, es básicamente el cerebro del equipo a desarrollar ya que es el que hace la interacción y controla todas las acciones, una antena de 3 DBI con la cual se garantiza la señal y una electrónica básica como resistencias, también diodos, reguladores de voltaje, relevos electromecánicos, borneras, conectores para sim card y demás recursos que permitirán el buen funcionamiento del sistema.

4.5.1 La seguridad, una necesidad básica del ser humano Según la Pirámide de Maslow o Jerarquía de las necesidades humanas, para el ser humano la seguridad es indispensable debido a que al sentirse seguro y protegido le genera mayor satisfacción lo cual, permite el desarrollo del cumplimiento de metas, necesidades y los deseos más supremos[26].

[26] UNIVERSIDAD DE ORIENTE. [Sitio web]. Puebla; Universidad de Oriente. [Consulta: 13 de marzo 2020]. Disponible en: https://www.academia.edu/8733930/UNIVERSIDAD_DE_ORIENTE-_PUEBLA

Así mismo, Abraham Maslow afirma, que las necesidades del ser humano conforman una escala o pirámide de cinco pilares, donde los cuatro primeros se agrupan como “necesidades de déficit” (primordiales); y el último pilar lo denomina finalmente como la “autorrealización”, “motivación de crecimiento”, o “necesidad de ser”[27].

Es decir, que, de acuerdo con lo anterior, la seguridad hace parte de las necesidades primordiales del ser humano, de ahí que el desarrollo de los Sistemas de Seguridad Electrónica le permitirá satisfacer la misma.

El ser humano, en busca de la superación siempre aspira a satisfacer más allá de las necesidades elementales, es decir, todos deseamos a satisfacer necesidades superiores[28]. Por tal razón, una vez se has satisfechas las necesidades primarias, vienen posteriormente la satisfacción de las necesidades de seguridad y protección, que contienen:

- Seguridad física, la cual busca proteger la integridad física del cuerpo y de la salud.

- Protección los bienes y activos como lo son casa, carro, dinero, etc.

- Necesidad de obtener un lugar donde vivir (protección).

Por otra parte, Bronislaw Malinowski, en su teoría antropológica social, sustenta de igual manera que la seguridad hace parte de las siete necesidades básicas a saciar

[27] Ibid.;

[28] Ibid.;

por parte del ser humano, y que demás se ubica a continuación de la reproducción, nutrición, y los bienestares físicos como lo son la vivienda y el vestido.

En conclusión, se puede decir que el ser humano actúa por la presión de lograr satisfacer sus necesidades elementales o básicas, donde la seguridad como se mencionó anteriormente hace parte de una de ellas. Lo cual es notable desde el inicio o evolución del hombre donde desde sus orígenes, los primeros pobladores, se agruparon en tribus con el fin de protegerse entre ellos de animales grandes y feroces, y en la actualidad con los avances tecnológicos y científicos se ha permitido lograr crear sistemas de protección no sólo a las personas sino a sus pertenencias, generando seguridad en los entornos.

5. DISEÑO METODOLOGICO

La metodología que se a aplicar en el desarrollar este proyecto es de índole cuantitativa y cuantitativa ya que se utiliza la recolección, el análisis de datos y la sistematización de la información. Visto desde la metodología planteada, surge la necesidad de trabajar a partir de las siguientes fases que se ven reflejadas en la construcción del documento:

Fase I: Análisis de la situación de seguridad presentada en el municipio de El Colegio para el año 2017.

Recursos usados.

- Observación y visitas a las comunidades del municipio, donde se evidencio la inseguridad y la falta de apoyo de los entes de seguridad del municipio.

Fase II: Encuentros con la comunidad donde se plantean algunas estrategias tecnológicas para fortalecer la seguridad física y de la información que puedan estar inmerso en el espacio donde se haga uso del sistema, teniendo presente los dominios A.9., A.11., A.12., A.16. y el A.18 de la norma ISO 27001:2013.

Fase III: Diseño del sistema FSE – Frente de seguridad electrónico

Recursos usados.

- Consulta documental de sistemas similares que existen en el mercado.

- Seleccionar los elementos electrónicos para la construcción del prototipo inicial.

- Diseñar los planos del sistema FSE.

- Construir el sistema FSE

Fase IV: Pruebas e implementación del sistema FSE en la comunidad del municipio del El Colegio Cundinamarca.

Recursos usados: Sistema de Seguridad FSE – Frente de Seguridad Electrónico.

6. DESARROLLO DE LOS OBETIVOS

6.1 Objetivo 1

6.1.1 Diseñar el Sistema de Seguridad Electrónico FSE (Frente de Seguridad Electrónico) Observación y visitas a las comunidades del municipio, donde se evidencio la inseguridad y la falta de apoyo de los entes de seguridad del municipio.

En el diseño del sistema FSE, se tuvieron presente dos tecnologías a ser analizadas la cuales se presentan a continuación:

Comparación entre las tecnologías PCB y ARDUINO, donde se indican las ventajas que ofrece cada una. Esta se tomó como referencia para tomar la decisión en cuanto a la tecnología a usar para la construcción del sistema FSE.

6.1.2 Tecnología de base a ser analizada

- SISTEMA EN PBC: Una tarjeta PCB es una es una lámina o placa la cual soporta la conexión de diferentes componentes electrónicos, es el elemento principal donde se encuentran ensamblados los sistemas tecnológicos actualmente, estas placas se componen de diferentes partes y estas partes a su vez poseen ciertas características las cuales deben cumplir con las especificaciones requeridas por el diseño.[29]

[29] ELECTROSOFT INGENIERIA. [Sitio web]. Viña del Mar. [Consulta: 1 de abril 2020]. Disponible en: http://www.pcb.electrosoft.cl/04-articulos-circuitos-impresos-desarrollo-sistemas/01-conceptos-circuitos-impresos/conceptos-circuitos-impresos-pcb.html

Las siguientes son características contenidas en un PCB:

- Caras, pueden contener cara arriba y cara abajo.

- Capas, algunos son de una capa de dos o más capas llamados multicapas.

- Refuerzo, este se compone de una capa de fibra de vidrio, la cual se encuentra en el centro del PCB, este debe soportar electrónica y mecánicamente todos los elementos contenidos en el PCB, Pistas conductivas, antisolder screen, y elementos electrónicos.

- Capa de cobre, la cual se encuentra en ambos lados del laminado, allí se encuentran todos los caminos conductores, como vías o pads, pistas o trazos los cuales comunican pines o terminales entre sí.

- Pad THT, porción de cobre para ensamblar el pin del componente tipo smt o THT.

- Vía, es un hueco metalizado pasante entre capas para realizar la conexión entre pines cuando tenemos PCB de dos capas de cobre y así realizar la comunicación entre elementos electrónicos.

- Trough hole, similar a una pista, es un hueco metalizado, compuesto por un pad arriba y un Pad abajo y en el centro contiene un tubo metalizado para conectar los dos pines de las diferentes capas.[30]

[30] PREZI. [Sitio web].Budapest. [Consulta: 23 de octubre 2019]. Disponible en: https://prezi.com/8ih96ob-bqh0/tecnologia-de-agujeros-pasantes-through-hole/

- Máscara de soldadura, es una máscara protectora, por lo general de color verde, también se puede encontrar en otros colores, rojo, azul etc, el cual sirve para la protección de pistas y terminales de cobre expuestas, esta ayuda a evitar la corrosión también protege la fibra de vidrio o laminado de altas temperaturas y humedad.

- Máscara de componentes, sin textos imágenes o letras que se imprimen en el PCB, por lo general se usa para referenciar los componentes electrónicos que se van a instalar en la PCB.

- Solder spacing, es un espacio vacío que se encuentra entre el anti solder y el Pad, la función principal de este es evitar que se suelden terminales entre sí.

➢ SISTEMA ARDUINO

Plataforma de hardware libre la cual incluye un microcontrolador, con un entorno de desarrollo listo, de esta forma poder interactuar con sensores y actuadores, de esta manera poder llevar a cabo un sin número de proyectos.[31]

Para poder realizar un proyecto necesariamente se debe dar instrucciones de cómo debe realizar su trabajo, pues simplemente es un dispositivo electrónico sin ningún tipo de programación, por lo tanto, se deben generar algoritmos e instrucciones para que sea capaz de interactuar con periféricos tales como relés, sensores leds, etc, al igual que los PIC o microcontroladores. Estas instrucciones se deben realizar por medio de lenguajes de programación de alto nivel, de esta forma, este lenguaje se

[31] Op. Cit

traduce en ceros y unos, estos a su vez son entendidos por el microcontrolador, de manera que pueda realizar su tarea final.

Sus componentes son:

- Microcontrolador para la conexión serial a USB.

