ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

“Comercialización de Sistemas de Acceso Vehicular y Control Peatonal para las ciudadelas privadas, basada en sistemas biométricos de reconocimiento facial.”

TESINA DE SEMINARIO

Previa a la obtención del Título de:

LICENCIADO EN SISTEMAS DE INFORMACION

Presentado por

Kerly Elizabeth Figueroa Peñafiel

Alan Erasmo Villacreses Pincay

Guayaquil - Ecuador

2013

AGRADECIMIENTO

A tu incondicional apoyo y comprensión.

A tu ayuda desinteresada en la culminación de esta etapa. Gracias Freddy por estar siempre a mi lado.

Kerly Elizabeth Figueroa Peñafiel

AGRADECIMIENTO

A Dios por la fortaleza y guía.

A su esfuerzo, sacrificio y contribución gracias Kerly, mi compañera de fórmula durante la culminación de este proceso.

Alan Erasmo Villacreces Pincay

DEDICATORIA

A Dios, proveedor de fortaleza en situaciones difíciles.

A mis padres, que me han ayudado con mucho esfuerzo para que cumpla mis metas, a mis hermanos y sobrinos.

Kerly Elizabeth Figueroa Peñafiel

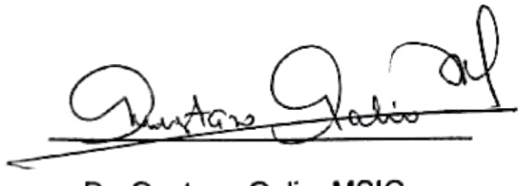
DEDICATORIA

A Dios por ser la luz y guía en mi camino. A mis padres, hermanos y familia por ser pilar fundamental en mi vida.

A mi novia Melany por su apoyo incondicional en la culminación de esta etapa profesional.

Alan Erasmo Villacreces Pincay

TRIBUNAL DE SUSTENTACIÓN



Dr. Gustavo Galio, MSIG.

PROFESOR DEL SEMINARIO

DE GRADUACIÓN

Ing. Nestor Arreaga, MSIG.

PROFESOR DELEGADO POR

LA UNIDAD ACADEMICA

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de Exámenes y Títulos profesionales de la ESPOL)

Kerly Figueroa Peñafiel

Alan Villacreses Pincay

RESUMEN

En el Capítulo uno, la empresa y su producto, se describen los problemas de seguridad que poseen las ciudadelas privadas y empresas del país, se presenta un sistema de control de acceso basado en sistemas biométricos de reconocimiento facial como solución a las necesidades del mercado actual en lo que a seguridad se refiere, contribuyendo de manera significativa con el mejoramiento de la seguridad en todos los sectores que lo implementen. En el Capítulo dos, Marco Teórico, se detalla información referente a la biometría, su etimología, así como la aplicación en diferentes escenarios, ya que se han realizado avances tecnológicos que demuestran que se puede tener un control más eficiente a través de estos dispositivos que son utilizados a nivel mundial, se listan las características que poseen los diferentes tipos de biométricos que existen en la actualidad. Se plantea el reconocimiento facial como solución de control en el acceso de personas y vehículos a un lugar determinado. En el Capítulo tres, Análisis de Mercado, se realiza un análisis de las estadísticas de años anteriores con respecto al número de viviendas que están construidas en la provincia del Guayas, y se evalúa el nivel de delincuencia que existe, esto ayuda a concienciar a los posibles clientes de la necesidad de protegerse utilizando sistemas biométricos, adicional, se muestran varios mecanismo que pueden ser utilizados para captar clientes, lo que asegura el crecimiento de la empresa y

el posicionamiento del producto en el mercado, se realiza la evaluación de las fortalezas, debilidades, oportunidades y amenazas que posee la empresa. Se definen las estrategias que se utilizarán para poder llegar al mercado objetivo, y se exponen los beneficios que obtendrían al adquirir el sistema de control de acceso biométrico, se ha construido un Sitio web, el mismo que será nuestro canal de distribución ya que a través de él pueden hacer pedidos o solicitar demostraciones a fin de que el cliente conozca el producto directamente. En el Capítulo cuatro, Tecnología, se describen la justificación de la tecnología utilizada, así como las herramientas que se utilizan para el desarrollo del sitio web, estableciendo los estándares que deben ser utilizados en la elaboración del sitio, se detalla el mapa del sitio web, y se establecen las seguridades necesarias para proteger la información de los productos, de los clientes, así como de las transacciones que realizan. En el Capítulo cinco, Diseño General, se expone el funcionamiento del sistema control de acceso biométrico, el hardware y el software necesarios para su elaboración, se analiza la arquitectura que se manejaría y los escenarios que se pueden presentar en el uso de la aplicación. En el capítulo seis, Análisis Financiero, se hace un estudio de los costos y la utilidad que generaría el proyecto de acuerdo a lo planteado.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

A nivel mundial se utilizan sistemas biométricos para llevar el control de asistencia de personal, control de acceso a personal autorizado, identificación de personas, voto electrónico, entre otras. Esto surge de la evolución de los dispositivos biométricos, lo que permite la creación de sistemas confiables al utilizar rasgos únicos y difícilmente replicables para identificar a una persona. En los últimos años los dispositivos biométricos están siendo utilizados para fortalecer los sistemas de seguridad ciudadana en general.

Existen varios tipos de sistemas biométricos, como son el dactilar, reconocimiento de iris, mano, rostro, en el proyecto actual se utilizará la biometría basada en el reconocimiento facial, teniendo como objetivo contrarrestar los problemas de seguridad de las ciudadelas privadas y empresas del país, mediante la elaboración de un sistema de control de acceso, el mismo que se detallará más adelante.

CAPITULO 1

1. DESCRIPCIÓN DEL PROBLEMA

1.1 PROBLEMÁTICA

En la actualidad, en los conjuntos habitacionales y empresas se utilizan una serie de sistemas de seguridad, los cuales van desde barras de ingreso, cerramientos, presencia de guardias, alarmas comunitarias, etc. buscando a través de estos medios, proteger sus bienes de elementos inescrupulosos que pudieran perjudicar y apropiarse de aquello que han construido con el paso del tiempo.

En el caso de las ciudadelas privadas, los métodos que utilizan para protegerse se ha vuelto vulnerables y en ocasiones obsoletos, debido al gran crecimiento de estos sectores y de la población que habita en ellas, además

de su ubicación geográfica, que en su mayoría, están alejada de la parte urbana, hace que sean un “mercado atractivo” para la delincuencia, además de la falta de un control verdadero por parte de los encargados de la protección de los habitantes. Los costos por guardianía suelen ser altos y poco rentables para los beneficiarios, ya que los robos son frecuentes y nadie se hace responsable por los daños o pérdidas ocasionadas, lo que crea inconformidad por parte de los residente, los cuales migraron en busca de seguridad, tranquilidad y para garantizar el bienestar de sus familias.

Con el fin de contrarrestar estos problemas se ha optado, tanto en las empresas como en las ciudadelas, por la utilización de cámaras de seguridad, alarmas, botones de auxilio, los cuales suelen estar interconectados con las entidades de control, como las unidades de vigilancia comunitarias que se encuentran en el sector, proporcionando cierto grado de confianza, pero hay que ir más allá, se deben establecer varios niveles de seguridad, y uno de ellos es el de poder restringir el acceso a personas y vehículos no autorizados, evitando el ingreso de desconocidos y controlando efectivamente el robo o préstamo de identidad, por lo que se recomienda la utilización de sistemas biométricos para ayudar a reducir significativamente estos problemas.

1.2 SOLUCIÓN PROPUESTA

Las huellas dactilares y los patrones faciales son las características propias más confiables de cada individuo, actualmente son utilizadas con frecuencia en las implementación de sistemas de seguridad. Dichas características son irrepetibles en los seres humanos, es por ello que entidades públicas y privadas están utilizando sistemas biométricos en diferentes áreas.

Figura 1.1: Sistemas Biométricos

Los biométricos se constituyen como mecanismos de control de acceso seguros, se da la oportunidad de que sea utilizado como medida preventiva, y se propone un sistema que controle de forma efectiva el acceso de personas y vehículos basado en el reconocimiento facial. Cabe recalcar que los Sistemas Biométricos de Reconocimiento Facial tienen características especiales que permiten identificar a personas por medio de sus rasgos físicos, convirtiéndose en un aliado indudable cuando de seguridad se trata.

Además le permitirá contrarrestar la pérdida u olvido de la contraseña, también el robo de identidad a través de sus sensores capaces de reconocer si la persona es quien dice ser, de esa forma se llevará un registro documentado a través de imágenes de quienes ingresaron o salieron del lugar. Estas imágenes se podrían proporcionar a las entidades de auxilio, para poder construir hipótesis y determinar directamente al o los responsables de alguna contravención ocurrida en el sector. La persona encargada de la seguridad, se ve obligada a registrar a cada individuo, y a pedir autorización si la persona sólo va de visita, otorgándole mayor responsabilidad en su trabajo, y al mismo tiempo dándole el soporte tecnológico que necesita para poder tener un alto desempeño.

La tecnología ayuda en la transformación de los procesos actuales, permitiendo el fortalecimiento de la seguridad en todos los sectores, el apoyo absoluto al personal de seguridad, y obteniendo la confianza de los usuarios finales.

1.3 ALCANCE

- Diseñar un sitio web que gestione la venta de sistemas de seguridad biométricos.
- Venta en línea de los productos ofertados mediante carrito de compras.
- Elaboración del Análisis del Sistema de Acceso Vehicular y Peatonal basado en reconocimiento facial.

1.4 MISIÓN

Fortalecer el nivel de seguridad en el control de acceso de las ciudadelas privadas del país, utilizando la tecnología a través de sistemas biométricos de control de acceso, y personal técnico altamente calificado.

1.5 VISIÓN

Ser el referente nacional de sistemas de control de acceso en seguridad tecnológica de los hogares y empresas del país.

1.6 OBJETIVOS

1.6.1 OBJETIVOS GENERALES

Comercializar a través de nuestro portal web, sistemas biométricos de reconocimiento facial, para fortalecer el sistema de control y acceso de personas, otorgando seguridad y confianza a los hogares y empresas ecuatorianas.

1.6.2 OBJETIVOS ESPECÍFICOS

- Alcanzar el 10% de los hogares y el 5% de las empresas ecuatorianas al primer año de operaciones.
- Estar en el Top Five de las empresas que ofertan seguridad tecnológica para hogares y empresas ecuatorianas al 3er año de operaciones comerciales.
- Tener la tasa de rotación de personal más baja del mercado.
- Alcanzar una razón circulante de 2.50 al término del mes 24.

CAPITULO 2

2. MARCO TEORICO

2.1 BIOMETRÍA

La palabra biometría deriva del griego *bios* vida y *metron* medida, emplea uno o más rasgos conductuales de un ser humano con el fin de crear métodos de reconocimiento únicos de personas, ya que se basan en características intransferibles e irrepetibles de cada individuo. Los sistemas biométricos más utilizados actualmente son:

- Huella dactilar.
- Reconocimiento de voz.
- Reconocimiento de retina
- Reconocimiento del iris del ojo.

- Reconocimiento facial.
- Reconocimiento de los vasos sanguíneos de la mano o la geometría de la mano.

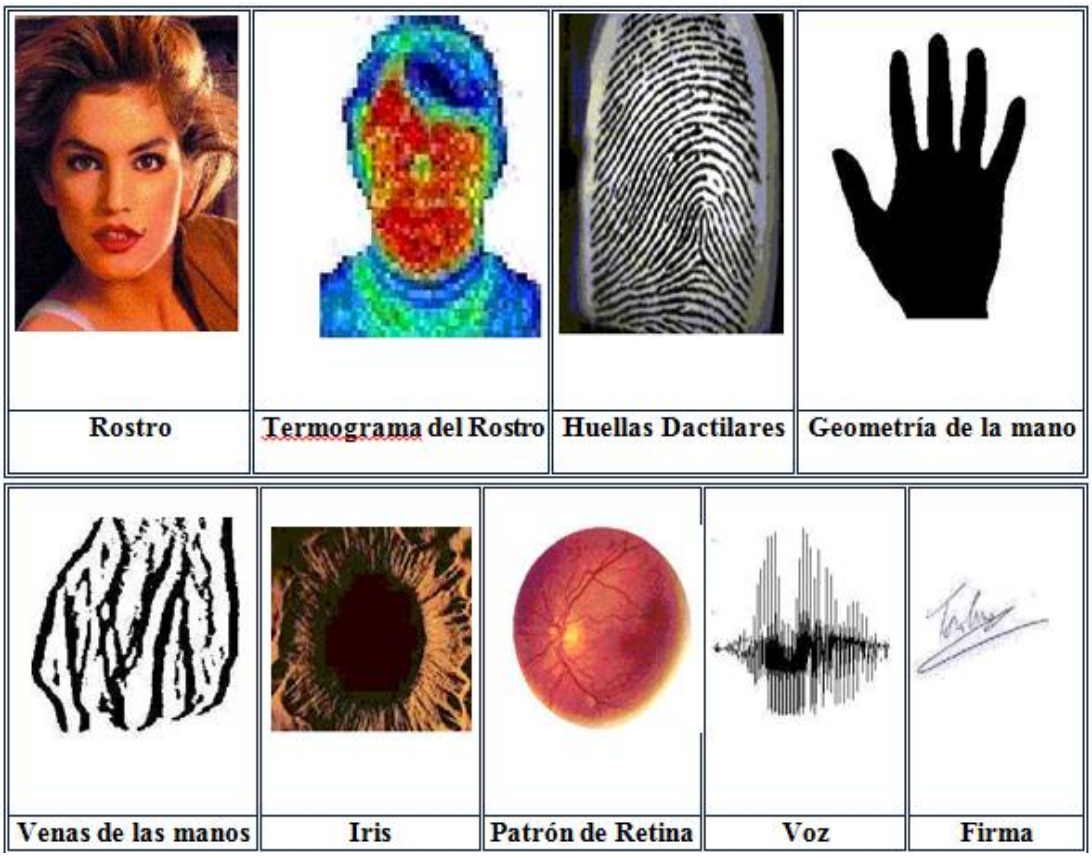


Figura 2.1: Tipos de Sistemas Biométricos

A continuación se define el procedimiento generalizado de reconocimiento biométrico:

- Adquisición de datos: características biológicas se adquieren para su posterior análisis.
- Modelado de datos: hay dos efectos en el modelado de datos, uno es para el almacenamiento y el otro es para verificar coincidencias. Los datos capturados son utilizados para ser almacenados en una base de datos para el reconocimiento futuro o para ser comparados con la base de datos existente.
- Toma de decisiones: los datos adquiridos para autentificación se comparan con la base de datos para tomar la decisión final de si o no ser reconocido. [14]

Los sistemas biométricos aún están en apogeo, a pesar de ello, estos sistemas están catalogados como excelentes ya que ayudan en la simplificación de los procesos de identificación de personas, ofrecen seguridad y comodidad a los usuarios, son sistemas fiables y su utilización no es compleja.

La biometría crece considerablemente de gobierno a gobierno y de gobierno a ciudadanos, los cuales requieren aplicaciones encaminados hacia la gestión de identidad ciudadana. Se han introducido en Filipinas y Malasia y Bangladesh, tarjetas biométricas de identificación nacional, implementando el voto electrónico basado en la biometría. Por lo que se puede concluir que la mayor cantidad de desarrollos biométricos están en las aplicaciones gubernamentales. Según un informe de investigación de mercado de International Biometric Group (IBG), se espera que el mercado de las tecnologías biométricas crezca de 3.4 billones en el 2009 a 9.3 billones de dólares en el 2014. [13]

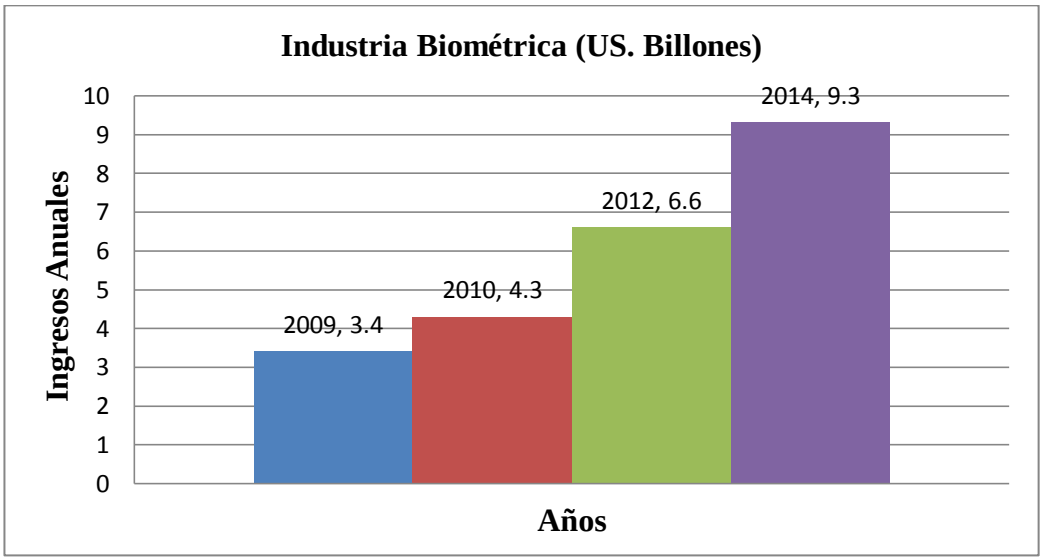


Figura 2.2: Ingresos Anuales de las industria biométrica [13]

Según el sitio web www.evaluandoerp.com, en las empresas las aplicaciones que más se utilizan los sistemas biométricos son para el Control de Accesos y/o Control de Presentismo. Entre los biométricos más utilizados se encuentran la geometría de la mano, reconocimiento facial o por medio de la huella digital. Tal como se indica en el gráfico a continuación:

Figura 2.3: Distribución de los métodos biométricos más usados. Fuente: www.evaluandoerp.com

2.2 APLICACIONES EN LAS QUE SE UTILIZA LA BIOMETRÍA

Los sistemas biométricos han evolucionado en diferentes ámbitos, existen países que los han implementado para cubrir deficiencias o para la agilización de procesos. En Ecuador se lo utiliza generalmente para el control de personal en las empresas, y en casos particulares para realizar compras en locales comerciales.