- Microcontrolador de entradas y salidas con funciones adicionales.

- Conmutador de fuente, es el encargado de seleccionar si la fuente viene por USB desde un pc o si la fuente viene externa generalmente polarizada entre 6 y 15 v DC.

- Regulador de voltaje, corresponde a la entrada externa, este a su vez contiene unos comparadores, para poder entregar voltajes de 3.6 a 5 v. a su lado tiene un diodo de protección en caso de usar de manera incorrecta ya sea por altos voltajes o por polarización inversa la alimentación externa, este diodo impide que se dañe el regulador y a su vez protege toda la placa Arduino.[32]

- Contiene un oscilador, el cual trabaja con el microcontrolador encargado de la comunicación del puerto USB a serial hacia el microcontrolador de funciones.

[32] SHERLIN.XBOT.ES. [Sitio web]. [Consulta:26 de marzo 2020]. Disponible en: Sherlin xbot es. Obtenido de http://sherlin.xbot.es/microcontroladores/introduccion-a-los-microcontroladores/que-es-un-microcontrolador

- Contiene tres leds, uno es para visualizar el encendido del Arduino, el otro es para visualizar la recepción de datos y otro que se utiliza para realizar pruebas en el Arduino.

- Posee dos conectores de pines esenciales para programar el microcontrolador encargado de la comunicación USB serial y otro para la comunicación y programación del microcontrolador de funciones.

- Entradas analógicas, estas entradas están diseñadas para recibir voltajes entre 0 y 5 voltios a su vez también tiene entradas digitales y un botón de reset el cual se utiliza para el reinicio del Arduino en caso de que se bloquee.

Fusible de medio amperio, el cual es utilizado para la protección del puerto del pc en caso de ser necesario, esto se puede dar cuando el PC se conecta al Arduino por medio del puerto USB y en el momento de realizar instalaciones de periféricos se genera algún corto, automáticamente el fusible se abre impidiendo que el corto llegue hasta el puerto de computador conectado.

Tabla 1. Comparativo de sistema PCB y sistema Arduino

PCB - VENTAJAS	ARDUINO - VENTAJAS
Se puede hacer todo más pequeño.	Trae programador incorporado
Alta velocidad de comunicación por ser una estructura compacta.	Listo para usar, pues se programa y solo es conectar sensores actuadores etc.
Al ser una estructura compacta y reducida, se minimiza la interferencia y el ruido.	El uso de librerías hace de la programación más sencilla.
Bajo costo en materiales.	Por ser hardware y software libre, los proyectos se pueden realizar

PCB - VENTAJAS	ARDUINO - VENTAJAS
Disminución de costos d ensamblaje. Manejo de potencias más pequeñas. Fácil de dañarse por manipulación. Se requiere de bastante soldadura. Al momento del ensamblaje, los componentes se pueden caer o dañarse. Difícil inspección visual a la hora de probar. Hay que comprar el programador.	alejándose de la idea de violar derechos de autor. La mayoría de las librerías para la programación tienen costo además estas generan retraso de microsegundos al ejecutar instrucciones. Por ser una tecnología ya ensamblada, quita la posibilidad de hacer más flexibles los proyectos, esto obliga a usar espacios y formas acordes al arduino.

Fuente: Elaboración propia.

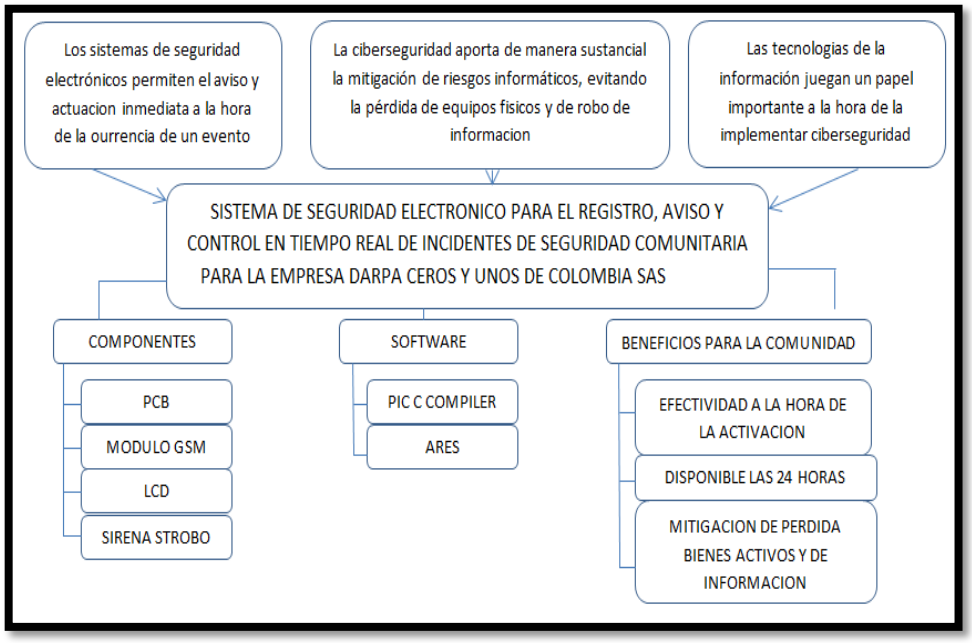
Para el proyecto realizado se escoge la tecnología PCB, ya que es una forma abierta para diseñar el circuito de tal forma que se adapte a los requerimientos, da la facilidad de diseñar el proyecto bajo normas técnicas y estándares exigidos por el dispositivo de Quectel M95, ya que este funciona bajo parámetros eléctricos fijos el cual no permite pérdidas de corriente o de voltajes definidos por el fabricante, es de anotar que este exige un diseño especial en la fuente de alimentación, a su vez el módulo no permite que se generen perdidas de señal, al ser un dispositivo sumamente delicado en cuanto a su estructura física y estructura de funcionamiento.

Al realizar el montaje sobre la misma placa se puede tener la confianza que las pérdidas y ruidos electromagnéticos van a ser mínimos y por lo tanto se garantiza el funcionamiento de este con un nivel de confiabilidad sumamente alto.

Descripción del sistema propuesto teniendo en cuenta los elementos tecnológicos que intervienen en el diseño FSE “FRENTE DE SEGURIDAD ELECTRÓNICO” mostrando una visión del objetivo principal.

La siguiente figura describe los componentes de hardware, software y los beneficios de implantación que podría tener la comunidad objetivo u organización.

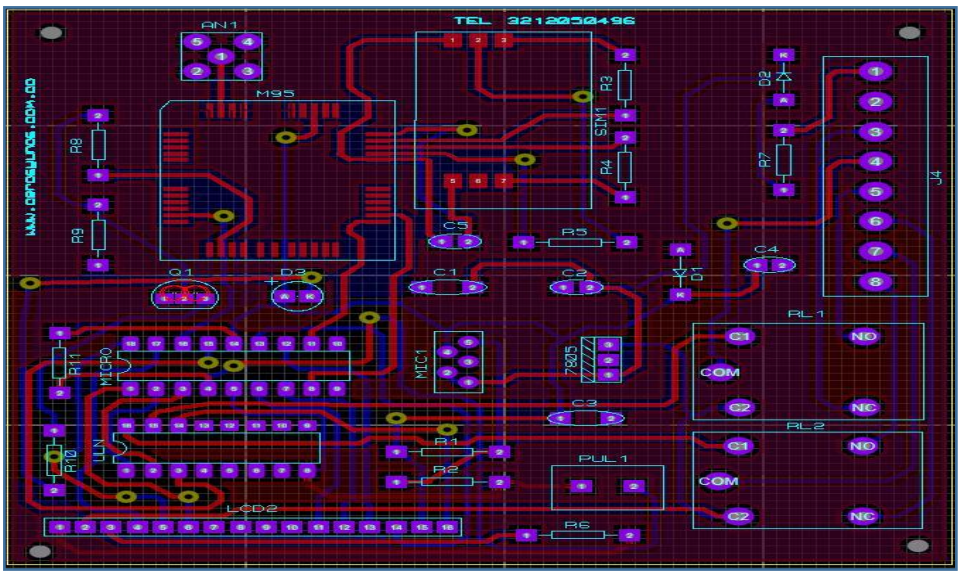
Figura 1. Descripción del sistema de seguridad.



Fuente: Elaboración Propia.

A continuación, se presentan los planos diseñados del sistema FSE, así como los componentes de hardware usados para su construcción.

Figura 2. Diseño de PCB en software de modelado ARES



Fuente: Elaboración Propia.

6.1.3 Componentes de hardware propuestos para la construcción del sistema FSE

A continuación, se relaciona y se conceptualizan los componentes requeridos para el diseño y construcción sistema electrónico propuesto:

- ✓ Microcontrolador

Contiene un hardware y software como un computador, por lo que se define como un pequeño dispositivo de cómputo.[33] Es de tal manera que como su nombre lo indica es un pequeño conector el cual tiene como función controlar el sistema que se crea a partir de él.

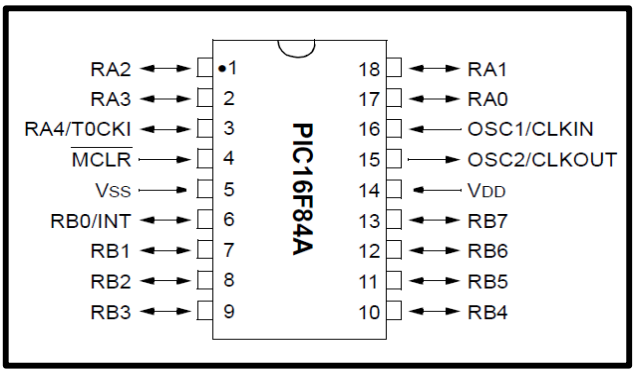
- ✓ Microcontrolador PIC 16f84A

[33] Ibid.,

El PIC16F84A es un microcontrolador que contiene características de gama media el cual consta de 18 pines, su memoria de programa es de tipo flash, lo que nos permitirá grabarlo hasta unas 10000 veces; tiene una velocidad máxima de 20 MHz, contiene una memoria de 68 Bytes de RAM, 4 fuentes de interrupción, 64 byte de EEPROM, 2 puertos de salida, 4 fuentes de interrupción, 13 Líneas de I/O configurables individualmente y 25 mA de corriente por pin[34].

Teniendo en cuenta las características anteriores este microcontrolador nos permitirá diseñar el sistema electrónico de seguridad, por la diversidad en su conformación además de la capacidad de memoria y funcionalidad.

Figura 3. Distribución de pines del PIC 16F84A



Fuente: MICROCHIP TECHNOLOGY INC. [Sitio web]. Estados Unidos. [Consultado 23 de agosto 2019]. Disponible en: https://ww1.microchip.com/downloads/en/DeviceDoc/30430D.pdf

- ✓ ULN2003A Amplificador Darlington NPN:

[34] Ibid.,

El ULN2003A es un IC que contiene un Arreglo de 7 transistores Darlington, cada uno es capaz de manejar 0.5 A y 50 V. Contiene diodos de protección de voltaje opuesto para manejar cargas inductivas[35].

Las características más relevantes son:

Contiene la estructura de transistor: pnp, tiene 7 transistores NPN Darlington en emisor común, 7 diodos de supresión de voltajes inversos para manejar cargas inductivas, con conexiones de cátodo común, tiene salidas de 0.5 A (500 mA) max., sus transistores se pueden conectar de forma paralela para dar más capacidad de corriente, tiene Voltaje de salida entre-0.5 V a 50 V, cuanta con una resistencia de entrada a la base de 2.7 kΩ, capacidad de Voltaje de entrada entre 0.5 V a 30 V, de igual manera tiene entradas compatibles TTL y CMOS de 5 V y finalmente está encapsulado con DIP 16 pines.[36]

- ✓ Sistema GSM

La red GSM (Sistema global de comunicaciones móviles) da su inicio en el siglo XXI, siendo el más utilizado en Europa. Se llama modelo de segunda generación (2G) teniendo en cuenta que se realiza de una forma totalmente digital siendo esta la característica que difiere de la primera generación de teléfonos móviles.[37]

[35] PREZI. [Sitio web].Budapest. [Consulta: 23 de octubre 2019]. Disponible en: https://prezi.com/8ih96ob-bqh0/tecnologia-de-agujeros-pasantes-through-hole/

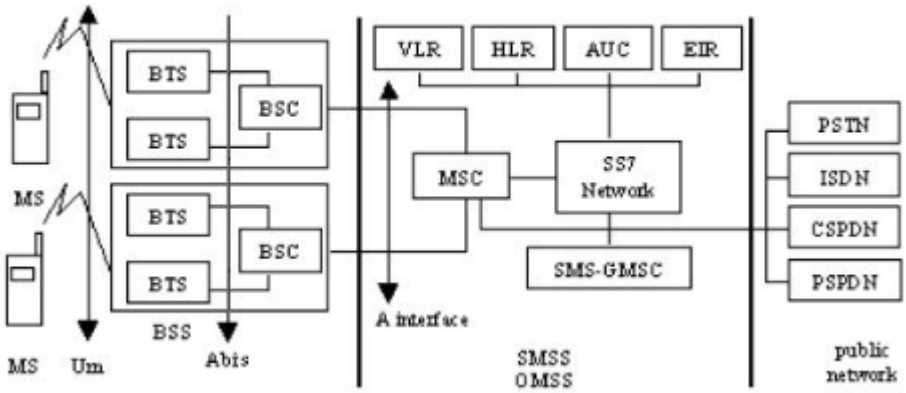
[36] Ibid.;

[37] ENTEL CHILE. S.A. [Sitio web]. Santiago de Chile. [Consulta: 2 de noviembre 2019]. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P11800567291273156038130

Todas las estaciones base de una red celular están conectadas a un controlador de estaciones base (o BSC), que dirige la repartición de los recursos.

Los controladores de estaciones base están conectados al Centro de conmutación móvil (MSC) que los enlaza con la red de internet o telefonía pública; y son administrados por el operador de la red telefónica.[38]

Figura 4. Arquitectura de una red GSM



Fuente: CASTILLA, Rossana Margarita y MEZA, Víctor Manuel. Descripción y evolución de tecnologías para redes de datos en ambiente GSM. Tesis de pregrado Ingeniero eléctrico. Cartagena. Universidad Tecnológica de Bolivar. Facultad de Ingeniería Electrónica. 2005.87p.

- ✓ Tarjeta SIM

[38] ENTEL CHILE. S.A. [Sitio web]. Santiago de Chile. [Consulta: 2 de noviembre 2019]. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P11800567291273156038130

Es una tarjeta inteligente denominada SIM, desmontable y usada en teléfonos móviles y módems HSPA o LTE los cuales se conectan al equipo por medio de una ranura lectora o lector SIM que poseen los mismos[39].

Las tarjetas SIM, acopian de manera segura y confiable la clave de servicio del usuario la cual es utilizada para ser identificado ante la red, de tal forma que el usuario pueda cambiar la tarjeta de un terminal a otro sin afectar su servicio o suscripción al operador.[40]

- ✓ GPRS

"GPRS que significa General Packet Radio Service (servicio general de paquetes vía radio) y es una versión mejorada del GSM, que permite que exista y se dé la mensajería instantánea, de igual manera los servicios de mensajes cortos (SMS) y los mensajes multimedia (MMS) y así como el acceso al correo electrónico generando conectividad constante. Así mismo, el sistema brinda cobertura inalámbrica completa con velocidades de transferencia de entre 56 a 114 kbps (kilobits por segundo)[41], permitiendo de esta manera que el servicio tenga mayor velocidad y a su vez eficacia y garantice la conexión en tiempo real.

Por lo anterior, este sistema es fundamental dentro del proyecto teniendo en cuenta que se va a utilizar el mecanismo de mensajería para la activación del Sistema Electrónico de Seguridad.

---

[39] XATAKA BASICS. [Sitio web]. Xataka. [Consulta: 25 de abril 2020]. Disponible en: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya.

[40] Ibid.,

[41] Op. Cit

- ✓ WAP

(Protocolo de Aplicación Inalámbrica) es una descripción que se le da a un conjunto de protocolos de comunicación para nivelar la forma en que los dispositivos inalámbricos, como lo son los teléfonos celulares y transceptores de radio, puedan tener acceso a Internet, y los diferentes servicios que brinda la conectividad en el cual está incluido el correo electrónico, la World Wide Web, grupos de noticias, y mensajería instantánea.[42]

Es de esta forma como se logra evidenciar que este estándar técnico permite obtener información a través de la conectividad a internet.

- ✓ THT

Es la Tecnología de agujeros pasantes (Through-Hole Technology). Es una clase de tecnología donde se utilizan los agujeros que están impresos en las placas de los circuitos con el fin de llevar a cabo el ensamble de los diferentes elementos electrónicos y así diseñar puentes eléctricos entre una de las caras de la placa de montaje hacia la otra, por medio de un tubo conductor que generalmente es una combinación de zinc, cobre y plata, para impedir su oxidación y lograr su soldadura."[43]

Se puede indicar que el THT, es una tarjeta que contiene unos agujeros que sirven para crear puentes que facilitan la conexión en los elementos electrónicos.