A continuación se detalla las áreas, en las que se están utilizando sistemas biométricos en diversos países.

ÁREAS	APLICACIONES ESPECÍFICAS
Biometría	Licencia de Conducir, Programas de Derecho, Inmigración, DNI, Pasaportes, Registro de Votantes, Fraude
Seguridad de la información	Inicio de Sesión, Seguridad en Aplicaciones, Seguridad en Bases de Datos, Cifrado de Información, Seguridad en Internet, Acceso a Internet, Registros Médicos, Terminales de Comercio Seguro, Cajeros Automáticos
Cumplimiento de	Video vigilancia Avanzada, Control CCTV, Control

la ley y vigilancia	Portal, Análisis Post-event, Hurto, Seguimiento de Sospechosos, Investigación
Tarjetas inteligentes	Valor Almacenado, Autenticación de usuarios
Control de acceso	Acceso a Instalaciones, Acceso a Vehículos

Tabla I: Aplicaciones Biométricas. Fuente: www.Wikipedia.com

En la tabla que se muestra a continuación, se ha realizado un cuadro comparativo de las características que poseen los diferentes sistemas biométricos, las mismas que pueden ser tomadas en cuenta al momento de escoger el biométrico que se ajuste a lo que se necesita implementar:

	Fiabilidad	Facilidad de uso	Prevención de ataques	Aceptación	Estabilidad
Ojo (Iris)	Muy alta	Media	Muy alta	Media	Alta
Ojo (Retina)	Muy alta	Baja	Muy alta	Baja	Alta
Huella dactilar	Muy alta	Alta	Alta	Alta	Alta
Vascular dedo	Muy alta	Muy alta	Muy Alta	Alta	Alta
Vascular mano	Muy alta	Muy alta	Muy Alta	Alta	Alta

Geometría de la mano	Alta	Alta	Alta	Alta	Media
Escritura y firma	Media	Alta	Media	Muy Alta	Baja
Voz	Alta	Alta	Media	Alta	Media
Cara 2D	Media	Alta	Media	Muy Alta	Media
Cara 3D	Alta	Alta	Alta	Muy Alta	Alta

Tabla II: Características de Sistemas Biométricos. Fuente: www.Wikipedia.com

2.3 COMPONENTES DE UN SISTEMA BIOMÉTRICO

Los principales componentes que se pueden identificar son:

- Sensor: Realiza la captura de los rasgos físicos de una persona, como huella dactilar, éstos varían dependiendo del tipo biométrico utilizado.
- Repositorio: Es el lugar o base de datos en la que se almacenan las plantillas biométricas las mismas que luego son utilizadas en el proceso de comparación.
- Algoritmos: Es el método que se utiliza para la extracción de características biométricas y su comparación con las plantillas almacenadas.

2.4 SISTEMAS BIOMÉTRICOS DE RECONOCIMIENTO FACIAL

Los sistemas de reconocimiento facial se basan en una técnica que realiza la verificación de la identidad de una persona a partir de una imagen. Para lograr ese objetivo, se utilizan programas de cálculo, los cuales son capaces de analizar imágenes de rostros humanos. Se realizan varias fotografías del rostro y se enfocan diferentes ángulos para obtener más detalles para una adecuada identificación y para permitir una búsqueda de coincidencias más precisa. Estos sistemas utilizan dispositivos que recogen puntos característicos del rostro de una persona, tales como las distancias entre ojos, distancia con nariz, labios etc.

Existen cuatro métodos que son empleados por los proveedores de reconocimiento facial. A continuación el detalle de ellos:

- Eigenface: Es una tecnología patentada en el Instituto de Massachusetts (MIT) que utiliza imágenes bidimensionales en escala de grises que representan características distintivas de una imagen facial, este método es capaz de operar con millones de caras en poco tiempo, su desventaja es que las imágenes capturadas deben ser frontales y en condiciones de luz similares.

- Análisis de características locales: Es la tecnología más utilizada en el reconocimiento facial. Esta tecnología está relacionada con Eigenface, pero es capaz de adaptarse mejor a los cambios en la apariencia o aspecto facial (sonriendo, frunciendo el ceño, etc.).

- Neural Network Mapping: En este método las redes neuronales emplean un algoritmo para determinar la similitud de las características únicas de la muestra adquirida y de la obtenida en el registro, utilizando tantas partes de la imagen facial como sea posible.

- Procesamiento automático de la cara: Es una tecnología más rudimentaria, que utiliza las ratios de distancia entre las características de fácil adquisición, tales como los ojos, la punta de la nariz y las comisuras de la boca. Aunque en general no es tan robusto como los demás métodos, puede ser más eficaz cuando la captura de imagen es frontal y en condiciones de poca luz.

Uno de los principales inconvenientes es su escasa resistencia al fraude, puesto que una persona puede modificar visualmente su cara de manera sencilla, como por ejemplo, utilizando unas gafas de sol o dejándose crecer la barba. Asimismo, debe considerarse que el rostro de las personas varía con la edad. [10]

2.5 VENTAJAS Y DESVENTAJAS

Existen dos tipos de dispositivos biométricos basados en reconocimiento facial, los cuales presentan variaciones en sus características, por ende también varían sus precios, dependiendo de las funcionalidades que posean. Estos son:

- Reconocimiento Facial en 2D
- Reconocimiento Facial en 3D

A continuación se presentan las ventajas y desventajas de cada uno de ellos:

2.5.1 BIOMÉTRICOS DE RECONOCIMIENTO FACIAL EN 2D

VENTAJAS	DESVENTAJAS
No invasivo	Precisión baja
Coste moderado	Ataque de gemelos
Cámara convencional	Potencial violación de privacidad
	Muy afectado por apariencias y entorno
	Posible funcionamiento encubierto

Tabla III: Ventajas de reconocimiento facial

2.5.2 BIOMÉTRICOS DE RECONOCIMIENTO FACIAL EN 3D

VENTAJAS	DESVENTAJAS
No invasivo	Coste elevado
Estable	Afectado por estado de salud
No afectado por cambios externos	Potencial violación de privacidad
Resistente a gemelos	Posible funcionamiento encubierto

Tabla IV: Desventajas de reconocimiento facial

2.6 FUNCIONAMIENTO

El proceso consta de cuatro fases principales:

- **Detección de la cara:** Este proceso detecta y localiza una cara en la imagen o video, sin identificarla. En el caso de un vídeo, se puede hacer un seguimiento de la cara, la misma que será identificada posteriormente.

- **Alineación de la cara:** Se detectan las características de la cara utilizando cálculos que realizan transformaciones geométricas, normaliza el rostro basándose en propiedades como el tamaño, la pose, y la iluminación del lugar. Para disminuir la carga del

procesamiento del software, se utilizan imágenes pequeñas en escala de grises.

- **Extracción de características:** Se proporciona información para distinguir entre las caras de diferentes personas según variaciones geométricas o de luz.

- **Reconocimiento:** El vector de características extraído se compara con los vectores de características extraídos de las caras de la base de datos. Si encuentra uno con un porcentaje elevado de similitud, nos devuelve la identidad de la cara; si no, nos indica que es una cara desconocida. [24]

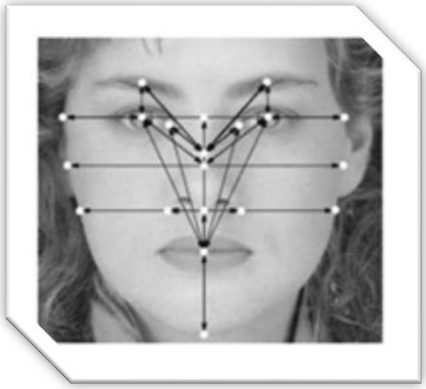


Figura 2.4: Representación del sistema de reconocimiento facial

2.7 ESTANDARES INTERNACIONALES

Los principales estándares existentes para las diferentes tecnologías se reflejan en la siguiente tabla:

ASPECTO	ESTANDARES
Imagen de la huella dactilar	• ISO/IEC 19794-4 Formatos de intercambios de datos biométricos. Parte 4: Información de imagen facial. • ASNI INCITS 381-2004 Formato de intercambio de información del dedo.
Minucia de la huella dactilar	• ISO/IEC 19794-2 Formatos de intercambio de datos biométricos. Parte 2: Información de la minucia de la huella dactilar. • ANSI INCITS 378-2004 Formato de la minucia del dedo para intercambio de datos. • ANSI INCITS 377-2004 Formato de intercambio de la información básica del patrón dedo.
Reconocimiento facial	• ANSI INCITS 385-2004 Formato de

	reconocimiento facial para intercambio de datos. • ISO/IEC 19794-5 Formatos de intercambio de datos biométricos- Parte 5: Información de la imagen facial.
Reconocimiento de iris	• OSP/IEC 19794-6 Formato de intercambio de datos biométricos-Parte 6: Información de la imagen del iris. Añadir una guía de implementación para especificar el uso de representación cartesiana.
Otras tecnologías	• ANSI/NIST ITL 1-2000 Formato de la información para el intercambio de huella dactilar, facial cicatrices y tatuajes (SMT). • INSI/NIST ITL 1-2007 Formato de la información para el intercambio de huella dactilar, facial y otro tipo de datos biométricos-Parte 1. • ANSI INCITS 396-2005 Formato para el intercambio de datos de la geometría de la

	mano. • ANSI INCITS 395-2005
Interfaces técnicos	• ISO/IEC 19784-1 BIOAPI- Interfaz de programación de la aplicación biométrica – Parte 1: Especificación BioAPI. • ISO/IEC 19784-2 Interfaz de programación de la aplicación biométrica (BioAPI) – Parte 2: Interfaz del proveedor del archivo biométrico. • ISO/IEC 19785-1:2006: Marco común de intercambio de formatos biométricos- Parte 1: Especificación de los elementos de la información. • ISO/IEC 19785-2: 2006: Marco común de intercambio de formato biométricos- Parte 2: Procedimientos para la autorización de registros biométricos. • ANSI INCITS 358-2002 Especificación BioAPO (Version 1.1). • ANSI INCITS 398-2005 [NISTIR 6529-A].

	Marco común de intercambio de formatos biométricos. (CBEFF)
Rendimiento	• ANSI INCITS 409.1-2005 Reporte y testeo del rendimiento biométrico-Parte 1: Principios y marco. • ANSI INCITS 409.2-2005 Reporte y testeo del rendimiento biométrico. Parte 2: Reporte y testeo de la tecnología. • ANSI INCITS 409.3-2005 Reporte y testeo del rendimiento biométrico. Parte 3: Reporte y testeo del escenario. • ANSI INCITS 409.4 Reporte y testeo del rendimiento biométrico.

Tabla V: Estándares existentes. Fuente: Estudio sobre las tecnologías biométricas aplicadas a la seguridad Edición Diciembre 2011

La tecnología de reconocimiento facial está siendo utilizada para combatir el fraude de pasaportes, soporte al orden público, identificación de niños extraviados y minimizar el fraude en las identificaciones, las cuales puede ser de fácil clonación o robo.

Nuestra propuesta consiste en mejorar la protección no solo a empresas sino también a los hogares ecuatorianos, con el único fin de asegurar el bienestar de las familias que habitan en ellas.

CAPITULO 3

3. ANÁLISIS DEL MERCADO

3.1 MERCADO PRIMARIO

Una vez obtenida la información necesaria para establecer la demanda del mercado y los objetivos de la empresa, se define al mercado primario como el grupo potencial que más acerca su perfil al de nuestros productos, siendo sus principales características, su ubicación en ciudadelas privadas, las cuales requieren fortalecer sus sistemas de seguridad actuales y mejorar el control de acceso de personas y vehículos.

Mercado Primario: Ciudadelas privadas de clase media y alta; y, empresas del país.

3.2 ANÁLISIS DE LA SITUACIÓN ACTUAL

Según el censo de población y vivienda que realizó el Instituto Nacional de Estadísticas y Censos (INEC) en el año 2010, se informó que en la provincia del Guayas hay construidas aproximadamente 797,066 casas/villas. Tal como se indica a continuación:

Tipo de Vivienda - Provincia del Guayas

Tipo de Vivienda	Casos	%	Acum.%
Casa / Villa	797,066	73.94	73.94
Departamento en casa o edificio	102,375	9.5	83.44
Cuarto(s) en casa de inquilinato	41,188	3.92	87.26
Mediagua	34,089	3.16	90.42
Rancho	79,525	7.38	97.80
Covacha	14,610	1.36	99.16
Choza	2,739	0.25	99.41
Otra vivienda particular	5,601	0.52	99.93
Hotel, pensión, residencial u hostal	174	0.02	99.95
Cuartel Militar o de Policía/Bomberos	75	0.01	99.95
Centro de rehabilitación social/Cárcel	27	0.00	99.96
Centro de acogida y protección para niños y niñas, mujeres indigentes	19	0.00	99.96
Hospital, clínica, etc.	78	0.01	99.96

Convento o institución religiosa	88	0.01	99.97
Asilo de ancianos u orfanato	16	0.00	99.97
Otra vivienda colectiva	213	0.02	99.99
Sin vivienda	64	0.01	100
TOTAL	**1,077,947**	**100**	**100**

Tabla VI: Censo Año 2010. Fuente: INEC [9]

Tomando como ejemplo la provincia del Guayas, y por observación directa se puede afirmar que en los últimos años ha crecido extraordinariamente en todas direcciones, para citar algunos ejemplos tenemos ciudadelas privadas construidas en los cantones de Samborondón, Durán, Nobol, Yaguachi, Daule, Vía a la Costa, etc. Todo este crecimiento se le atribuye mayormente a las inmobiliarias, que son las que han impulsado la ampliación de ésta y varias ciudades del país.

Varios proyectos inmobiliarios han contribuido con la población de zonas que antes parecían inhóspitas y alejadas, muchas familias especialmente guayaquileñas han cambiado la agitada y ruidosa ciudad, por espacios verdes, clubes privados, piscinas, y aspiraron a tener un mejor ambiente con seguridades y comodidades. Sin embargo, muchas de esas ilusiones han

tomado otro rumbo debido a la inseguridad que se ha hecho notar en todo el país.

Durante el año 2012, la Fiscalía de Guayaquil a través de un estudio realizado por la Escuela Superior Politécnica del Litoral ESPOL, informó que el número de denuncias por delitos contra la propiedad y contra las personas ascendió a 15,247. Lo que representa el 49.7% de las denuncias totales realizadas por la ciudadanía.

Denuncias Receptadas en las oficinas del Ministerio Público de Guayaquil (AÑO 2012)

CATEGORIA DE DELITO	NUMERO DE DENUNCIAS	PORCENTAJE
Principales delitos contra las Personas	8129 (9731)	26.50%
Principales delitos contra la Propiedad	7118 (6912)	23.20%
Suma de Principales delitos	15247 (16650)	49.70%
Otras Denuncias	15434 (17802)	50.30%
TOTAL DE DENUNCIAS RECEPTADAS EN 2012	**30681 (34452)**	**100.00%**

Tabla VII: Denuncias Año 2012

Según las estadísticas proporcionadas por el Observatorio de Seguridad Ciudadana de Guayaquil, informa que de enero a noviembre del 2012 se registraron 396 casos de robos en ciudadelas privadas. El 90% fue bajo la modalidad de estruche y el 10% restante corresponde a robo agravado, en los tres primeros meses de 2013, en relación con el mismo periodo de 2012, los delitos en Guayaquil tuvieron un aumento comparativo de casi el 50 por ciento, según el Sitio web de un medio local. [4]

El nivel de delincuencia en el país hace que las personas y empresas necesiten protegerse a través de diferentes mecanismos. En la actualidad los sistemas de seguridad tienen el compromiso de ser cada vez más confiables para el mercado, por esta razón se ofrecen soluciones con sistemas biométricos, que se basan en el reconocimiento de rasgos físicos, los mismos que son de difícil reproducción, por lo tanto, son sistemas más confiables que los comúnmente usados.