---

[42] ACURED. [Sitio web]. Cuba; AcuRed. [Consulta: 3 de mayo 2020]. Disponible en: https://www.ecured.cu/WAP

[43] PREZI. [Sitio web].Budapest. [Consulta: 23 de octubre 2019]. Disponible en: https://prezi.com/8ih96ob-bqh0/tecnologia-de-agujeros-pasantes-through-hole/

Teniendo presente lo expuesto, y sabiendo que el hardware a ser usado fue analizado componente por componente y es sugerido por el fabricante del módulo GSM-GPRS el cual hace la recepción y transmisión de llamadas y mensajes, a continuación, se presenta la ficha técnica del sistema FSE.

6.1.4 Ficha técnica Alarma con funciones digitales de transmisión de datos compuesta de:

Tarjeta PCB con tecnología THT de 4.1”x4.1”, comunicación GSM, con capacidad de operación en las bandas de 850/900/1800/1900 MHZ, con un consumo de energía de 60w, conectada a una fuente switcheada de 12v a 5a con conexión de antena inalámbrica de longitud de 9.5 cm, pedestal con imán y una ganancia de mínimo de 3dbi, polarización vertical, impedancia de 50 ohm, potencia de 50w, con conector sma macho y una longitud de cable mínimo de 3 metros con funcionamiento de operación de - 40 grados centígrados hasta 85 grados centígrados. Leds indicadores de estado, con activación de salidas a relevo para Leds de aviso y luz policial sonora, personalizable con un mensaje de recibido y 5 mensajes de aviso del evento.

Salida de mensajes de túnel GPRS (IP), botón de programación y pantalla de cristal líquido de 2*16 alfanumérica para la visualización de información y programación, socket para simcard H1016.

Caja antivandálica tipo intemperie color blanco con fondo aislante naranja y terminales de conexión a tierra. Conforme a lineamientos técnicos y normativos de baja y media tensión. Fuente de respaldo de 12 v 5ª, con capacidad de recibir alarmas comunitarias instaladas en los sectores de la ciudad.

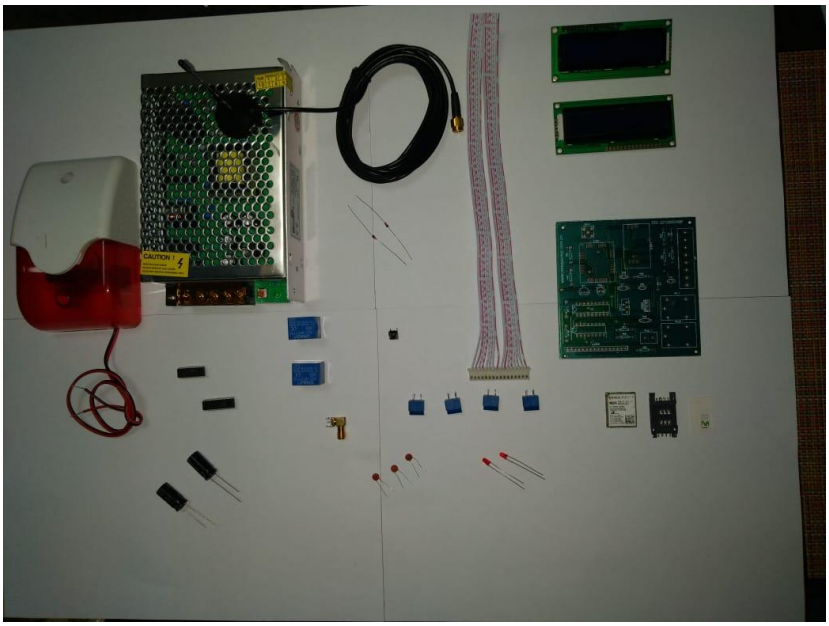
Este dispositivo al tener comunicación directa con las autoridades de policía permitirá la mitigación de los diferentes actos delincuenciales permitiendo generar seguridad y armonía en los diferentes sectores.

6.1.5 CONSTRUCCIÓN DEL SISTEMA ELECTRÓNICO DE SEGURIDAD -FSE

Diseño PCB La fabricación de este Sistema se inicia con el diseño de la PCB, el cual se realiza en un software denominado ARES, una vez es realizado el diseño se envía al laboratorio donde se efectúa una primera prueba y de ser aprobada se realiza la fabricación correspondiente, la cual es mínimo de 50 unidades.

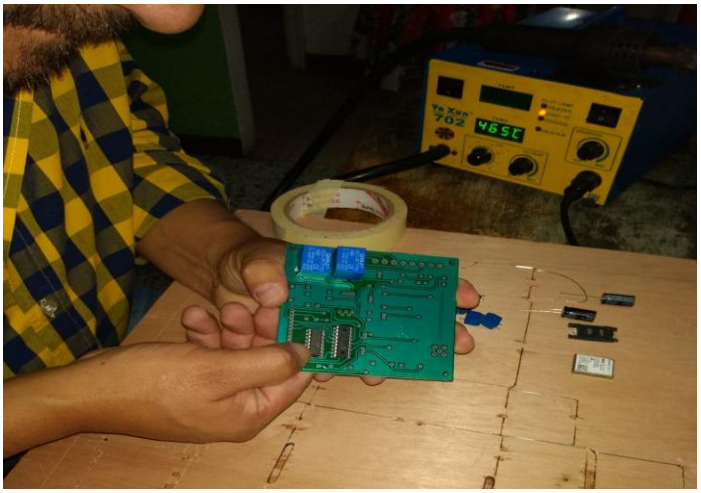
Ensamble de PCB: El ensamble se inicia con la conexión del Módulo Quectel M95, módulo de superficie, posteriormente se instala el shocker de la antena SMA, desde el pin de la antena y a su vez se instala el módulo de la SIM CARD, conectando los pines a los módulos de entrada y salida del módulo Quectel. Posteriormente se instala el Microcontrolador, donde algunas entradas se conectan al módulo y las salidas son las que nos brindan la información de cómo actúa el sistema y otras son usadas para mostrar en el LCD, lo programado en los mensajes de texto. Seguidamente se instala un micro denominado ULN, el cual nos brinda una corriente y unos voltajes que permitirá activar el sistema desde el microcontrolador (Las Sirenas, Luces, etc). Luego se instalan las cintas que van al bus de datos y de igual manera se instalan dos relevos que serán los que permiten la activación del sistema y también se conectan unas borneras las cuales se sitúan en los relevos, que son las que alimentan las tarjetas y otras para la actuación, es decir la activación o funcionamiento de las luces robos tópicas y las sirenas.

Figura 5. Materiales para ensamble de la PCB



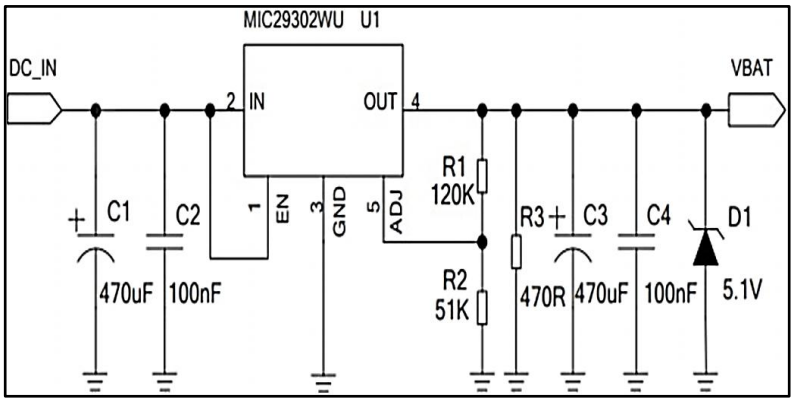
Fuente: Elaboración Propia.

Figura 6. Ensamble de la PCB



Fuente: Elaboración Propia.

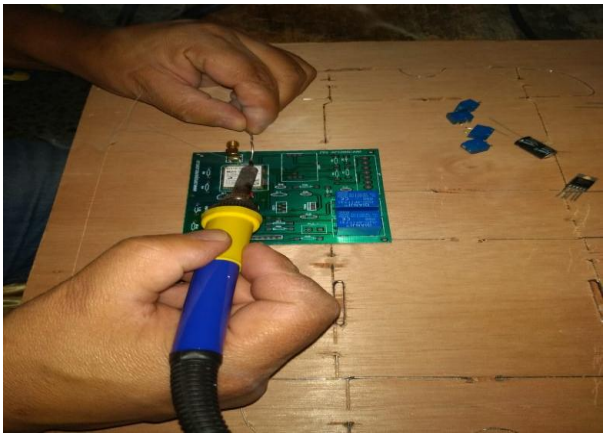
Figura 7. Plano de la Fuente Módulo Quectel



Fuente:GIZWITS. [Sitio web]. China. [Consultado 05 enero 2020]. Disponible en http://docs.gizwits.com/zh-cn/module_source/TinyCon3350-M26/TinyCon3350-M26.html

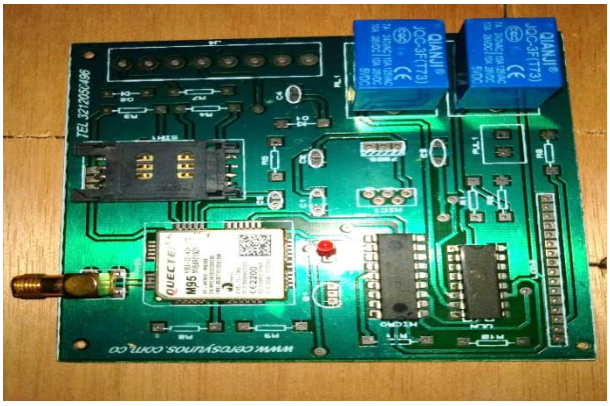
Armar la Fuente: Luego de eso se inicia armar la fuente de voltaje especial para que trabaje el módulo teniendo en cuenta que este trabaja dentro del rango de unos voltajes el cual no puede ser ni mínimo ni máximo, por lo tanto, debe hacerse con exactitud máximo 4.6 Voltios para garantizar su funcionamiento.

Figura 8. Ensamble de la fuente.



Fuente: Elaboración Propia.

Figura 9. Tarjeta ensamblada



Fuente: Elaboración Propia.

Terminado del ensamble: Para finalizar se toma una caja metálica Tecnología IP66 para intemperie con un fondo aislante plástico color naranja y se utiliza una fuente de voltaje de 12 Voltios a 5 amperios con el fin de que brinde buena corriente y garantice el funcionamiento de la alarma y del Sistema Electrónico de Seguridad. De igual manera se utiliza una antena de 3 DBI que va conectada al conector SMA que está en la placa y este sistema tiene un diseño para trabajar con las cuatro bandas que se encuentran vigentes en el país y para finalizar se conecta a un sistema de Corriente de 110 Voltios y se hace la configuración específica para dar inicio a su utilización.

Figura 10. Ensamble Final

Fuente: Elaboración Propia.

Se presenta tarjeta ensamblada con la cual se realizaron las pruebas en campo y la respectiva implementación.

Figura 11. Presentación final de la tarjeta PCB con tecnología THT de 4.1” x 4.1”

Fuente: Elaboración Propia.

6.2 Objetivo 2

Realizar pruebas de funcionalidad del prototipo con el fin de proteger la integridad de las personas y de los bienes físicos y tecnológicos de las mismas.

Las pruebas de funcionalidad se realizaron en el municipio de El Colegio Cundinamarca, apoyado de la Policía Nacional, teniendo presente:

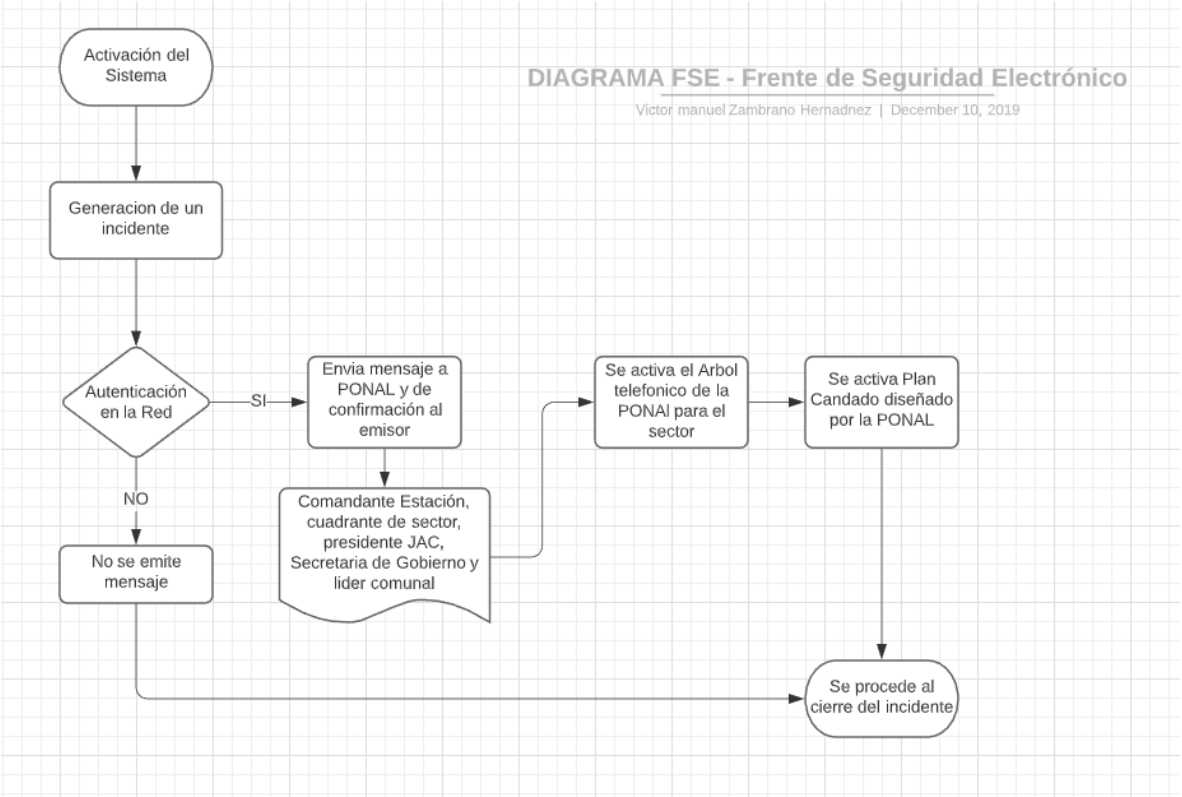
6.2.1 Funcionamiento del Sistema – FSE Este diseño tiene una activación automática, la cual se impulsa una vez el sistema detecta una llamada a la SIM CARD asignada por parte de alguno de los números que han sido seleccionados y registrados por parte de los usuarios.

Una vez el sistema identifica este número ella de forma automática genera un mensaje de texto y alerta el cual indica: “Alarma activada por…” y muestra la dirección o ubicación del sitio donde se presenta la anomalía de seguridad. De esta manera la alarma genera un primer mensaje de texto dirigido a la persona o número de teléfono que activa el sistema en el cual le informa que “La solicitud está siendo atendida por la PONAL”, y de forma inmediata y paralela el sistema genera máximo 5 mensajes lo cuales son distribuidos en las personas quienes hayan obtenido el sistema de Seguridad y con el cuadrante de la policía Nacional, Comandante de la policía y de ser necesario a la Secretaria de Gobierno del Municipio según sea el caso, el mensaje que reciben dice: “Alarma Activada por…” el barrio o sector y el número de celular de quien activó el Sistema de Seguridad. Así mismo, una vez activada la Alarma este sistema tendrá una alarma de sonido la cual se activará en el centro de control de la Policía, la cual es programada por tiempos dados en

segundos. Y de esta manera se forja el Plan Candado o Árbol telefónico de Seguridad como lo denomina la Policía Nacional.[44]

A continuación, se presenta diagrama de flujo que muestra como actual el sistema de frente de seguridad electrónico FSE

Figura 12. Actuación del sistema de Frente de Seguridad Electrónico FSE.



Fuente: Elaboración Propia.

[44] ZAMBRANO, Víctor Manuel. Alarma uno. [Video]. Facatativa. YouTube. (20 de noviembre 2019). 3:15 minutos. [Consulta: 5 de mayo 2020]. Disponible en: https://www.youtube.com/watch?v=iap27sKt9UI

Teniendo presente la figura anterior, se presenta cada uno de los pasos que se deben dar para la generación de un mensaje de alarma

1. Activación del sistema: Se activa el sistema a través de una llamada telefónica al frente de seguridad electrónico o al departamento de seguridad en su defecto.

2. Generación de un incidente: La genera la persona que se encuentra registrada en el sistema Frente de Seguridad Electrónico.