A nivel mundial la biometría se aplica en varios sectores, el nivel tecnológico es alto, y la exploración de nuevos métodos y de mejoras en el campo biométrico están en todo su apogeo, estos sistemas son utilizados en aeropuertos, control de migración, sistemas de pago a través de huella

digital, voto electrónico, son algunos de los ejemplos que podemos mencionar.

En Ecuador, se está implementando la biometría en las entidades gubernamentales, uno de los ejemplos es La Seguridad Portuaria Biométrica, que permite el registro de personal autorizado para que puedan tener acceso a determinadas áreas dentro de la Aduana, sean estos proveedores, trabajadores, administradores, etc.; otro ejemplo, es el campo judicial ecuatoriano, están utilizando la biometría para la Identificación de Delincuentes Reincidentes, esto lo hacen a través de archivos de grabaciones de voz y fotografías de las personas con antecedentes penales. [5]

Según un estudio realizado por la empresa Biometría de Argentina, se estima que en América Latina hay más de 538 millones de registros dactilares. Se calcula que el 37 por ciento de estos registros es utilizado para fines electorales, y 45 por ciento es para los fines de garantizar la identidad de beneficiarios de servicios sociales. “Tan sólo el restante 18 por ciento es para fines de seguridad policial, migratoria y otras funciones relacionadas.” [1]

3.3 ANÁLISIS FODA

A continuación se expone el análisis de las fortalezas y debilidades prevalecientes, así como de las oportunidades y amenazas que se generan, con el fin de plantear estrategias que conduzcan hacia los objetivos propuestos.

Fortalezas

- El producto es un dispositivo que combina los parámetros biométricos con el reconocimiento facial, utilizando métodos aprobados y reconocidos a nivel mundial.
- Los sistemas biométricos son más seguros que los dispositivos actuales en el mercado.
- Estamos en la vanguardia de la tecnología, lo que nos ayuda a ser más eficientes en temas de seguridad.
- A diferencia de otras tecnologías biométricas como las de tipo de iris o huella dactilar, el reconocimiento facial es no intrusiva y no necesita de colaboración por parte del usuario. Solo es necesario que su rostro sea capturado por una cámara.

- Al no tener contacto el dispositivo con ninguno de los usuarios, se cuida su salud de enfermedades virales.

Debilidades

- Aversión a la tecnología.
- Costo del biométrico de reconocimiento facial es más elevado que los de otros existentes, como es el caso del biométrico de huella dactilar.
- El mantenimiento de los sensores de los biométricos puede ser costosos.

Oportunidades

- Mayor protección y confianza, las ciudadelas privadas y empresas no cuentan con un sistema biométrico para el control de acceso de personas y vehículos, lo común es usar tarjetas o que el guardia verifique los documentos de la persona que ingresa.
- El nivel de delincuencia en lugares alejados de la ciudad crea la necesidad de protección y de sistemas de seguridad confiables.

- Los sistemas biométricos de reconocimiento facial, son un campo poco explotado en nuestro medio, lo que podría convertirse es una gran ventaja.

Amenazas

- Competidores existentes y el ingreso de nuevos competidores.
- En el mercado existen sistemas biométricos más utilizados que el sistema de reconocimiento facial.
- Que exista una mayor confianza en contratación de personal de seguridad.
- Cambio acelerado de la tecnología, por lo que los equipos pueden quedar obsoletos, en poco tiempo.

3.4 CADENA DE VALOR

Figura 3.1: Cadena de Valor de un Sitio Web

3.4.1 ACTIVIDADES PRIMARIAS

3.4.1.1 LOGÍSTICA DE ENTRADA

La empresa para funcionar, mantenerse y competir en el mercado, necesita de:

- Los clientes potenciales, que estarían en las ciudadelas privadas y empresas con parqueo privado.

- Dispositivos Biométricos, necesarios para la implementación del sistema de control de acceso de personas y vehículos.

3.4.1.2 OPERACIONES

La empresa desarrollará el Sistema Biométrico de Reconocimiento Facial para controlar el acceso de peatones y de vehículos, de esta forma se logrará el aumento de las ganancias de la empresa, y se mejorará el nivel de satisfacción de los clientes, ya que se puede personalizar el sistema con las necesidades que ellos tengan, sin depender de terceros.

3.4.1.3 MARKETING Y VENTAS

Para apoyar a las actividades de Marketing y Ventas, se ha implementado un Sitio Web, el cual proporcionará información de:

- La empresa.
- Productos que se ofertan.
- Promociones y eventos.
- Recordación de Marca.

- Compras en línea.

Esto con el fin de lograr captar clientes, y de crear la fidelización de los que clientes que poseemos.

3.4.1.4 LOGÍSTICA DE SALIDA

Debido a que el producto es no perecible, pero son aparatos delicados para su transportación, estos deben ser correctamente embalados para evitar daños.

3.4.1.5 SERVICIO POST-VENTA

Para mejorar la calidad del servicio se proporcionará a los clientes asistencia en:

- Soporte Técnico.
- Garantías por equipos vendidos.
- Cambios en el software por requerimientos adicionales de los usuarios.

- Mantenimiento preventivo y correctivo de los equipos.

3.4.2 ACTIVIDADES SECUNDARIAS

3.4.2.1 INFRAESTRUCTURA DE LA EMPRESA

La empresa posee el Sitio Web www.seguridadbio.com, el cual está alojado en un servidor compartido en www.godaddy.com, el Sitio es gestionado por el administrador del Sitio Web de la organización, está basado en PHP y posee como base de datos MySql.

El Sitio Web está disponible, y su uso es sencillo ya que al ofertar un producto específico se proporciona información del mismo, usted puede solicitar demostraciones para que se pueda observar su funcionamiento. La empresa posee en su Sitio Web compras en línea, para mayor comodidad y seguridad.

El sitio web está habilitado 24 horas, 7 días a la semana, nuestros horarios de oficina y de atención al cliente serán de lunes a viernes, de 09:00 a 18:00.

Aunque en casos particulares que el cliente lo requiera se podría pactar un horario distinto al establecido, el cual debe ser confirmado con anticipación.

3.4.2.2 TECNOLOGÍA, INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

El sitio web cuenta con seguridad SSL, que provee protección a los datos que viajan a través de la red, para lo cual se contrató un protocolo de seguridad o sitio seguro en VeriSign. Se busca captar la confianza de los clientes al realizar compras en línea, y garantizar la seguridad de toda la información proporcionada, evitando el fraude.

3.4.2.3 GESTIÓN DE COMPRAS

Se realizará una Planificación de las compras que se deben realizar basándose en las demandas de los productos, con el fin de contar con el stock disponible para las ventas pronosticadas en un periodo determinado, es necesario que los proveedores sean calificados, que tengan garantía en sus productos y que sean puntuales con los envíos de los dispositivos solicitados.

3.4.2.4 GESTIÓN DE COMPETENCIAS Y RECURSOS HUMANOS

Seguridad Biométrica está legalmente constituida respetando todas las reglas y normativas que posee la Superintendencia de Compañías, está registrada como Sociedad Anónima en nuestro país, además está debidamente afiliada a la Cámara de Comercio, e inscrita bajo número patronal en el Instituto Ecuatoriano de Seguridad Social, por lo que todos nuestros colaboradores están debidamente afiliados y obtienen los beneficios que por ley les corresponden. En el Servicio de Rentas Internas se obtuvo el R.U.C. (Registro Único de Contribuyente) que nos permite la emisión de los documentos legales por los servicios que sean solicitados por los clientes.

Con el fin de mejorar el servicio que se provee a los clientes, la empresa tiene como política capacitar al personal, orientándose a las nuevas tecnologías, y enfocándose en la resolución de problemas que reporten los clientes, así como los posibles inconvenientes en los dispositivos que se utilicen o el desarrollo de nuevos requerimientos que se soliciten.

3.5 ESTRATEGIAS

Se persigue como objetivo principal el ser percibido como un sistema de seguridad en el control de acceso a ciudadelas privadas o sectores que demanden un nivel de seguridad confiable.

3.5.1 LANZAMIENTO DEL PRODUCTO

Para conseguir que el producto se convierta en uno de los principales sistemas de seguridad biométricos en el país, nos apoyaremos en varias estrategias de promoción, con el fin de llegar a nuestros clientes potenciales para que conozcan el producto, y los beneficios que ofrecemos, para alcanzar este objetivo realizaremos las siguientes actividades:

- Implementar un sitio web en el que se levantará toda la información referente al producto.
- Realizar una estrategia comunicacional utilizando correos electrónicos masivos, con estándares IAB (InteractiveAdvertasingBoreu) para evitar

ser considerado como correo no deseado y asegurar la recepción y lectura de la información.

- Utilizar volantes para promocionar y fomentar el acceso al sitio web.
- Utilizar medios de comunicación gratuitos para la difusión del sistema, como son las redes sociales y YouTube, junto a estrategias de marketing viral.

3.5.2 PLAN OPERATIVO (MARKETING MIX)

3.5.2.1 Cliente satisfecho

Una de las tareas que se debe manejar con cautela en cualquier empresa es el tema del servicio al cliente. Todos reconocen que éste es un aspecto muy importante para su éxito, por lo que se puede decir que dependemos de la fidelidad de nuestros compradores y de satisfacer sus necesidades de manera eficiente, en cada una de las sugerencias, problemas y demás situaciones en las que ellos soliciten nuestra ayuda.

Luego de que las ventas de los dispositivos se hayan concretado, se dará atención adicional y personalizada a los clientes, con el fin de que informen el nivel de satisfacción del servicio, saber que necesitan y en que podemos mejorar, además de ofertar nuestros nuevos productos o servicios.

La información que nos proporcionen nos permitirá la mejora continua del producto, así como del servicio, e incluso para poder abrir nuestras perspectivas basándonos en lo que el cliente necesita.

3.5.2.2 Precio

Conocer los precios probables es importante, porque es la base para el cálculo de los ingresos futuros. Se recomienda fijar los valores máximos y mínimos probables del precio unitario de venta.

Entre las principales referencias para fijar el precio se encuentra:

- Los costos, basándonos en lo que nos cuesta producir y comercializar cada producto o servicio.

- Precio Objetivo, se establece como punto de partida el precio de venta del mercado, y se ajusta el precio basándonos en los costos de la elaboración del producto.
- Precio de referencia del mercado, sobre la base del producto y el tipo de mercado en el que se inserta el proyecto se elige y justifica el precio que estime correcto.
- Precio Comercial, es aquel que utilizan la mayoría de las empresas y es el resultado de un análisis del ciclo de vida del producto, grado de diferenciación del producto, confianza del comprador respecto al mismo, amenazas de la competencia.

3.5.2.3 Canales de distribución

La empresa se encargará de la *COMERCIALIZACION* del producto a través del Sitio Web www.seguridadbio.com. La negociación se realizará directamente con el cliente. Se considerará como objetivos para la distribución del producto, las ciudadelas privadas y las empresas del país.

3.5.2.4 Comunicación

Una vez que se han determinado los servicios que se van a ofrecer, el precio y el canal de acceso, nos enfocaremos en dar a conocer, informar y convencer al mercado de que le producto que se oferta es la solución a sus problemas de seguridad y que puede ser implementado en cualquier lugar en el que se desea reforzar la vigilancia y seguridad.

3.5.2.5 Promoción

Utilizaremos como herramienta principal para la promoción, el Sitio Web www.seguridadbio.com, el mismo que ha sido diseñado para que las personas interesadas puedan conocer el producto, dentro de la misma tendremos enlace con las redes sociales más comunes en nuestro medio, tales como Facebook, Twitter, etc. Para que puedan conocer el producto, se buscará realizar alianzas estratégicas con las empresas constructoras e inmobiliarias para poder ofertar el producto a los residentes de las ciudadelas, para que puedan estar informados de los beneficios que obtendrían al adquirirlo.

Se otorgará un 10% de descuento a los clientes que adquieran el producto dentro del primer mes de lanzamiento. Si nuestros clientes traen a una persona referida, y se efectiviza la compra se pagará una comisión del 5%, esto solo será válido por tiempo limitado, esto permitirá la creación de una red de promoción basándose en las experiencias que nuestros clientes transmiten a otros individuos que podrían interesarse en conocer nuestro producto.

3.5.3 POLÍTICAS DE COMERCIALIZACIÓN

Se han elaborado las siguientes políticas, para que se conozcan los detalles de los compromisos que adquieren tanto el cliente como la empresa:

3.5.3.1 Políticas de pago

3.5.3.1.1 Pago al Contado

Se considerará el 10% de descuento sobre el valor total de la venta, se entenderá como pago de contado a la cancelación total de la compra en una sola transacción comercial previa contratación e instalación del producto.

3.5.3.1.2 Pago Crédito

Los períodos de crédito otorgados a los clientes serán de 3, 6 y 9 meses calendarios, el valor inicial será del 50% previa contratación e instalación del producto, al 50% restante se le aplicará la correspondiente tasa de interés bancario vigente para 3, 6 y 9 meses de crédito.

3.5.3.2 Políticas de venta

La venta de producto puede ser realizada en línea en el sitio web nuestra empresa, puede ser solicitada a través de las demostraciones que se realizan en diferentes sectores de la ciudad, o directamente en nuestras oficinas, en el Sitio Web se detallan las características de los productos, por lo que es responsabilidad del cliente que se informe antes de adquirirlo.

La venta del producto incluye el hardware y el software requeridos para el funcionamiento del dispositivo, además se incluyen los reportes predeterminados del sistema, los mismos que pueden ser personalizados, dependiendo de los requerimientos solicitados. En el caso de solicitar funciones adicionales o cambios en el funcionamiento del dispositivo, tendrán un recargo adicional, el cual dependerá de lo que se requiera y que será informado al solicitante para su aprobación.

La implementación del proyecto comenzará 48 horas después de la firma del contrato. Una vez finalizada la implementación se entregará al cliente la documentación respectiva, esto es: manuales, software, y el dispositivo instalado.

3.5.3.3 Capacitación

El proveedor proporcionará al cliente la capacitación exclusiva para el uso del sistema mediante 1 curso de 3 horas de duración, impartidos a 3 personas, en el que se harán pruebas con el fin de que el personal se familiarice con el entorno que debe utilizar. La capacitación no incluye impartir conocimiento de la instalación del equipo ni del sistema operativo, si esto fuera necesario

sería motivo de una cotización especial. El cliente designará al personal que asistirá.

3.5.3.4 Políticas de Devoluciones

No se aceptarán devoluciones, a excepción que se trate de causas establecidas en el contrato o fallas técnicas en el equipo entregado lo cual debe ser debidamente comprobado.

En caso de que el cliente decline contratación del producto, se retendrá el 10% sobre el valor de la compra para cubrir los gastos operativos y administrativos efectuados durante la negociación.

3.5.3.5 Mantenimiento

Al vencimiento del periodo de garantía, el cliente podrá celebrar con el proveedor un contrato de mantenimiento que le permite solicitar nuevas versiones o actualizaciones, de conformidad con los términos, condiciones y precios que ambas partes determinen en ese momento.

3.5.3.6 Garantía

Los equipos tendrán la garantía que el proveedor haya dispuesto, una vez terminado este tiempo el cliente no tiene opción a ningún tipo de reclamo por fallas de los mismos. El cliente cuenta con tres meses a partir de la fecha de terminación e instalación del sistema de seguridad para reportar fallas o errores exclusivos del sistema, en este caso el proveedor atenderá inmediatamente las reclamaciones del cliente y efectuará las correcciones que resulten necesarias, sin cargo adicional.

3.5.3.7 Servicio Post Venta

En caso de reclamos por garantía de hardware, la empresa se compromete a realizar el trámite respectivo con los proveedores. Además realizamos la venta de dispositivos nuevos que pueden servir para el reemplazo de dispositivos que no estén funcionando correctamente y que ya no cuenten con garantía. Además la empresa cuenta con servicio de mantenimiento preventivo y correctivo de los equipos con el fin de garantizar el funcionamiento del mismo.

3.5.3.8 Políticas de servicio

Los horarios de atención al cliente serán de lunes a viernes, de 09:00 a 18:00. Aunque en el caso de que el cliente lo requiera se podría pactar un horario distinto al establecido, el cual debe ser confirmado con anticipación.

CAPITULO 4

4. SITIO WEB

Para que el sistema de seguridad biométrico sea reconocido en todo el Ecuador se ha desarrollado un Sitio Web, www.seguridadbio.com, a través del cual se pretende llegar a más personas y empresas a nivel nacional, con el fin de aumentar nuestras ventas, y lograr el cumplimiento de todos los objetivos planteados como empresa.

Para el desarrollo del Sitio Web se emplearán las herramientas que se detallan a continuación:

4.1 SERVIDOR HTTP APACHE

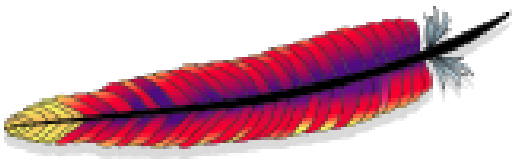


Figura 4.1: Logo Apache

El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. [25]

Se ha optado por utilizar Apache, debido a que es un software libre, eso nos permitirá minimizar costos por licenciamiento, además que presenta características altamente configurables, y una potente base de datos que nos permitirá explotar los recursos de esta herramienta, que es muy utilizada por los desarrolladores de software en la mayoría de las aplicaciones web que existen.