3. Autenticación en la red: Si se presenta autenticación al sistema con éxito, se emiten los mensajes de texto a:
    a. Quien activa
    b. Comandante de estación
    c. Cuadrante del sector
    d. Presidente de Junta de Acción Comunal
    e. Secretaria de Gobierno
    f. Líder comunal

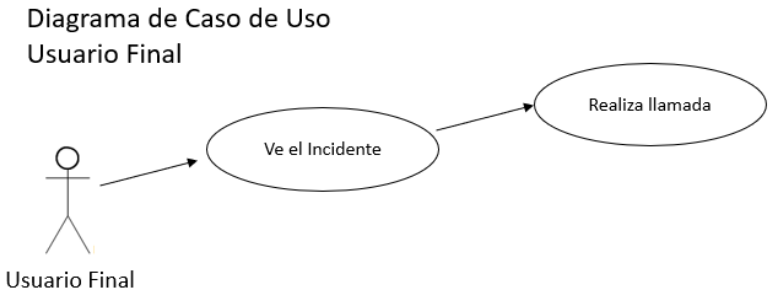
    O al equipo que considere la organización donde se implemente la el Frene de Seguridad Electrónico.

4. Si no se presenta la autenticación: El sistema genera un mensaje en pantalla que indica “Numero invalido”.

5. Cierre del incidente: Son las partes interesadas las que dan cierre al incidente, a partir de la activación del árbol telefónico y el plan candado establecido por la PONAL o en su defecto el establecido por la organización.

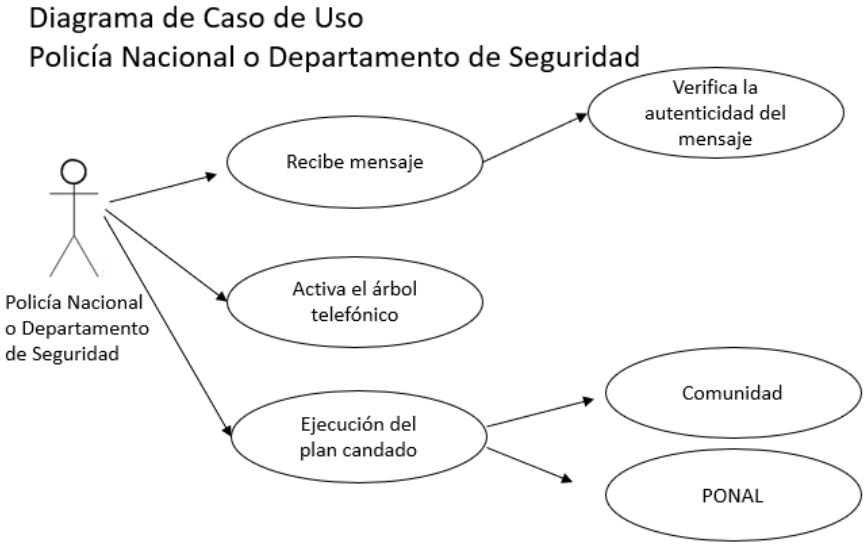
A continuación, se representa a partir del uso de diagramas de uso cada uno de los actores que intervienen en el proceso:

Figura 13. Actuación del usuario final en el sistema de Frente de Seguridad Electrónico FSE



Fuente: Elaboración Propia.

Figura 14. Actuación del equipo de respuesta en el sistema de Frente de Seguridad Electrónico FSE.



Fuente: Elaboración Propia.

6.2.2 Activación de la Alarma Este diseño tiene una activación automática, la cual se impulsa una vez el sistema detecta una llamada a la SIM CARD asignada por parte de alguno de los números que han sido seleccionados y registrados por parte de los usuarios. Una vez el sistema identifica este número ella de forma automática genera un mensaje de texto y alerta el cual indica: “Alarma activada por…” y muestra la dirección o ubicación del sitio donde se presenta la anomalía de seguridad. De esta manera la alarma genera un primer mensaje de texto dirigido a la persona o número de teléfono que activa el sistema en el cual le informa que “La solicitud está siendo atendida por la PONAL”, y de forma inmediata y paralela el sistema genera máximo 5 mensajes lo cuales son distribuidos en las personas quienes hayan obtenido el sistema de Seguridad y con el cuadrante de la policía Nacional, Comandante de la policía y de ser necesario a la Secretaria de Gobierno del Municipio según sea el caso, el mensaje que reciben dice: “Alarma Activada por…” el barrio o sector y el número de celular de quien activó el Sistema de Seguridad. Así mismo, una vez activada la Alarma este sistema tendrá una alarma de sonido la cual se activará en el centro de control de la Policía, la cual es programada por tiempos dados en segundos. Y de esta manera se forja el Plan Candado o Árbol telefónico de Seguridad como lo denomina la Policía Nacional.[45]

6.3 Objetivo 3

Presentar de manera funcional el sistema de seguridad electrónico FSE (Frente de Seguridad Electrónico).

[45] Ibid.,

Como resultado final en la ejecución de este proyecto a continuación se presenta el funcionamiento del sistema de seguridad de frente electrónico – FSE, en este se tiene presente que la implementación de este impacta de forma directa en contribuir no solamente en la seguridad física del entorno donde se implemente, sino también el impacto que este presenta desde la ciberseguridad a partir de:

El permitir gestionar y apoyar el control de acceso en una comunidad o en una organización (Dominio A.9. Anexo A norma ISO 27001:2013), contribuyendo en dar cumplimiento a los siguientes objetivos:

A.9.1. Requisitos del negocio para el control de acceso.

A.9.2. Gestión e acceso de los usuarios.

El dar soporte a la gestión de la seguridad física y del entorno (Dominio A.11. Anexo A norma ISO 27001:2013), contribuyendo en dar cumplimiento a los siguientes objetivos:

A.11.1. Áreas seguras.

El apoyar además en la gestión de incidentes de la seguridad de la información (Dominio A.16. Anexo A norma ISO 27001:2013), dando cumplimiento al siguiente control:

A.16.1.5. Respuesta a incidentes de seguridad de información.

A partir de esto, se expone a continuación, el funcionamiento del Sistema FSE.

Se realiza la instalación del FSE en el sitio donde va a ser monitoreado el sistema, realizando la conexión eléctrica y verificando el respaldo de energía de una UPS y una planta eléctrica de esta manera se garantiza 24/7.

Figura 15. Instalación de los Frentes de Seguridad Electrónica

Fuente: Elaboración Propia.

Para que el dispositivo funcione correctamente primero se debe realizar la programación del mismo, este equipo se programa por medio de mensajes de texto, los pasos son los siguientes:

El FSE tiene un botón que al obturar abre un menú el cual da la posibilidad de programar el nombre del sector, la dirección o nombre del predio, los segundos que dura la activación y para incluir a los usuarios estos se registran en una tarjeta simcard.

Para realizar la puesta en marcha del FSE, se invitó a una usuaria, en este caso la presidente de junta de unos de los sectores de El Colegio, esta persona realizó la

llamada, el sistema reconoció el número de celular devuelve el primer mensaje de texto confirmando la activación, el sistema se y comienza a generar ruido de sirena para alertar al encargado del monitoreo de la sala de seguridad.

Figura 16. Socialización del Sistema FSE - Frentes de Seguridad Electrónica con la comunidad del municipio de El Colegio Cundinamarca

Fuente: Elaboración Propia.

La persona encargada de realizar el monitoreo del FSE es un miembro de la PONAL el cual se acerca a verificar por que se activa el sistema y por medio de su radio de comunicación avisa al cuadrante de la zona para que se dirija al sector y dirección que arrojo el sistema.

Figura 17. Activación del Sistema FSE - Frentes de Seguridad Electrónica

Fuente: Elaboración Propia.

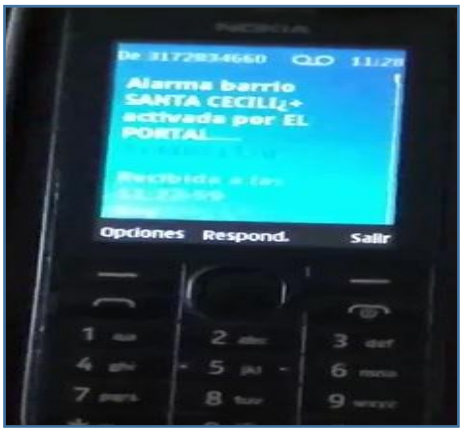
Figura 18. Generación de alerta ante un incidente del FSE - Frentes de Seguridad Electrónica

Fuente: Elaboración Propia.

El sistema luego genera cinco mensajes de texto, a las siguientes personas involucradas en el esquema de seguridad: comandante de estación de policía, secretaria de gobierno, Cuadrante del sector, presidente o líder comunal. Otro de legado por la comunidad para apoyo en la seguridad del sector.

A todos ellos el FSE genera un mensaje de aviso del evento el cual dice el sector y la dirección de donde se activó el sistema.

Figura 19. Generación de alerta ante un incidente del FSE - Frentes de Seguridad Electrónica



Fuente: Elaboración Propia.