Ventajas

- Modular

- Código abierto
- Multi-plataforma
- Extensible
- Popular (fácil conseguir ayuda/soporte)

4.2 OSCOMMERCE

Figura 4.2: Logo OsCommerce

OsCommerce es un programa de comercio electrónico y administración online. Desarrollado en PHP por Harald Ponce de Leon y lanzado el 12 marzo de 2000, requiere de una base de datos MySQL y un servidor Apache.

En el 2012 se encuentran activas 12.704 tiendas virtuales bajo OsCommerce según la página oficial. Tiene posibilidad de instalar un gran número de idiomas. Como adicional se encuentra en el panel de control de páginas web para su instalación automática.

Características Generales de una Tienda en Línea basada en OsCommerce

Los pedidos, clientes y productos se almacenan en una base de datos de fácil consulta vía administración-web.

- Los clientes podrán comprobar el histórico y el estado de sus pedidos una vez registrados.
- Los clientes pueden cambiar sus datos de perfil de usuario desde su apartado cliente.
- Múltiples direcciones de envío por usuario.
- Búsqueda de productos.
- Posibilidad de permitir a los usuarios valorar los productos comprados, además de comentarlos.
- Posibilidad de implementar un servidor seguro (SSL).
- Puede mostrar el número de productos en cada una de las categorías.
- Lista global o por categoría de los productos más vendidos y más vistos.
- Fácil e intuitiva navegación por categorías.
- Plataforma multi-idiomas, por defecto estarán disponibles en español, inglés y alemán.

4.3 PHP

Figura 4.3: Logo PHP

PHP 5 *(PHPHypertext Pre-processor)*, es un lenguaje de programación, originalmente diseñado para el desarrollo web de contenido dinámico. PHP puede ser usado en la mayoría de los servidores web al igual que en casi todos los sistemas operativos y plataformas sin ningún costo.

Características

- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos.
- Es considerado un lenguaje fácil de aprender.
- El código fuente escrito en PHP es invisible al navegador web y al cliente. Esto hace que la programación en PHP sea segura y confiable.
- Capacidad de conexión con la mayoría de los motores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL y PostgreSQL.

- Posee una amplia documentación en su sitio web oficial.
- No requiere definición de tipos de variables aunque sus variables se pueden evaluar también por el tipo que estén manejando en tiempo de ejecución.

4.4 MYSQL

Figura 4.4: Logo MySQL

MySQL es un sistema de gestión de bases de datos relacional, multihilo y multiusuarios. Entre las características disponibles en las últimas versiones se puede destacar:

- Amplio subconjunto del lenguaje SQL. Algunas extensiones son incluidas igualmente.
- Disponibilidad en gran cantidad de plataformas y sistemas.

- Posibilidad de selección de mecanismos de almacenamiento que ofrecen diferente velocidad de operación, soporte físico, capacidad, distribución geográfica, transacciones.

4.5 PERFILES DE ACCESO AL SITIO WEB.

En el sitio web www.seguridadbio.com, se permitirá el acceso bajo dos perfiles, dependiendo de cada uno de ellos se podrán visualizar diferentes opciones. El detalle a continuación:

- Interfaz para Clientes
    - Visualizar el contenido del Sitio Web.
    - Conocer el catálogo de productos.
    - Realizar compras en línea (Carro de Compras).
    - Efectuar sugerencias o comentarios.
    - Solicitar demostraciones de productos.
- Interfaz para usuarios Administradores
    - Permitirá editar el contenido en el Sitio web.
    - Agregar/Modificar/Eliminar categorías de productos.

- Agregar/Modificar/Eliminar productos.
- Administrar clientes.
- Verificar las transacciones realizadas.
- Configuración del Sitio Web.
- Modificación de las páginas que conforman el Sitio Web.

4.6 REQUERIMIENTO TECNICO

4.6.1 Servidor

El servicio de alojamiento (Hosting) es proporcionado por GoDaddy.

GoDaddy es un proveedor de hosting para sitios web, almacena el sitio www.seguridadbio.com en su servidor y le brinda una dirección única (DNS). A través de esta dirección, las personas de todo el mundo pueden encontrar, abrir e interactuar con tu sitio.

4.6.2 Cliente

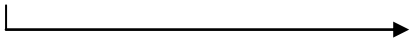
Son todas las personas que tengan acceso a Internet, y que hayan instalado un browser en su computador. Para que puedan acceder al Sitio Web www.seguridadbio.com, e informarse de los productos y promociones publicadas.

4.7 ESTANDARIZACIÓN DEL SISTEMA

4.7.1 ESTÁNDARES PARA ALMACENAMIENTO DE INFORMACIÓN

Nombre de la Base de datos

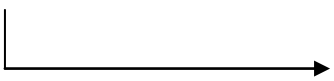
XXXXXXXXX



Nombre descriptivo de la Base de datos.

Nombre de Tablas

XXXXXXXXXXXXXXXX



Nombre descriptivo de la tabla de máximo 24 caracteres.

Nombre de campos

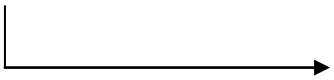
XXXXX_XXXXXXXXXX

Descriptivo del campo. De ser mayor a una palabra, la primera se separará del resto con un sub-guión. Máximo 24 caracteres.

Nombre de Índices

Primary Key

PK_XXXXXXX_XXXXXXXX



Letras PK para identificar el Primary Key, seguido del nombre o referencia a de la Tabla.

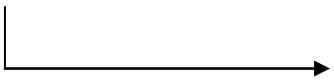
Foreign Key

FK_XXXXXXX_XXXXXXXX

Letras FK para identificar el Foreign Key, seguido del nombre de la Tabla origen, sub-guion y el nombre de la tabla destino.

Checks

CK_XXXXXXX

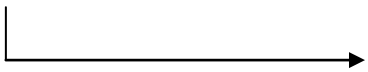


Letra CK para identificar el Check, seguido del nombre del campo.

4.7.2 FORMATOS PARA ELEMENTOS DEL SISTEMA

Nombre de páginas web.

XXXXXXXXXXXXXXXXXXX



Nombre de la página, en español, en minúsculas.

Secciones de páginas

XXXXXXXXXXXXXXXXXXX

Nombre de la página, en español, en minúsculas.

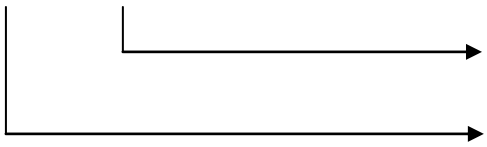
Separador(sub-guión)

Código Mnemónico de 3 caracteres.

Las Secciones de página determinan la función de la misma en el sitio web, por ejemplo ingresar o modificar datos o grabar archivos.

Nombre de Funciones.

PREF_XXXXXXX_XXXXXXXXX

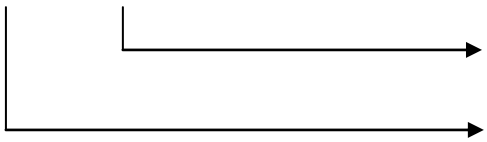


Nombre descriptivo de la función.

Prefijo Nemónico.

Nombre de Procedimientos.

PREF_XXXXXXX_XXXXXXXXX



Nombre descriptivo del procedimiento.

Prefijo Nemónico.

Nombre de variables

XXXXXXXXX_XXXXXXXXXXX

Nombre descriptivo del control Nombre descriptivo del control de la página web.

Si es mayor a una palabra, se dividirá por un sub-guión.

4.8 ESTRUCTURA DEL SITIO WEB

El sitio web SeguridadBio.com, ha sido diseñado con la estructura que se detalla a continuación:

4.8.1 ESTRUCTURA DE LA PAGINA PRINCIPAL

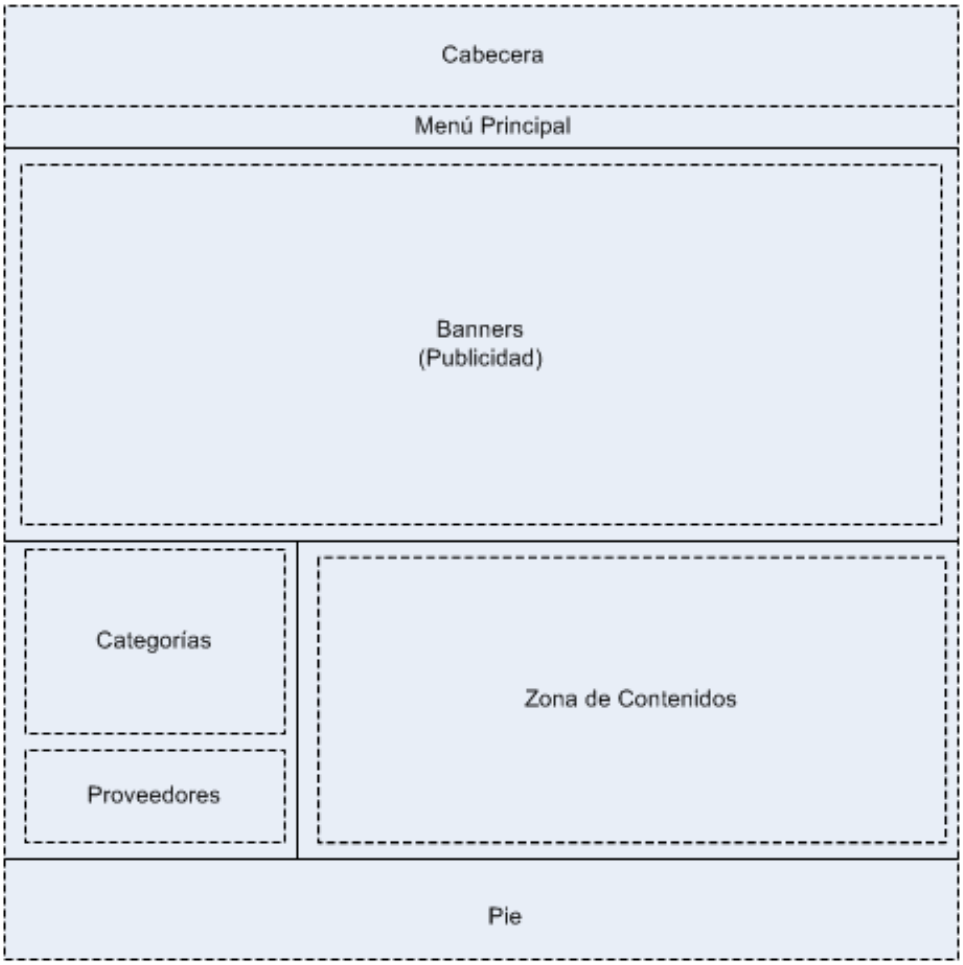


Figura 4.5: Estructura Sitio Web

- **Cabecera:** Incluye el logo de la empresa, el logo del carro de compras y el número de productos que se están solicitando, también contiene el menú y la opción de búsquedas rápidas.

- **Banners:** Posee un área donde se muestra la publicidad relacionada a las actividades de la empresa así como de los productos relevantes que se promocionan constantemente.
- **Categorías:** Se listan todas las clases de productos que la empresa oferta a sus clientes.
- **Proveedores:** Menú de fabricantes, proveedores, y los enlaces a sus sitios web.
- **Zona de contenidos:** Es la zona dedicada a presentar la información de cada página.
- **Pie:** Posee el menú principal, copyright, año de creación de la página.

El código fuente del Sitio Web es propiedad de la empresa, con lo que se asegura que se puedan realizar todas las modificaciones que sean necesarias para personalizarlo, permitiendo el mejoramiento continuo de nuestro Sitio.

A continuación se muestran imágenes que corresponden al Sitio web www.seguridadbio.com

4.8.2 PÁGINA PRINCIPAL DEL SITIO WEB

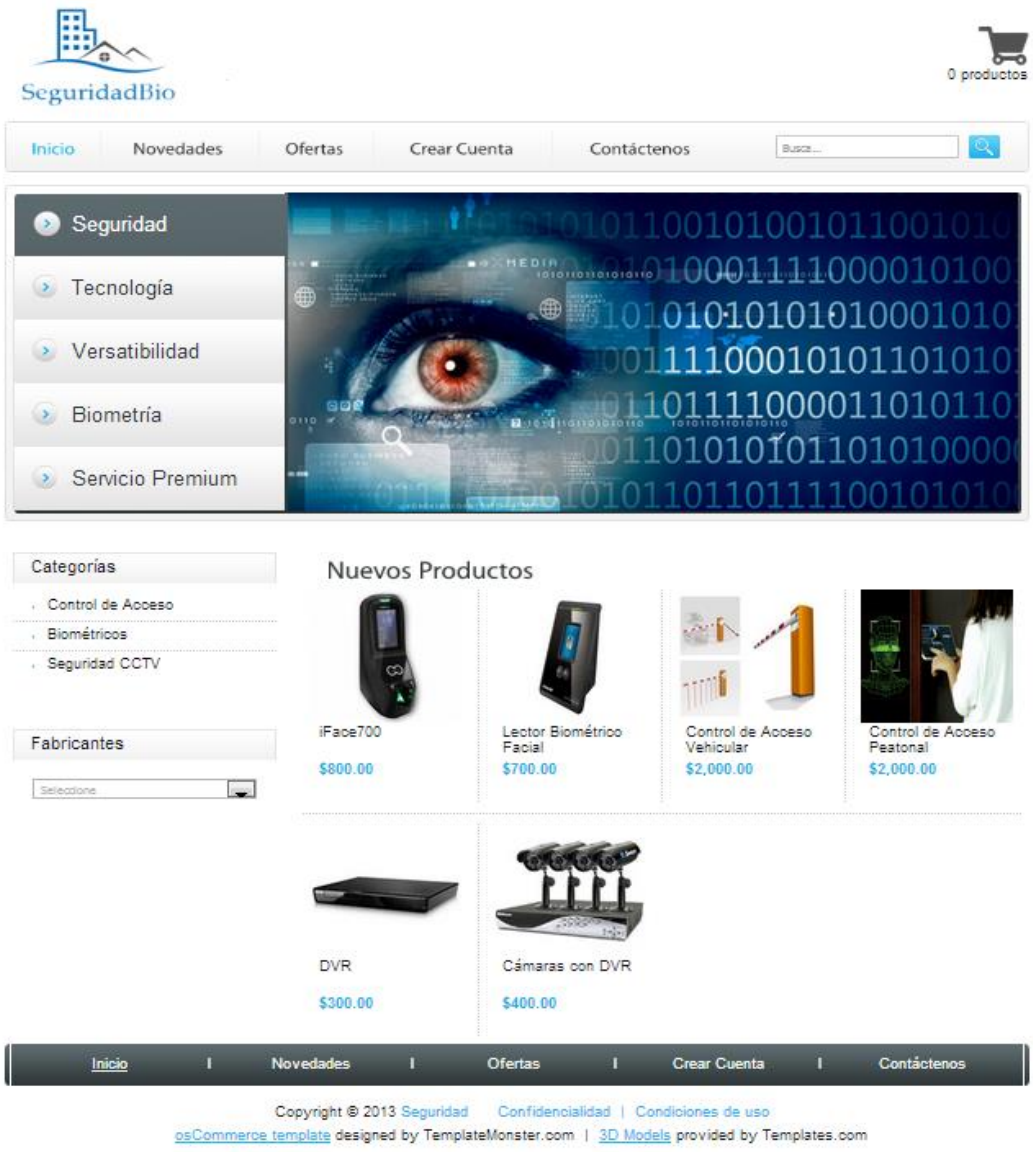


Figura 4.6: Página Principal

4.8.3 CATALOGO DE PRODUCTOS

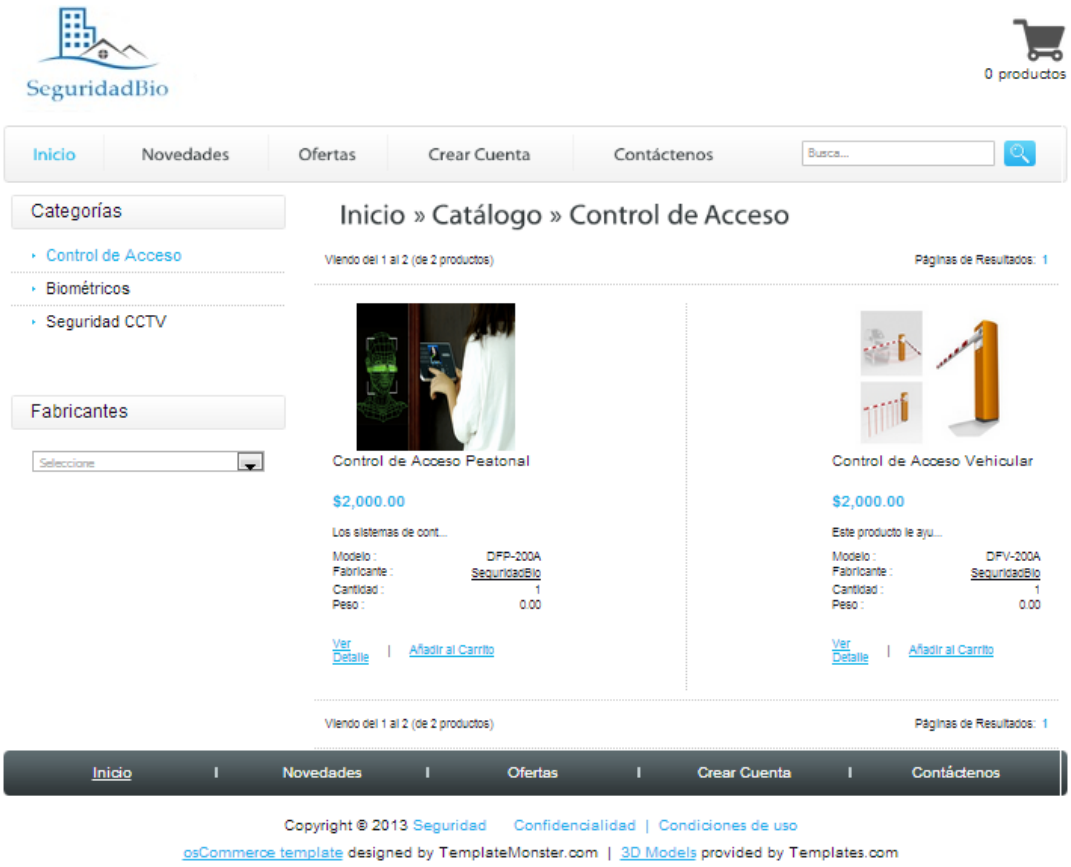


Figura 4.7: Página de Catálogo de Productos

4.8.4 REGISTRO DE USUARIOS

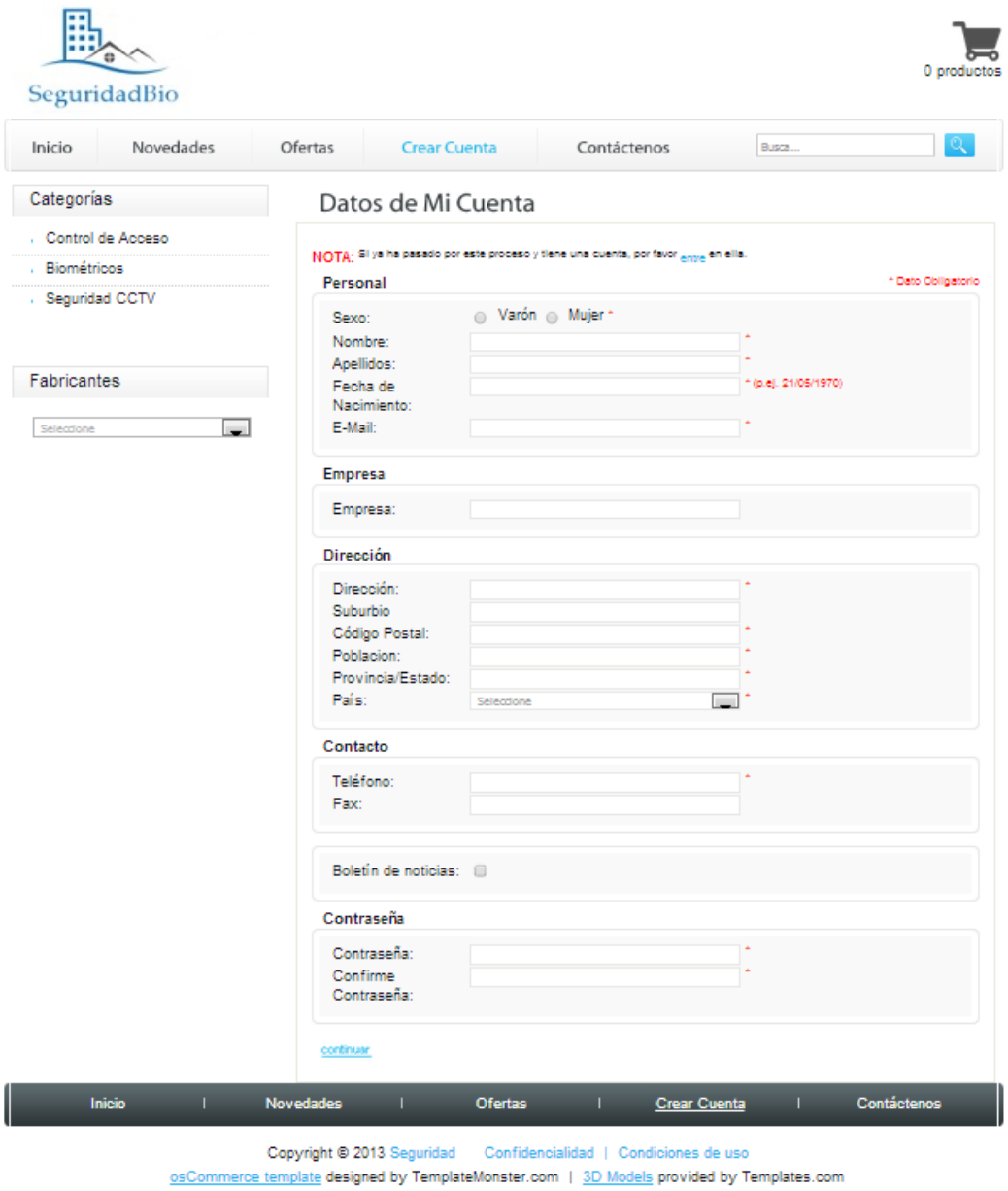


Figura 4.8: Página de Creación de Cuentas de Usuarios

4.8.5 CONTACTENOS

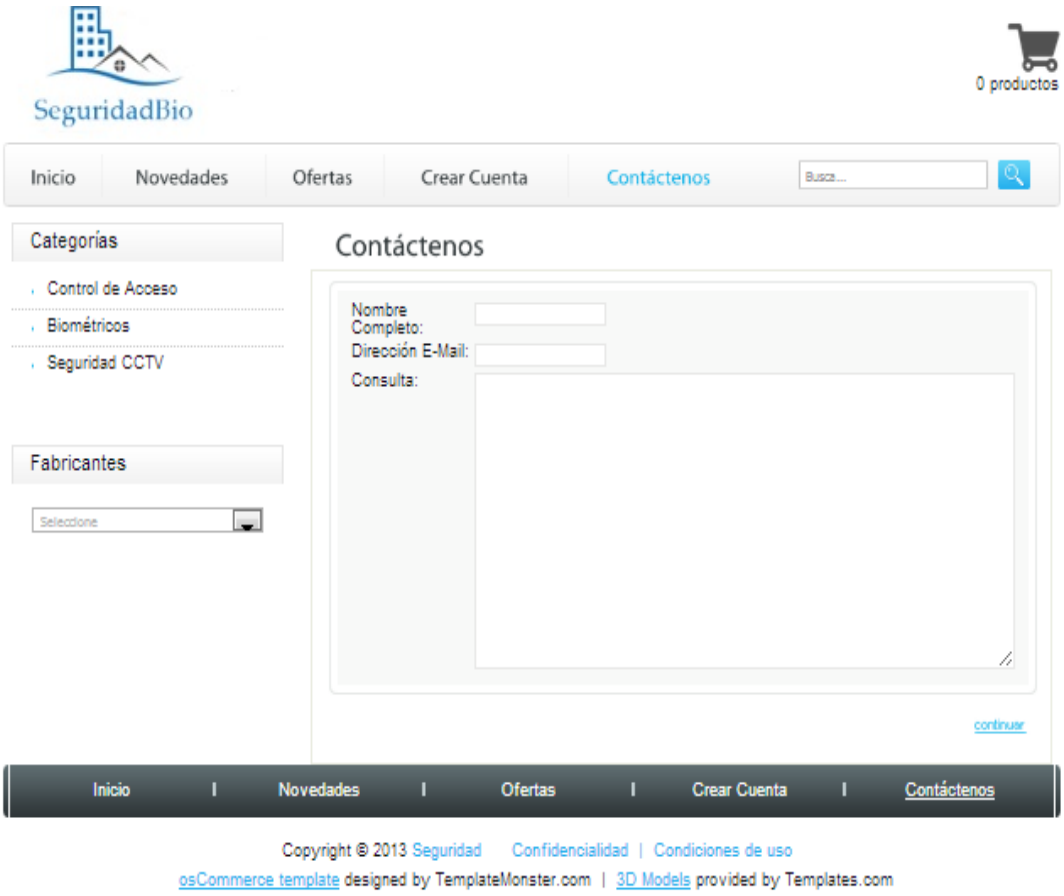


Figura 4.9: Página Contáctenos

4.8.6 CARRO DE COMPRAS

Figura 4.10: Página Carro de Compras

4.9 PROTOCOLOS DE SEGURIDAD SSL.

4.9.1 CERTIFICADO DE SEGURIDAD

Un Certificado de Seguridad es un conjunto de documentos electrónicos emitidos por una entidad certificadora, que permiten encriptar la información transmitida e identificar a la fuente de dicha información. Para que el certificado sea fiable, la entidad certificadora debe ser un organismo de confianza capaz de verificar la procedencia de la información. Para que un Certificado de Seguridad se encuentre operativo, es necesario instalarlo en el servidor donde se encuentre alojado el dominio que se desea proteger.

4.9.2 GARANTÍAS DEL CERTIFICADO DE SEGURIDAD

Al contar con un Certificado de Seguridad los clientes tendrán mayor confianza en el sitio web de la empresa ofertante, la misma que proporcionará total seguridad en las transacciones que se realicen. Al ingresar al Sitio Web se observará el ícono de candado en el navegador o en la barra de direcciones que cambiará de color.

4.9.3 BENEFICIOS DEL CERTIFICADO SSL

- Activar el cifrado de su sitio con un certificado SSL. Si los clientes acceden o hacen compras en su sitio Web, necesita un cifrado SSL. De esta manera el cliente se sentirá seguro y se reducirá las posibilidades de abandonar la compra una vez que el cliente se encuentra decido.

- Mostrar el sello de seguridad y conserve a sus clientes. Una gran mayoría de compradores afirman que un sello puede indicar que su información va a estar segura.

- Conseguir un mayor tráfico con un certificado SSL. Los ataques de phishing y los incidentes de fraude a empresas influyentes han provocado que los usuarios de Internet estén muy preocupados por los robos de identidad. Los nuevos navegadores de alta seguridad proporcionan una garantía de identidad en línea con la información incluida en su certificado SSL.

- Confianza en seguridad. Si su sitio Web se considera en los navegadores más recientes como un sitio de alta seguridad y el de su competidor no, su empresa dará una apariencia de mayor confianza y

legitimidad. Este hecho es una ventaja competitiva en el comercio electrónico.

- Seguridad de la Información: SSL garantiza que terceros no tengan acceso a la información mientras viaja por internet al encriptarla.

- Integridad de los datos: La información recibida desde un servidor por SSL puede ser "validada" para comprobar que no ha sido alterada en la trayectoria.

- Autenticidad de los Datos: Mediante los algoritmos de encriptación, es posible comprobar que los datos realmente han llegado del servidor que el cliente espera. Esto evita que alguien se haga pasar por un sitio para cometer fraudes (evitando ataques como Phishing, Man in the Middle, etc.).

CAPITULO 5

5. DISEÑO GENERAL

5.1 HARDWARE

5.1.1 DISPOSITIVOS DE RECONOCIMIENTO FACIAL

Existen diferentes tipos de dispositivos biométricos, en este caso usaremos un dispositivo biométrico de reconocimiento facial, es necesaria la adquisición de un equipo que posea una cámara con sistema óptico infrarrojos, esta característica optimizará su uso, debido a los diferentes grados de iluminación que pueden variar en un lugar dependiendo si es de día o de noche. La capacidad de almacenamiento de rostros depende del dispositivo, es importante tomar en consideración este punto para cubrir las necesidades del cliente.

Figura 5.1: Dispositivos biométricos de reconocimiento facial

5.1.1.1 LIBRERIAS

ZKTeco es una compañía proveedora de una gran variedad de equipos biométricos, en su Sitio Web se puede encontrar su catálogo de productos, sin embargo el SDK de los dispositivos de reconocimiento facial es proporcionado por ZKSoftware, lo puede encontrar en el siguiente link http://www.itecra.com. Se descargan las librerías que se detallan a continuación:

- Commpro.dll
- Comms.dll
- Rsagent.dll
- Rscomm.dll
- Tcpcomm.dll
- Usbcomm.dll

- Zkemkeeper.dll
- Zkemsdk.dll

5.1.2 REQUERIMIENTOS PARA PUNTO DE CONTROL DE ACCESO

El número de Puntos de Acceso puede variar dependiendo de cuantas entradas y salidas desee controlar.

Requerimientos	
Biométrico	Reconocimiento Facial iFace300 o superior
Red	Cable UTP (variable dependiendo de la distancia al router)
Red Inalámbrica	Antena Wifi (opcional)
Interruptor	Botón de salida
Cerradura Eléctrica	Para la puerta que se desea controlar

Tabla VIII: Requerimientos para punto de control de acceso

5.1.3 SERVIDOR

Computador servidor, tendrá instalada la base de datos del sistema de reconocimiento facial, la misma que almacenará los patrones de los rostros de las personas registradas. El servidor debe estar conectado a la red y debe ser configurado para mantener protegida la información almacenada en él, en este equipo se instalará el software de reconocimiento facial que permitirá el control de acceso en el lugar.

Características

Requerimientos	
Generales	Microsoft Windows (32 bits o 64 bits), Procesador Intel Core i3, Windows XP o superior
Memoria RAM	8 GB
Disco Duro	500 GB (Sistema Operativo y Base de Datos)
Disco Duro 2	500 GB (Respaldos)
Base de Datos	MySql
Monitor	LCD

Red	RouterWi-Fi Pachcord de 2 metros cable UTP Categoría 6A

Tabla IX: Requerimientos Generales

5.1.4 ROUTER WIFI

Dispositivo que permite la conexión de los dispositivos biométricos de reconocimiento facial y el servidor, se requiere que sea Wi-Fi para utilizar el espacio u ondas de radio para transmitir la información desde y hacia el servidor; en otras palabras, el router wi-fi nos permitirá conectar los dispositivos en de la red sin necesidad de utilizar cables.

Se requiere un router que cumpla con las siguientes características:

- Conexión Inalámbrica.
- Alta cobertura.

5.1.5 BARRA VEHICULAR

Bloquea o permite el acceso de los vehículos, con el fin de evitar el ingreso de vehículos no registrados en la base de datos, se integra a través de la red con el software de reconocimiento facial, el mismo que controlará el acceso a las personas autorizadas, y se registrará en la bitácora de ingresos a las personas que no consten en la base de datos.

Figura 5.2: Barra de Acceso Vehicular

5.2 SOFTWARE

5.2.1 SISTEMA OPERATIVO

Figura 5.3: Logo Sistema Operativo Windows

Microsoft Windows es el nombre de una familia de sistemas operativos desarrollados y vendidos por Microsoft. Por observación directa en oficinas y hogares, se puede decir que Windows es el sistema operativo más conocido y utilizado por los usuarios en nuestro país, es por eso que debido a la familiaridad que tienen con este software, se les facilitará el manejo de las aplicaciones, y la manipulación de los programas que el usuario requiera.

Como requerimiento mínimo se recomienda Windows XP o versiones superiores. Hay que tener en consideración que necesitará su respectivo licenciamiento.

5.2.2 BASE DE DATOS

Figura 5.4: Logo MySQL

Para el almacenamiento de la información es necesaria una base de datos robusta y que garantice la integridad de los datos que estén registrados en ella. MySQL es un sistema de gestión de bases de datos relacional, es un interpretador de SQL.

5.2.3 LENGUAJE DE PROGRAMACIÓN

Para realizar el desarrollo del software se utilizaran las librerías que proporciona el proveedor del dispositivo en su Sitio Web, las soluciones informáticas que se plantean pueden ser elaboradas con .NET, sea esto en Visual Basic o en CSharp. Estos lenguajes de programación son los principales utilizados en la elaboración de software en la actualidad, por lo que se puede agregar que el sistema está a la vanguardia de la tecnología, que es de fácil mantenimiento para la empresa y de fácil manejo para los usuarios finales.