7. RESULTADOS

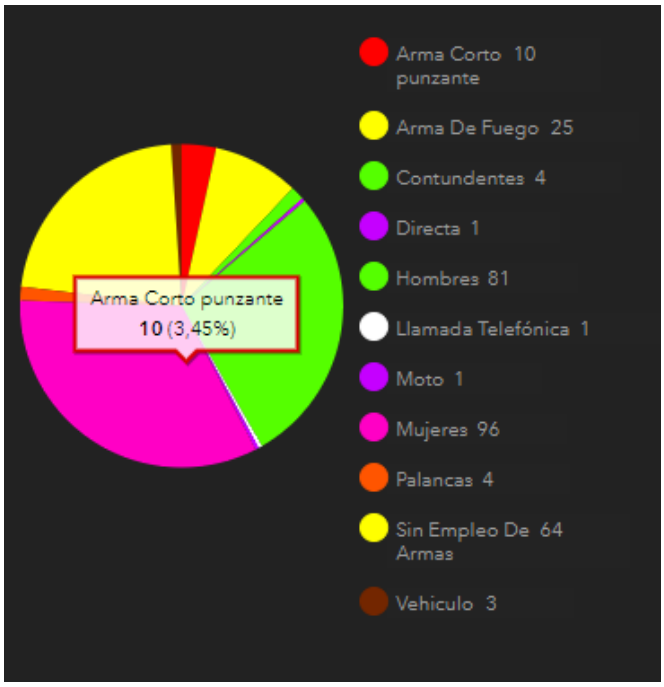
Una vez diseñada, ensamblada y puesta en funcionamiento el Sistema Electrónico de seguridad se logra evidenciar que tiene un buen funcionamiento y efectividad en la recepción de mensajes, por tal razón, la comunicación e información llega de manera inmediata y en tiempo real a la autoridad competente quien a su vez tomará las medidas de seguridad pertinentes de acuerdo a su competencia.

A continuación, se presentan datos estadísticos que indican la reducción de acciones delictivas donde puede estar comprometida la integridad de las personas y de la información de las mismas. Los datos que se presenta corresponden al informe generado por el observatorio de seguridad el departamento de Cundinamarca para los años 2017 y 2018.

7.1 RESULTADOS OBTENIDOS EN LA REDUCCIÓN DE INCIDENTES A PARTIR DEL USO DEL SISTEMA FSE.

Año 2017 total de delitos 290

Figura 20. Delitos reportados año 2017 municipio mesitas del Colegio



Fuente: CUNDINAMARCA-MAP. [Sitio web]. Cundinamarca. [Consultado 10 febrero 2020]. Disponible en http://cundinamarca-map.maps.arcgis.com/apps/opsdashboard/index.html#/2c4fcb5c134445c2a921c6ab4c013fd3

Año 2018 total, de delitos 203

Figura 21. Delitos reportados año 2017 municipio mesitas del Colegio

Fuente: CUNDINAMARCA-MAP. [Sitio web]. Cundinamarca. [Consultado 10 febrero 2020]. Disponible en http://cundinamarca-map.maps.arcgis.com/apps/opsdashboard/index.html#/2c4fcb5c134445c2a921c6ab4c013fd3

Con base en las dos graficas presentadas anteriormente se puede evidenciar la reducción de ataques a personas en el municipio de El Colegio, pasando de 290 acciones reportadas en el 2017 a 203 en el 2018.

7.2 CONTRIBUCIÓN DE LA CIBERSEGURIDAD EN EL PROYECTO

La seguridad informática es la posibilidad de seguridad que se brinda a través de las tecnologías y sistemas informáticos. Por tal razón es importante tener claro el

concepto de la seguridad, que está directamente relacionado con la información.[46] A continuación, se relacionan los pilares de la dimensión de la seguridad de la información que pueden verse afectados en un entorno inseguro de forma física o digital y que son pilares sobre los que se deben aplicar medidas para la protección de esta.

La disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración, o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema «cae» impidiendo accesos legítimos. Ambos tienen implicaciones serias para la seguridad de la información.

Figura 22. Dimensiones de la Seguridad de la información.

Ilustración 1: Dimensiones de la seguridad de la información

Fuente: INCIBE. [Sitio web]. España. [Consultado 25 julio 2020]. Disponible en https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

[46] SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA. [Sitio web]. Bogotá [Consulta: 13 de agosto 2019]. Disponible en Obtenido de http://www.supervigilancia.gov.co

La integridad de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano.

La confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como need-to-know. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplos de falta de confidencialidad, son el robo de información confidencial por parte de un atacante a través de internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso.

Este proyecto se enfoca en proponer una alternativa para reducir el accionar delictivo de hurto o de otro tipo de amenaza al que este expuesto una persona o una organización y que por defecto se vea involucrada la perdida de información física o digital, hace referencia a la necesidad de proteger y cuidar los bienes de las empresas y la integridad de las personas, por tal razón el dispositivo que se plantea y se diseña será de gran ayuda a la hora de proteger la integridad de las personas, las entidades públicas, privadas que lleguen a correr algún riesgo en el sector donde se encuentre ubicado el dispositivo.

Este dispositivo al tener comunicación directa con las autoridades de policía permitirá la mitigación de los diferentes actos delincuenciales permitiendo generar seguridad y armonía en los diferentes sectores.

7.3 CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN

Técnicos: medidas de carácter tecnológico dentro del ámbito de la seguridad. Son medidas técnicas: antivirus, cortafuegos o sistemas de copias de seguridad.

Organizativos: medidas que se centran en la mejora de la seguridad teniendo en cuenta a las personas, por ejemplo: formación en seguridad, identificación de responsables o implantación de procedimientos formales de alta y baja de usuarios.

Físicos: medidas físicas para proteger nuestra organización; ejemplo, acondicionar adecuadamente la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados, establecer un sistema de control de acceso para entrar en las oficinas, poner cerraduras en los despachos y armarios o guardar las copias de seguridad en una caja ignífuga.

Teniendo presente que el Sistemas de Seguridad FSE hace impacto en la seguridad de la información, es preciso indicar que este se puede catalogar como un control de orden físico.

El sistema de seguridad Electrónica se compone de hardware, software, terminales electrónicos y un equipo de control que será vigilado por un operador de seguridad. Al momento de diseñar esta clase de sistemas, se debe establecer el tipo de hardware y software que mejor se ajuste a las necesidades del usuario o

beneficiarios, lo cual garantiza que el sistema diseñado genere comodidad, confianza y seguridad al usuario.

Los sistemas de seguridad electrónica se encuentran controlados por programas y aplicativos los cuales pueden incluir la ejecución de una base de datos, asignar algunos límites de administración a los operadores y brindar un control categórico por los sensores de ambiente[47].

Por tal razón, los sistemas de seguridad electrónica permiten un control de los mecanismos y de la información que se establece para garantizar su funcionamiento.

Así mismo, es importante destacar que estos sistemas son la mezcla de la tecnología, innovación que se aplica a la seguridad, con el fin de obtener un control sobre las situaciones que vulneren o afecten las plantas físicas de cualquier instalación, así como la integridad de las personas en una comunidad o sector.

> *El hombre siempre ha tenido la necesidad de sentir seguridad, las primeras sociedades comenzaron su administración de justicia y seguridad, lo que permitiría comprender por qué las personas desean obtener esta sensación. Una definición técnica de este sistema se establece como un conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar la presencia, irrupción, o invasión de un desconocido o de un*

[47] LEZAMA, Ada. Modelado de dispositivos para un sistema de seguridad implementando tecnología Jini. Trabajo de grado Ingeniería de Sistemas Computacionales. Cholula. Universidad de las Américas Puebla. Departamento de Ingeniería en Sistemas Computacionales. 2001.

individuo que no posea un acceso permitido. Estos equipos nos avisarán cuando el sistema fue violado mediante un ruido característico o señal aguda, a su vez, el sistema de seguridad puede estar conectado a una central de vigilancia privada para que al cabo de pocos minutos personal policial se haga presente en nuestra ayuda.[48]

Se puede evidenciar en el escrito anterior como el hombre siempre ha tenido necesidad de sentir seguridad y aunque con el tiempo las tecnologías cambian y se perfeccionan, la sensación de sentirnos seguros y asegurar nuestros bienes y entornos siempre será una prioridad en el ser humano, por lo tanto, la implementación de sistemas de seguridad que funcionen en tiempos reales permite que exista mayor satisfacción en la necesidad presentada.[49]

Un sistema de seguridad debe contener un procesador central para garantizar su funcionalidad el cual controlara los eventos; de igual manera debe tener diferentes controladores inteligentes en su la instalación, los cuales deben monitorear los diferentes hechos ocurridos y así reportar cualquier anomalía que se genere.