Figura 5.5: Logo de Microsoft .NET

5.3 ARQUITECTURA

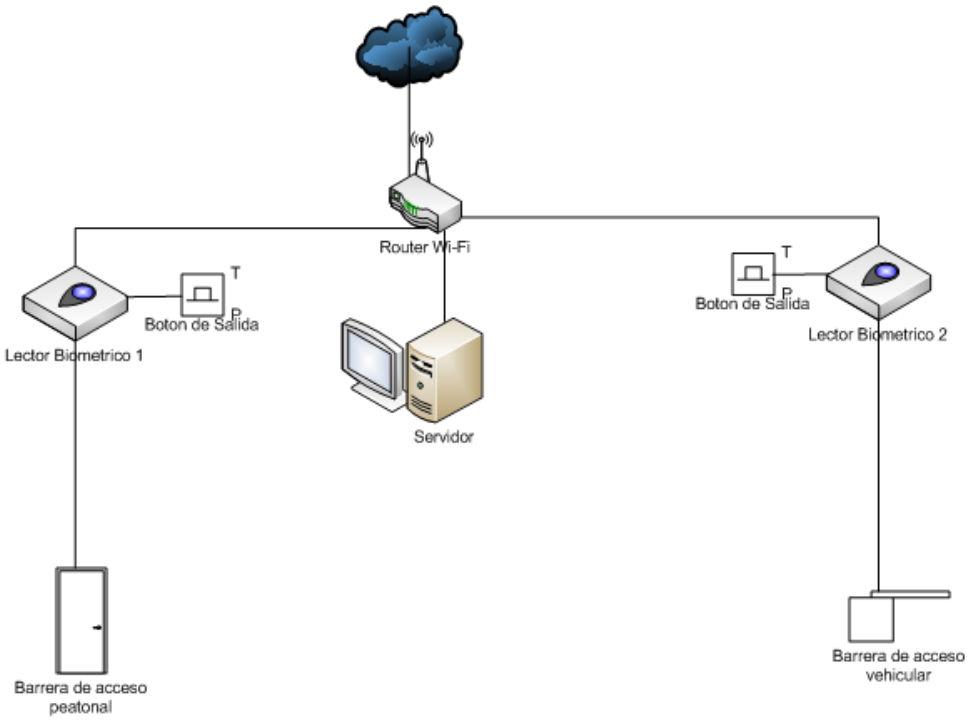


Figura 5.6: Arquitectura del sistema de control de acceso basado en dispositivos biométricos de reconocimiento facial

El sistema de control de acceso puede ser de dos tipos, el vehicular y el peatonal, por lo tanto se deben controlar las diferentes entradas que posea el lugar, esto proveerá de mayor seguridad, ya que se vigilará constantemente todos los accesos, lo que garantiza la efectividad del sistema.

Se utilizarán dispositivos de reconocimiento facial, estos deben llevar un recubrimiento para que los protejan, ya que estarán en la intemperie y deben soportar cualquier tipo de condiciones climatológicas, así como el polvo, éstas estarán conectadas de forma inalámbrica con el servidor, para evitar el cableado y también las limitaciones, ya que se podrían aumentar el número de dispositivos y extender la seguridad a otros sectores dentro del lugar.

Todas los dispositivos estarán conectados a un router Wi-Fi y los datos se almacenarán en un sólo servidor, el cual contiene la información de los patrones de las personas que tienen autorización para su acceso. El software de reconocimiento facial a su vez guardará la bitácora de ingresos al lugar en la base de datos. El dispositivo biométrico debe ser capaz de realizar el reconocimiento y será quien envíe la señal para que el interruptor se active y permita el acceso de las personas o vehículos.

5.4 PROCESOS

Para un mejor entendimiento del sistema, se detallan los siguientes procesos:

5.4.1 PROCESO DE INSCRIPCIÓN

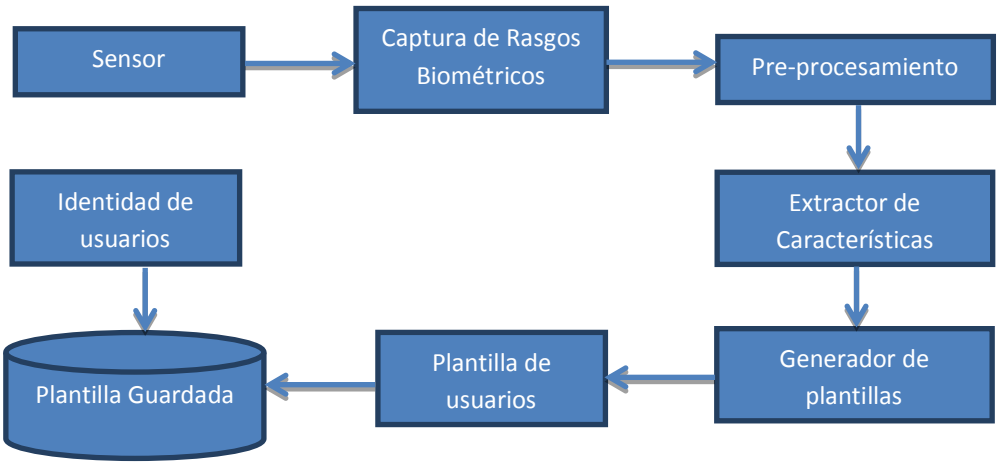


Figura 5.7: Proceso de Inscripción

5.4.2 PROCESO DE IDENTIFICACIÓN EN LA AUTENTIFICACIÓN

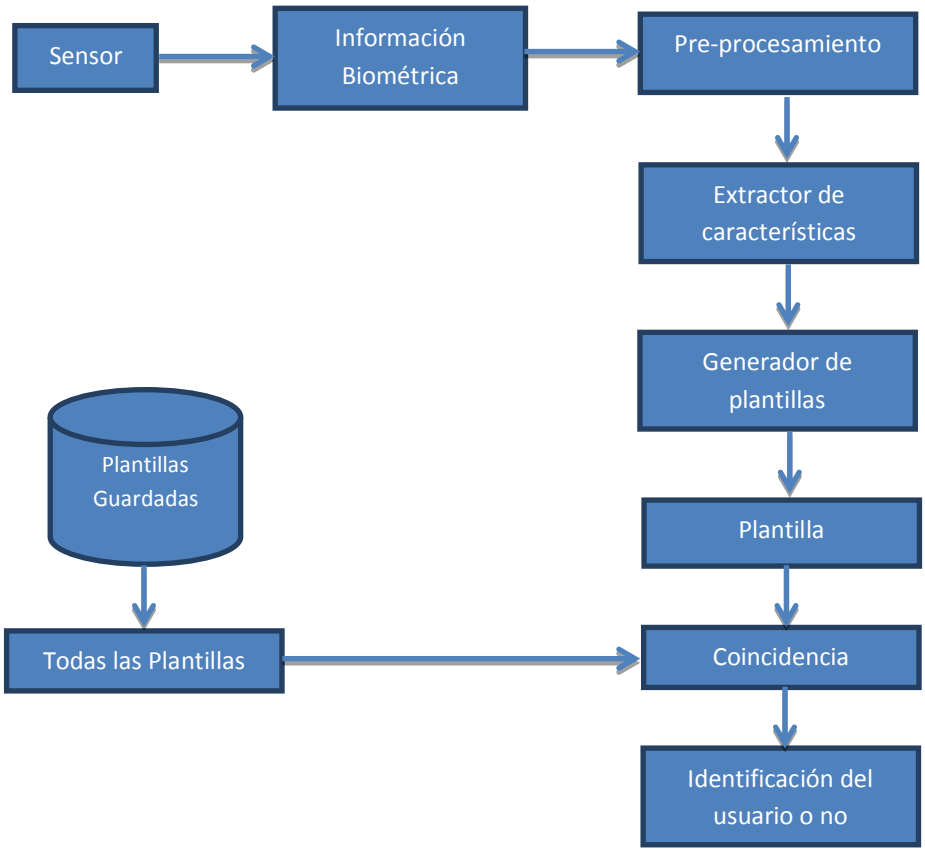


Figura 5.8: Proceso de Identificación

5.4.3 PROCESO DE VERIFICACIÓN EN LA AUTENTIFICACIÓN

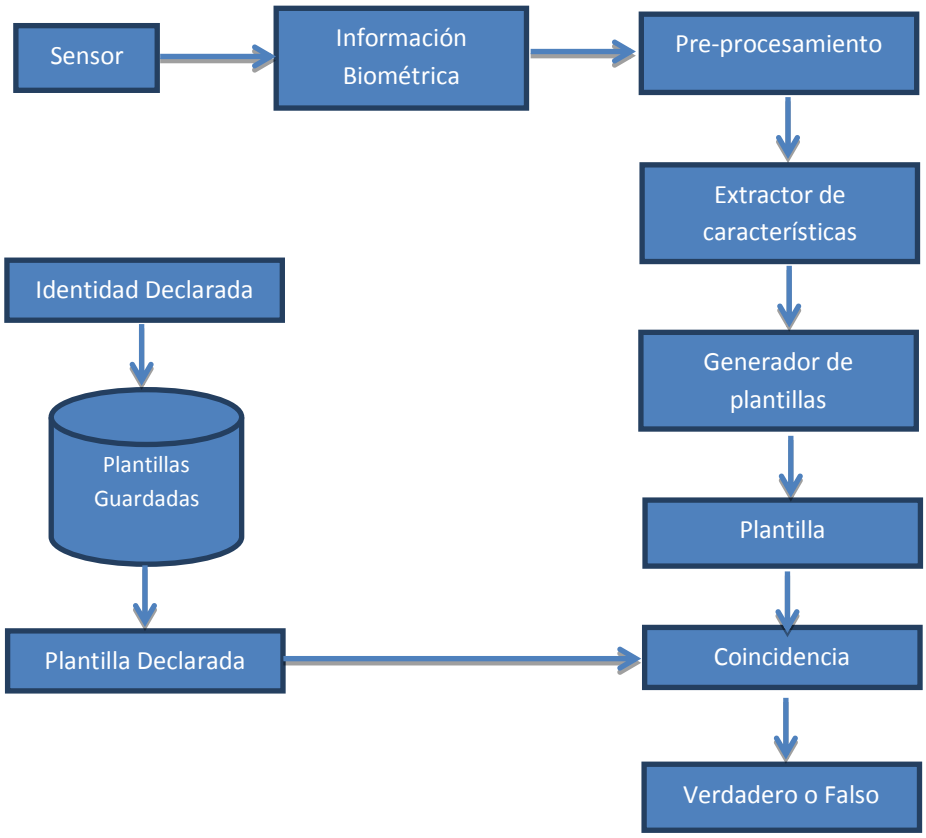


Figura 5.9: Proceso de Verificación

5.5 ESCENARIOS

5.5.1 ACCESO DE PERSONAL AUTORIZADO

Para acceder al lugar la persona deberá pararse frente al biométrico de reconocimiento facial, mirar hacia ella y una vez que el realice el reconocimiento del rostro de la persona, el sistema buscará en la base de datos previamente alimentada.

Figura 5.10: Reconocimiento Facial Peatonal.

Si detecta que la persona está autorizada para el ingreso al lugar, la puerta se abrirá de forma automática.

5.5.2 ACCESO DE VEHÍCULOS

Si se ingresa con vehículo, el auto deberá detenerse cerca del biométrico, una vez que la se analice el rostro de la persona, buscará en la base de datos previamente alimentada y si detecta que la persona está autorizada para el ingreso al lugar, la barra de acceso se elevará de forma automática.

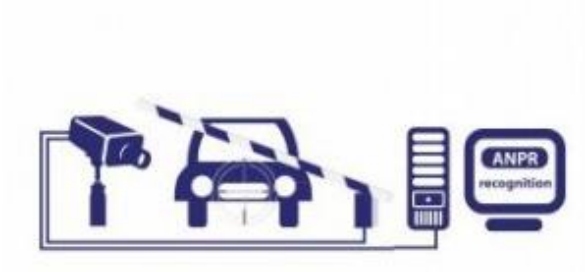


Figura 5.11: Acceso de Vehículos. Fuente: www.google.com

5.5.3 ACCESO DE VISITANTES

El visitante es una persona que no consta en la base de datos, y que asiste al lugar esporádicamente, el acceso de un visitante solo podrá darse con la respectiva autorización de un residente de la ciudadela o personal de la empresa, se registran los datos del visitante, así como también los datos del vehículo en el caso de que se ingrese con uno, este proceso es

responsabilidad del personal de seguridad de la ciudadela privada o empresa.

5.6 ESPECIFICACIONES TÉCNICAS

5.6.1 DISPOSITIVOS BIOMÉTRICOS

Para el diseño de la solución propuesta se utiliza el dispositivo biométrico IFACE300, que tiene una capacidad de almacenamiento de 700 rostros, se conecta a la red por TCP/IP, puede agregarse Wi-Fi para conectarse a la red de forma inalámbrica, tiene entrada USB para subir o bajar información del dispositivo, entre otras características. Las dimensiones se las indica a continuación:

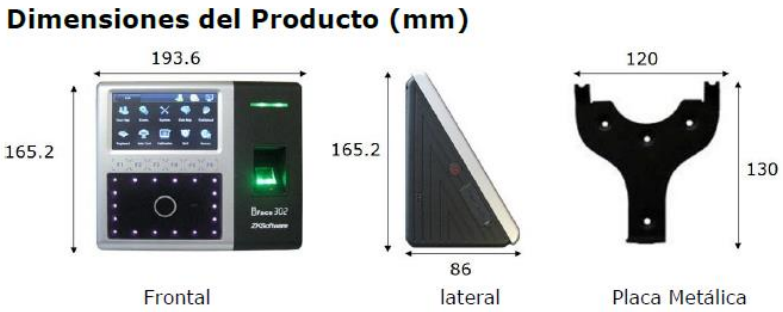


Figura 5.12: Biométrico IFace 300. Fuente: ZKSoftware.com

La ubicación de los dispositivos de reconocimiento facial es muy importante, ya que de ellas depende que el sistema de control de acceso funcione íntegramente, y ayude en los procesos de seguridad de cada uno de los lugares donde sea implementado. Para ello se dan las siguientes pautas:

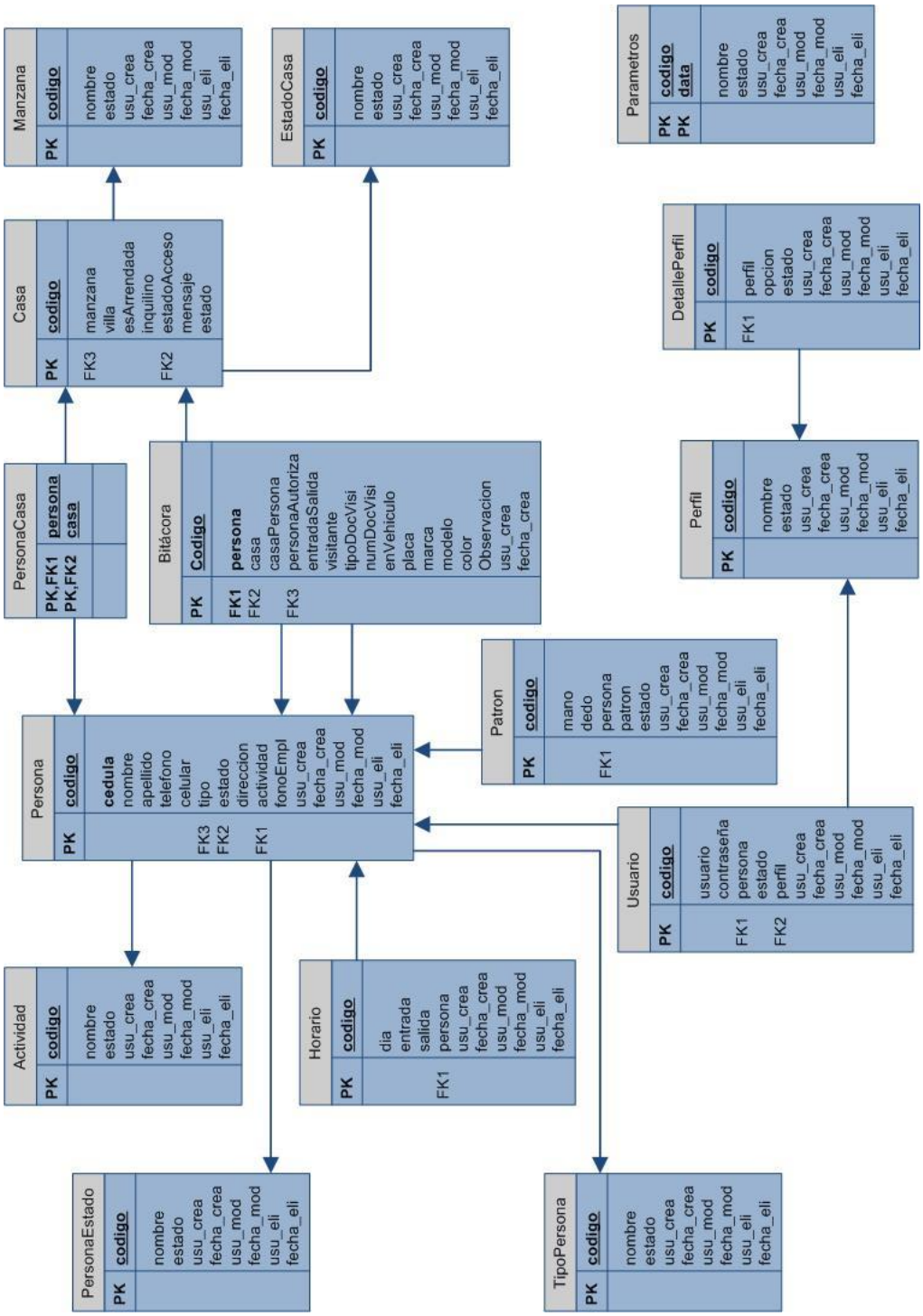
5.6.1.1 Acceso Peatonal

Para el control de acceso de peatones, los dispositivos deben ubicarse en cada una de las entradas que existan en el lugar que se desea controlar, es importante que estén en lugares visibles para evitar cualquier tipo de manipulación maliciosa, y debe estar protegido para evitar que sufra daños debido a las condiciones adversas a la que puede ser expuesto.

5.6.1.2 Acceso Vehicular

El dispositivo deberá estar a una altura promedio de 90 centímetros del suelo, o a la altura conveniente para que el conductor pueda tener la facilidad de autentificarse sin necesidad de bajarse de su vehículo. Debe contar con su respectiva protección, ya que estará a la intemperie.

5.7 MODELO ENTIDAD – RELACIÓN



5.8 PROTOTIPO (SOFTWARE)

Se ha elaborado un prototipo del control de acceso vehicular y de personas, el cual estará instalado en un computador en las garitas de la ciudadela en la que se implementa el proyecto.

A continuación se presenta las pantallas que conforman el sistema de control de acceso basado en dispositivos biométricos, para esto se ha utilizado un biométrico de huella dactilar. El sistema ha sido desarrollado en Visual Basic .NET, utilizando librerías GrFingerXLib para el control del dispositivo biométrico, base de datos MySQL y Crystal Reports para la emisión de reportes.

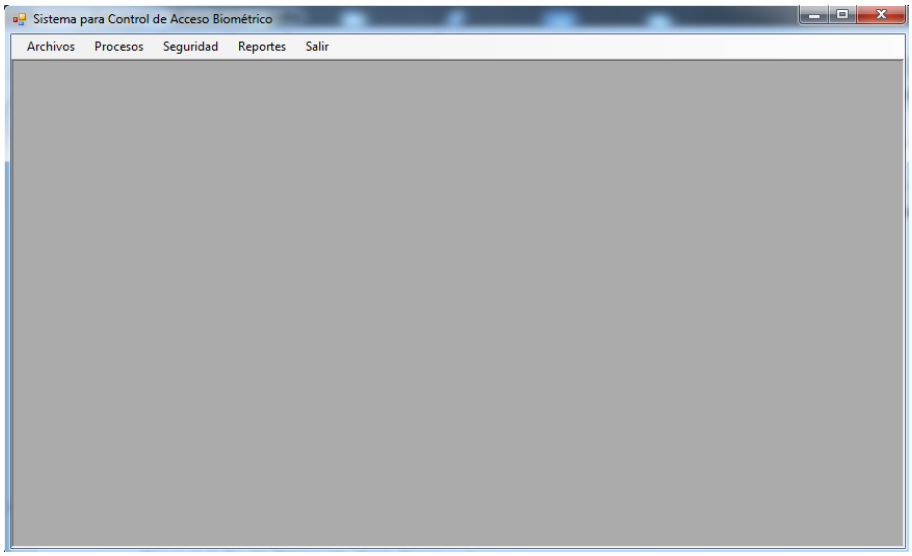


Figura 5.13: Menú Principal

5.8.1 MANTENIMIENTO

5.8.1.1 PERSONA

Se registra toda persona que tenga acceso al lugar, sean estos propietarios, inquilinos, empleados, trabajadores domesticos, entre otros.

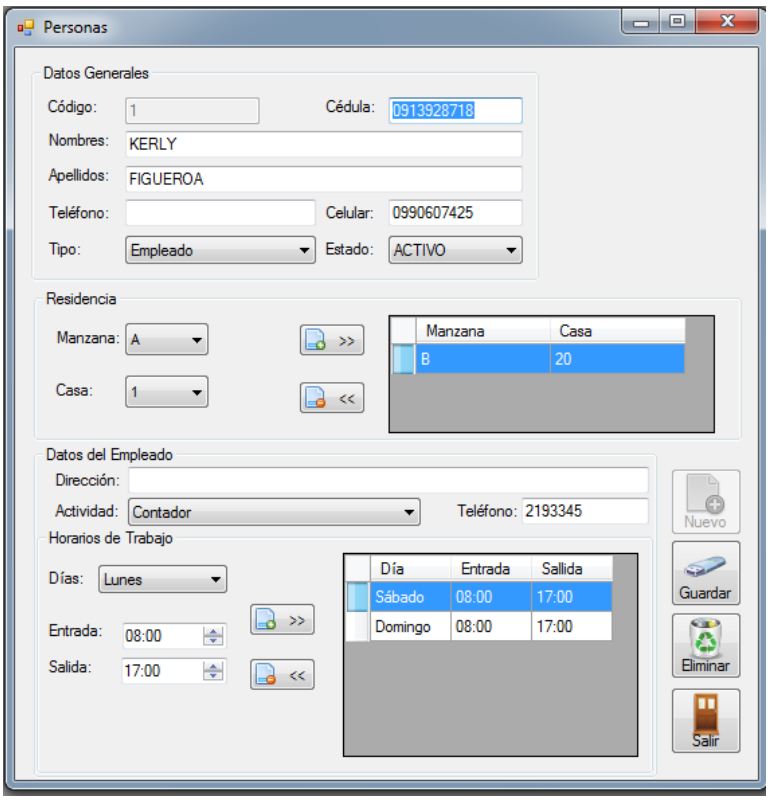


Figura 5.14: Mantenimiento de Persona

5.8.1.2 MANZANA

Se registra las manzanas que pertenecen a la ciudadela.

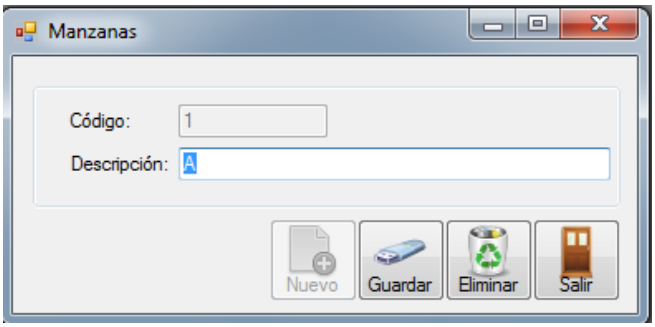


Figura 5.15: Mantenimiento de Manzana

5.8.1.3 CASA

Se registra las casas asociadas a la manzana a la que corresponden.

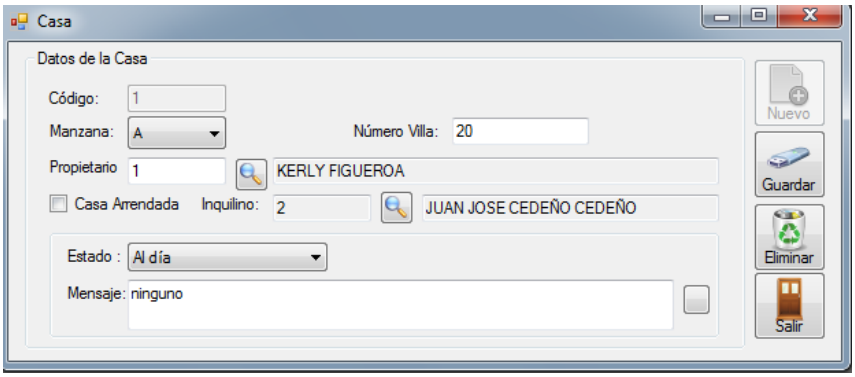


Figura 5.16: Mantenimiento de Casas

5.8.1.4 ACTIVIDAD

Se registra las actividades que pueden realizar las personas dentro del lugar.

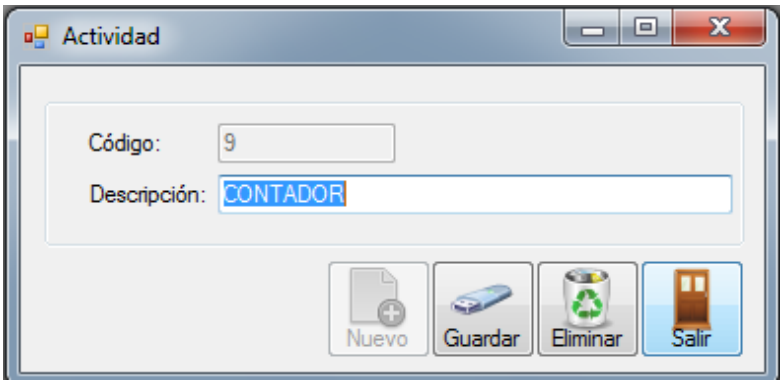


Figura 5.17: Mantenimiento de Actividades

5.8.2 PROCESOS

5.8.2.1 REGISTRO DE HUELLAS

Se realiza el proceso de captura de los patrones como: huellas dactilares, patrones faciales, etc. del individuo que se desea registrar, estos datos pueden ser usados para el enrrolamiento o almacenamiento de los datos en la base de datos, con el fin de que sean utilizados para ingresar a las instalaciones de la ciudadela o lugar que se desea controlar el acceso.

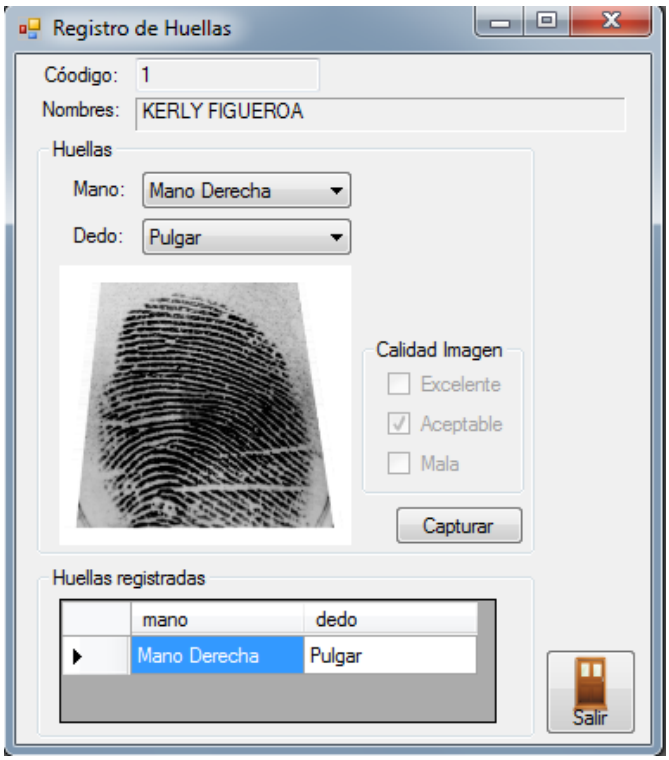


Figura 5.18: Registro de huellas

5.8.2.2 CONTROL DE ACCESO

Se realiza el control de personas y vehículos, para ello la persona que va a circular por el lugar debe estar previamente registrada. Este proceso también alimenta la bitácora de ingresos / egresos de personas o vehículos con el fin de llevar la historia de todos los sucesos que han ocurrido en el día. Si el individuo no está registrado en la base de datos, el personal de seguridad debe pedir autorización al residente involucrado, si el residente

autoriza el ingreso, el guardia debe registrar manualmente en esta pantalla los datos de la persona o vehículo que ingresa.

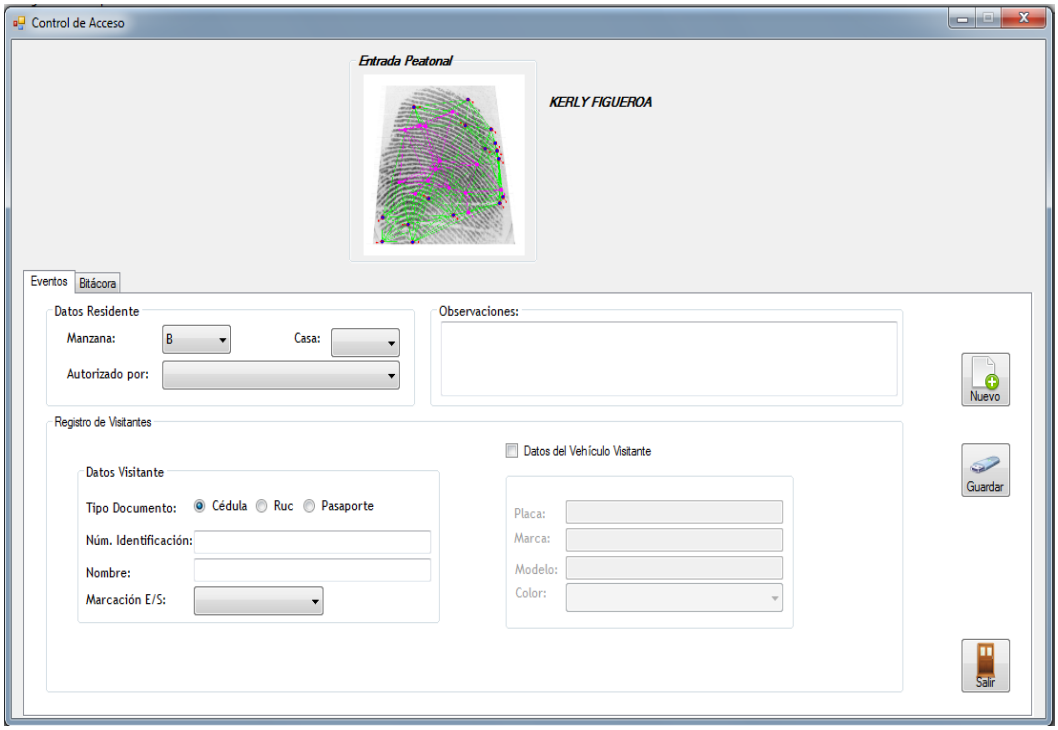


Figura 5.19: Control de Acceso Peatonal / Vehicular

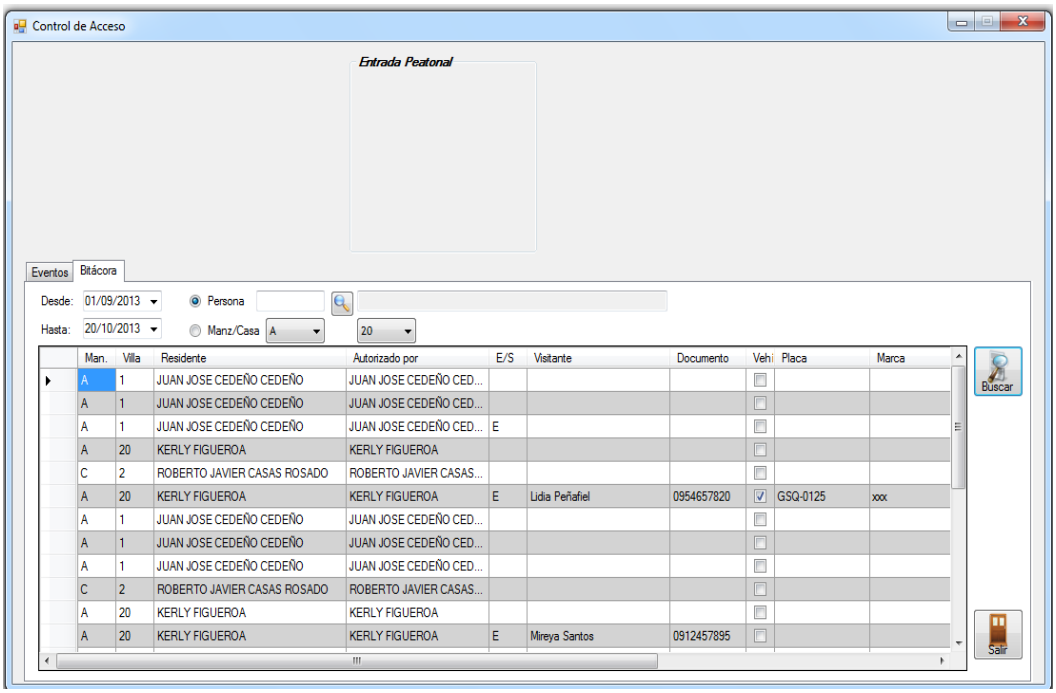


Figura 5.20: Consulta de Bitácora de Acceso

5.8.3 SEGURIDAD

5.8.3.1 USUARIOS

Registro y modificación de usuarios.

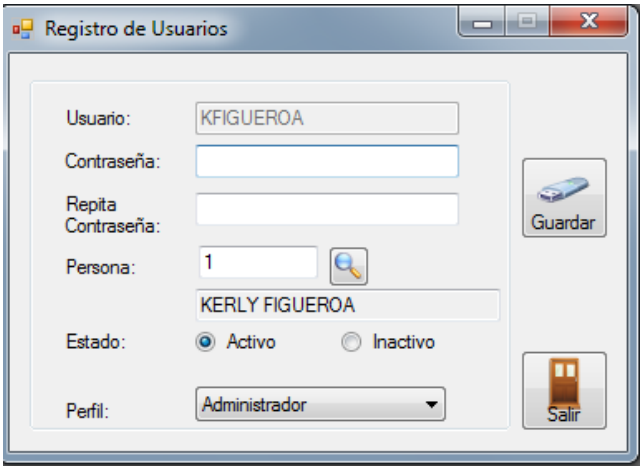


Figura 5.21: Registro de Usuarios

5.8.3.2 CAMBIO DE CONTRASEÑA

Modificación de clave de acceso para usuarios registrados.