7.4 DE LA SEGURIDAD INFORMÁTICA

La seguridad informática es la posibilidad de seguridad que se brinda a través de las tecnologías y sistemas informáticos. Por tal razón es importante tener claro el concepto de la seguridad física, que está directamente relacionado la seguridad.[50]

---

[48] CARDOZO, Mara. Mercado de seguridad electrónica en Colombia como una oportunidad de trabajo y emprendimiento. Tesis de postgrado Mercadeo y Servicio. Bogotá, D.C. Universidad Militar Nueva Granada. 2013. 21 p.

[49] Ibid.;

[50] SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA. [Sitio web]. Bogotá [Consulta: 2 de septiembre 2020]. Disponible en Obtenido de http://www.supervigilancia.gov.co

Este proyecto se enfoca en gran parte en proponer artefactos que contribuyan en endurecer la seguridad física, la cual hace referencia a la necesidad de proteger y cuidar los bienes de las empresas y la integridad de las personas, por tal razón el dispositivo que se plantea y se diseña es de gran ayuda a la hora de proteger la integridad de las personas, las entidades públicas, privadas que lleguen a correr algún riesgo en el sector donde se encuentre ubicado el dispositivo.

8. CONCLUSIONES

Se realiza el diseño propuesto del Sistema Electrónico de Seguridad, teniendo en cuenta los lineamientos y normas técnicas en construcción de PCB y ensamble de dispositivos electrónicos.

De igual manera, una vez realizado el diseño y estructuración del sistema se realizaron las pruebas de funcionalidad del prototipo, en las cuales arrojó como resultado el funcionamiento óptimo del Sistema Electrónico de Seguridad propuesto.

Por lo anterior, se da inicio a la instalación del Sistema Electrónico de Seguridad en la Estación de Policía de Mesitas del Colegio, Cundinamarca donde actualmente funciona en óptimas condiciones, generando los resultados esperados.

Finalmente, se realizó el diseño y la instalación del Sistema Electrónico de Seguridad haciendo el uso de las tecnologías GPRS, GSM Y PCB logrando que a través de este sistema la comunidad logre la comunicación de incidentes de seguridad, generando una reacción efectiva por parte de la policía nacional, generando de esta manera un sentido de seguridad en la comunidad beneficiaria del Municipio del El Colegio.

9. RECOMENDACIONES

Para la efectividad del Sistema Electrónico de Seguridad es necesario contar con un celular que tenga Sistema GSM, teniendo en cuenta que es la vía o medio de comunicación de la alerta a la entidad competente, que para el caso es la Policía Nacional.

De igual manera se recomienda a los usuarios que conformen frentes de seguridad, que permitan trabajar de manera armonizada con la Policía y de esta forma obtener mayor éxito y mejorar los resultados de seguridad en el sector específico en el cual se hace la instalación del Sistema Electrónico de Seguridad.

BIBLIOGRAFÍA

ACURED. [Sitio web]. Cuba; AcuRed. [Consulta: 3 de mayo 2020]. Disponible en: https://www.ecured.cu/WAP.

BBC NEWS. [Sitio web]. Reino Unido. [Consulta: 21 de diciembre 2019]. Disponible en http://www.bbc.com/mundo/noticias-37247130.

CASTILLA, Rossana Margarita y MEZA, Víctor Manuel. Descripción y evolución de tecnologías para redes de datos en ambiente GSM. Tesis de pregrado Ingeniero eléctrico. Cartagena. Universidad Tecnológica de Bolivar. Facultad de Ingeniería Electrónica. 2005.87p.

CARDOZO, Mara. Mercado de seguridad electrónica en Colombia como una oportunidad de trabajo y emprendimiento. Tesis de postgrado Mercadeo y Servicio. Bogotá, D.C. Universidad Militar Nueva Granada. 2013. 21 p.

CEVALLOS, Gabriel. En: SEGURIDAD ELECTRÓNICA. [Sitio web]. Quito: Clasificación de los sistemas de seguridad electrónica. [Consulta: 2 de diciembre 2019]. Disponible en: https://sites.google.com/site/seguridadelectronicagcm/capitulo-1/1-2-clasificacion-de-los-sistemas-de-seguridad-electronica.

COLOMBIA. CONGRESO DE LA REPÚBLICA. LEY 1453 (24, Junio, 2011). Por lo cual se reforma el Código Penal el Código de Infancia y Adolescencia, las reglas

sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad. En: Diario oficial. Junio, 2011. Nro. 48.110 .p.1-15.

COLOMBIA, CORTE CONSTITUCIONAL. CONSTITUCIÓN POLÍTICA DE COLOMBIA. (1991). En: Constitución Colombia

CUNDINAMARCA-MAP. [Sitio web]. Cundinamarca. [Consultado 10 febrero 2020]. Disponible en http://cundinamarca-map.maps.arcgis.com/apps/opsdashboard/index.html#/2c4fcb5c134445c2a921c6ab4c013fd3

DACCACH, José. En: DELTA ASESORES. [Sitio web]. Ley de delitos informáticos en Colombia. [Consulta: 23 de enero 2020]. Disponible en https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. [Sitio web]. Bogotá: DANE. [Consulta: 8 de agosto 2019]. Disponible en : http://www.dane.gov.co/files/investigaciones/poblacion/convivencia/2016/Bol_ECSC_2016.pdf

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. [Sitio web]. Bogotá: DANE. [Consulta: 9 de marzo 2020]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

EL TIEMPO. [Sitio web]. Bogotá. [Consulta: 28 de julio 2019]. Disponible en Obtenido de http://www.eltiempo.com/archivo/documento/CMS-15965877

ENTEL CHILE. S.A. [Sitio web]. Santiago de Chile. [Consulta: 2 de noviembre 2019]. Disponible en: http://personas.entel.cl/PortalPersonas/appmanager/entelpcs/personas?_nfpb=true&_pageLabel=P11800567291273156038130

GIZWITS. [Sitio web]. China. [Consultado 05 enero 2020]. Disponible en http://docs.gizwits.com/zh-cn/module_source/TinyCon3350-M26/TinyCon3350-M26.html

INCIBE. [Sitio web]. España. [Consultado 25 julio 2020]. Disponible en https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

LA REPÚBLICA. [Sitio web]. Bogotá. [Consulta: 31 de julio 2019]. Disponible en: https://www.larepublica.co/globoeconomia/la-inseguridad-ciudadana-hace-de-colombia-el-pais-mas-conflictivo-de-america-latina-2136581

LEZAMA, Ada. Modelado de dispositivos para un sistema de seguridad implementando tecnología Jini. Trabajo de grado Ingeniería de Sistemas Computacionales. Cholula. Universidad de las Américas Puebla. Departamento de Ingeniería en Sistemas Computacionales. 2001.

MICROCHIP TECHNOLOGY INC. [Sitio web]. Estados Unidos. [Consultado 23 de agosto 2019]. Disponible en: https://ww1.microchip.com/downloads/en/DeviceDoc/30430D.pdf

PREZI. [Sitio web].Budapest. [Consulta: 23 de octubre 2019]. Disponible en: https://prezi.com/8ih96ob-bqh0/tecnologia-de-agujeros-pasantes-through-hole/

SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. [Sitio web]. Bogotá. [Consulta: 10 de enero 2020]. Disponible en: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html

SHERLIN.XBOT.ES. [Sitio web]. [Consulta:26 de marzo 2020]. Disponible en: Sherlin xbot es. Obtenido de http://sherlin.xbot.es/microcontroladores/introduccion-a-los-microcontroladores/que-es-un-microcontrolador

SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA. [Sitio web]. Bogotá [Consulta: 13 de agosto 2019]. Disponible en Obtenido de http://www.supervigilancia.gov.co

TECHTARGET. [Sitio web]. Massachusetts. [Consulta: 11 de octubre 2019]. Disponible en: http://searchmobilecomputing.techtarget.com/definition/WAP

UNIVERSIDAD DE ORIENTE. [Sitio web]. Puebla; Universidad de Oriente. [Consulta: 13 de marzo 2020]. Disponible en: https://www.academia.edu/8733930/UNIVERSIDAD_DE_ORIENTE-_PUEBLA

WIKIPEDIA CONTRIBUTORS. [Sito web]. [Consulta: 22 de octubre 2019]. Disponible en https://es.wikipedia.org/wiki/El_Colegio#Organizaci%C3%B3n_territorial

XATAKA BASICS. [Sitio web]. Xataka. [Consulta: 25 de abril 2020]. Disponible en: https://www.xataka.com/basics/tarjeta-sim-como-funciona-como-saber-que-tipo-tuya.

ZAMBRANO, Víctor Manuel. Alarma uno. [Video]. Facatativá. YouTube. (20 de noviembre 2019). 3:15 minutos. [Consulta: 5 de mayo 2020]. Disponible en: https://www.youtube.com/watch?v=iap27sKt9UI