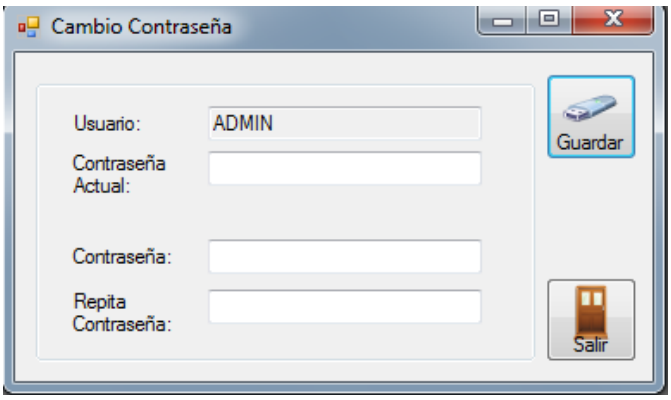


Figura 5.22: Cambio de Contraseña

5.8.4 REPORTES

5.8.4.1 BITÁCORA

Emite un documento que puede ser impreso de los eventos que han ocurrido, pueden ser filtrados por fecha, persona, manzana y casa.

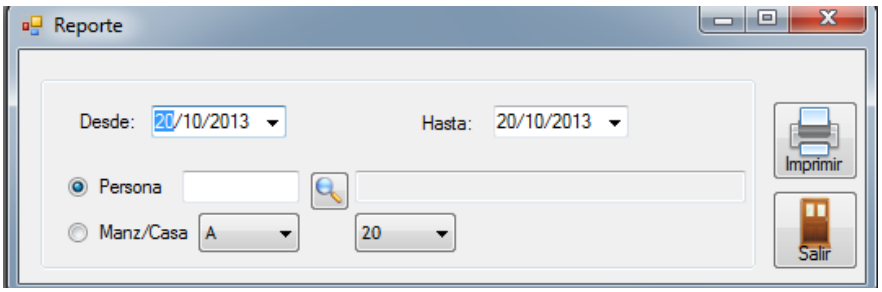


Figura 5.23: Pantalla para emisión de Reporte

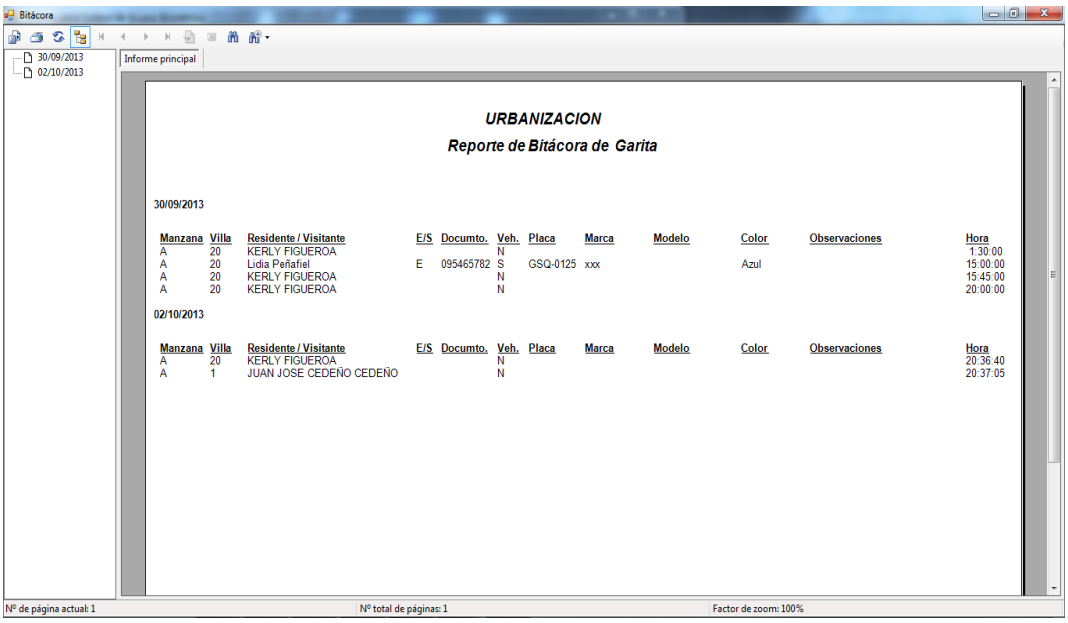


Figura 5.24: Reporte de Bitácora de Garita

5.9 PROTOTIPO (HARDWARE)

Para la elaboración del diseño se han utilizado los siguientes elementos:

- Lector Biométrico Microsoft Fingerprint Reader USB.
- Computador.
- Base de Datos MySQL.
- Arduino Atmel y Software del proveedor de la tarjeta.
- Relay.
- Cable serial, conectado del computador al arduino
- Led.
- Cerradura Eléctrica.

Figura 5.25: Prototipo

5.9.1 ARDUINO ATMEL

Es una plataforma de hardware libre, basada en una placa con un microcontrolador y un entorno de desarrollo. Por su sencillez y bajo coste permite el desarrollo de múltiples diseños.

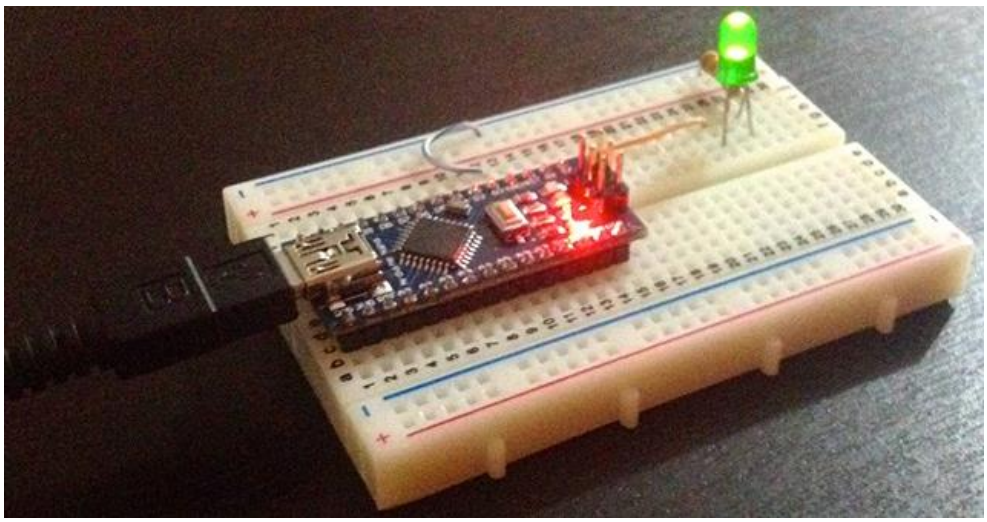


Figura 5.26: Arduino Atmel

5.9.2 RELÉ

El relé es un dispositivo electromecánico. Es un interruptor controlado por un circuito eléctrico en el que se controlan la apertura o cierre de otros circuitos eléctricos independientes.

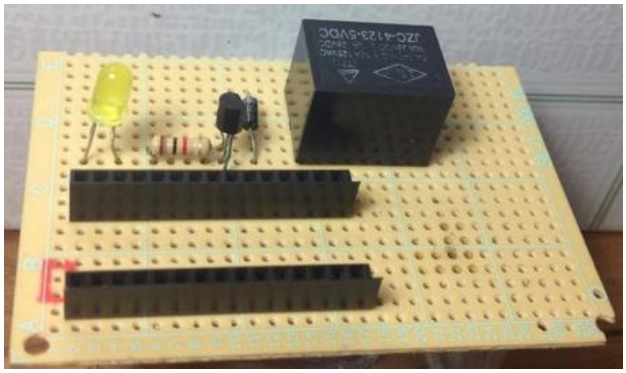


Figura 5.27: Tarjeta Relé

5.9.3 TARJETA CONTROLADORA

Es un conjunto de circuitos electrónicos que permiten que se dé la señal de acceso, está conformada por un arduino y una tarjeta relé, su unión es lo que permite que el mecanismo de acceso se active o que permanezca inactivo.

5.9.4 LED

Indica que el sistema ha enviado una señal de control. Esta señal puede ser utilizada para activar una cerradura eléctrica o barreras vehiculares.

CAPITULO 6

6. ANÁLISIS FINANCIERO

6.1 COSTOS DEL PROYECTO

El sistema biométrico de reconocimiento facial para control de acceso, tiene un costo de inversión que va de acuerdo a los beneficios que ofrece, lo que se puede apreciar en la seguridad de su hogar u oficina, así como, la confianza de vivir o trabajar en un lugar protegido.

El proyecto es un bien tangible, los dispositivos y elementos que se utilizan en el proyecto son adquiridos a diversos proveedores, con la finalidad de preservar los estándares de calidad del producto final.

A continuación se detallan los gastos en los que la empresa debe incurrir para su constitución y los costos para la elaboración de su producto principal. La recuperación de la inversión no es inmediata, pero la propuesta es viable, considerando que se está explorando nuevos nichos de mercado, en lo que a tema de seguridad se refiere.

Tecnología	**Inicial**	**Mensual**	**Anual**
Computadoras	1,400.00		
Impresora	200.00		200.00
Hosting	40.00		40.00
TOTAL	**1,640.00**	**-**	**240.00**

Gastos Administrativos	**Inicial**	**Mensual**	**Anual**
Sueldo Desarrollador		700.00	8,400.00
Contador Externo		300.00	3,600.00
Asesor de Ventas		400.00	4,800.00
Sueldo Administrador		600.00	7,200.00
Sueldo Secretaria		400.00	4,800.00
Arriendo Local		400.00	4,800.00
TOTAL	**-**	**2,800.00**	**33,600.00**

Inversión	**Inicial**	**Mensual**	**Anual**
Constitución Empresa	350.00		
Desarrollo 6 meses			

	4,200.00		
Escritorio	300.00		
Sillas	150.00		
Útiles de oficina	150.00		-
Botellones de Agua	2.00	8.00	94.00
Aire acondicionado	700.00		-
Muebles de oficina	1,000.00		
TOTAL	**6,852.00**	**8.00**	**94.00**

Servicios básicos	**Inicial**	**Mensual**	**Anual**
Agua		10.00	120.00
Luz		50.00	600.00
Teléfono		30.00	360.00
Internet		30.00	360.00
TOTAL	-	120.00	1,440.00
TOTAL GASTOS ADMINISTRATIVOS + SERVICIOS BÁSICOS			
TOTALES	**8,492.00**	**2,928.00**	**35,374.00**

Tabla X: Gastos Administrativos

PUNTO DE RECONOCIMIENTO FACIAL	
2 Biométricos de Reconocimiento Facial	1,300.00
2 Botones de Salida	50.00
Barra para control de vehículos	1,000.00
Instalación Barra	800.00
1 rollo de cable eléctrico	60.00
Cable USB	5.00
Router Wifi	60.00
Patch Cord	5.00
TOTAL	3,280.00

Tabla XI: Costo Punto de Reconocimiento Facial

Pronóstico De Ventas Anuales **10.00**

% Comisión **5.00**

Ingresos	V.Unitario	V.Anual
Kit Reconocimiento Facial	3,800.00	38,000.00
Personalización Software	300.00	3,000.00
Capacitación	150.00	1,500.00
TOTAL	4,250.00	42,500.00

Otros Ingresos	V.Unitario	V.Anual
Soporte	300.00	3,000.00
TOTAL	300.00	3,000.00

Tabla XII: Ingresos por Ventas

Análisis Financiero por local integrado				
Periodos				
Inversión	(11,772.00)	(11,772.00)		
Año 1	12,255	483		
Año 2	12,593	13,076		
Año 3	12,894	25,970		
Tiempo de recuperación en años		0.96		
Tiempo de recuperación en meses		11.5	12	Meses
TIR	90%			
Tasa Interna de Retorno o Tasa de Inversión de Retorno				
Tasa	6.0%			
V.A.N.	21,822.93			

Tabla XIII: Análisis Financiero

CONCLUSIONES

1. En la actualidad y a nivel mundial, los dispositivos biométricos son considerados como los métodos más efectivos en el control de seguridad, ya que se basan en patrones proporcionados por las características físicas de cada persona, estos patrones son únicos y no pueden ser replicados con facilidad, gracias a esta tecnología cada vez se están desarrollando nuevos avances, y con mayor frecuencia existe la necesidad de cambiar los métodos de control comunes por sistemas inteligentes que faciliten y a la vez sean más estrictos en la vigilancia de un lugar.

2. Las empresas y ciudadelas privadas carecen de un control efectivo por parte del personal de seguridad que labora en ellas, indiscutiblemente esto afecta directamente a las personas que habitan o trabajan en estos lugares. Los controles deben ser ejecutados desde el momento de la admisión al lugar, y es por eso que para

ayudar a mejorar los niveles de eficiencia se necesita de la tecnología, en este caso de los dispositivos biométricos, los cuales restringirán el acceso a las personas que no estén registradas, evitando el ingreso de personas ajenas al conjunto habitacional o institución privada que se desea controlar.

3. Se debe realizar capacitación constante al personal de seguridad, y la revisión minuciosa de todos procesos que se tienen en tema de seguridad, la evaluación de estos procesos pueden contribuir con el mejoramiento de la seguridad en todos los lugares públicos y privados del país.

RECOMENDACIONES

1. Se recomienda la utilización de dispositivos biométricos que posean cámara con infrarrojos para que pueda funcionar a la perfección en el día, así como en la noche, donde la iluminación puede ser desfavorable, cada dispositivo debe tener una protección para soportar mayor tiempo las condiciones climáticas, las cuales son variables en nuestro país. Se sugiere que se las cubra con un protector para ayudar a protegerlas de la intemperie, la lluvia y el sol.

2. Es importante que el personal administrativo y de seguridad del cliente, conozcan el funcionamiento del software, para dar soluciones agiles a situaciones cotidianas.

3. Se debe dar mantenimiento preventivo a todos los dispositivos que conforman el sistema, para evitar el desgaste y extender el tiempo de vida de cada uno de estos elementos.

BIBLIOGRAFÍA

[1] Biometría Argentina, Ecuador: Seguridad portuaria biométrica, http://www.biometria.gov.ar/noticias/2012/06/27/ecuador-seguridad-portuaria-biometrica.aspx, fecha de consulta agosto 2013

[2] Griaule Biometrics, SDK para Lector de Huellas de Microsoft, http://www.griaulebiometrics.com/page/en-us/downloads, fecha de consulta junio 2013

[3] Boulgouris, N. V., Konstantinos , P., & Evangelia , M., Biometrics: Theory, Methods, and Applications, Wiley,2009.

[4] Ecuavisa. Frustrado asalto en ciudadela privada deja a delincuente herido. http://www.ecuavisa.com/noticias/regionales-costa, fecha de consulta agosto 2013

[5] El Telégrafo. Ecuador identificará a delincuentes con tecnologías rusas. http://www.telegrafo.com.ec/noticias/judicial, fecha de consulta agosto 2013

[6] Gates, K. A., Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance, NYU Press, 2011

[7] Grupo IWI, Implantación de la LOPD en la empresa. Medidas de seguridad, Vértice, 2009

[8] Id Consultants, Dispositivos Biométricos, http://www.idconsultants.us, fecha de consulta junio 2013

[9] INEC, Instituto Nacional de Estadísticas y Censos, http://www.inec.gob.ec, fecha de consulta agosto 2013

[10] Instituto Nacional de Tecnologías de la Comunicación, Estudio sobre las tecnologías biométricas aplicadas a la seguridad, www.inteco.es, fecha de consulta agosto 2013

[11] Janices, P., Avances de la Biometría en América latina: una herramienta más para garantizar la identidad y la democracia, http://www.biometria.gov.ar/editoriales, fecha de consulta julio 2013

[12] López, P. A., Seguridad informática, Editex, 2010.

[13] Modi, S. K., Biometrics in Identity Management: Concepts to Applications, Artech House, 2011.

[14] Mou, D., Machine-Based Intelligent Face Recognition, Springer, 2010

[15] Muller, B. J., Security, Risk and the Biometric State: Governing Borders and Bodies, Routledge, 2010

[16] Newman, R., Biometrics: Application, Technology, and Management, Cengage Learning, 2009

[17] Ricaurte, J., Cámaras IP, http://img.redusers.com/, fecha de consulta junio 2013

[18] Sencar, H. T., Velastin, S., Nikolaidis, N., & Shiguo, L., Intelligent Multimedia Analysis for Security Applications, Springer, 2010

[19] Stan, L., & Anil, J., Handbook of Face Recognition, Springer, 2011

[20] Umanick., Autenticación Biométrica por Reconocimiento Facial, http://www.umanick.com/index.php/tecnologia/reconocimiento-facial, fecha de consulta julio 2013

[21] Vacca, J. R., Computer and Information Security Handbook, Morgan Kaufmann, 2009

[22] Wechsler, H., Reliable Face Recognition Methods: System Design, Implementation and Evaluation (Vol. 7), Springer, 2009

[23] Wikipedia, Biometría, http://es.wikipedia.org/wiki/Biometr%C3%ADa, fecha de consulta julio 2013

[24] Wikipedia, Sistema de Reconocimiento Facial. http://es.wikipedia.org/wiki/Sistema_de_reconocimiento_facial, fecha de consulta julio 2013

[25] Wikipedia, Servidor HTTP, http://es.wikipedia.org/wiki/Servidor_HTTP_Apache, fecha de consulta agosto 2013