REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA
"ANTONIO JOSÉ DE SUCRE"
VICERRECTORADO PUERTO ORDAZ
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL
TRABAJO DE GRADO

DISEÑO DEL SISTEMA DE AUTOMATIZACIÓN PARA LA IDENTIFICACIÓN Y CONTROL DE ACCESO DEL PERSONAL CONTRATISTA EN LAS INSTALACIONES DE CVG BAUXILUM OPERADORA MATANZAS

AUTOR: Rodríguez G., Rafael J.

CIUDAD GUAYANA, OCTUBRE DE 2015

DISEÑO DEL SISTEMA DE AUTOMATIZACIÓN PARA LA IDENTIFICACIÓN Y CONTROL DE ACCESO DEL PERSONAL CONTRATISTA EN LAS INSTALACIONES DE CVG BAUXILUM OPERADORA MATANZAS.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA
"ANTONIO JOSÉ DE SUCRE"
VICERRECTORADO PUERTO ORDAZ
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL
TRABAJO DE GRADO

DISEÑO DEL SISTEMA DE AUTOMATIZACIÓN PARA LA IDENTIFICACIÓN Y CONTROL DE ACCESO DEL PERSONAL CONTRATISTA EN LAS INSTALACIONES DE CVG BAUXILUM OPERADORA MATANZAS

Trabajo de Grado presentado ante el Departamento de Ingeniería Industrial de la U.N.E.X.P.O. Vicerrectorado Puerto Ordaz como requisito para optar al título de Ingeniero Industrial.

Rodríguez G., Rafael J.

Msc. Ing. Iván Turmero	Ing. Neyla Sayago
Tutor Académico	**Tutor Industrial**

CIUDAD GUAYANA, OCTUBRE DE 2015

RODRÍGUEZ GÓMEZ, RAFAEL JOSÉ

“DISEÑO DEL SISTEMA DE AUTOMATIZACIÓN PARA LA IDENTIFICACIÓN Y CONTROL DE ACCESO DEL PERSONAL CONTRATISTA EN LAS INSTALACIONES DE CVG BAUXILUM C.A. OPERADORA MATANZAS”

204 Páginas.

Trabajo de Grado.

Universidad Nacional Experimental Politécnica “Antonio José de Sucre”.

Vicerrectorado Puerto Ordaz.

Departamento de Ingeniería Industrial.

Tutor Académico: Msc. Ing. Iván Turmero.

Tutor Industrial: Ing. Neyla Sayago.

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA

"ANTONIO JOSÉ DE SUCRE"

VICERRECTORADO PUERTO ORDAZ

DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

TRABAJO DE GRADO

ACTA DE APROBACIÓN

Quienes suscriben, miembros del jurado evaluador designado por el departamento de ingeniería industrial de la UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA "ANTONIO JOSÉ DE SUCRE", VICERRECTORADO PUERTO ORDAZ, para examinar el TRABAJO DE GRADO presentado por el ciudadano **RAFAEL JOSÉ RODRÍGUEZ GÓMEZ**, titular de la cedula de identidad **V-17.911.092**, cuyo trabajo es titulado **"DISEÑO DEL SISTEMA DE AUTOMATIZACIÓN PARA LA IDENTIFICACIÓN Y CONTROL DE ACCESO DEL PERSONAL CONTRATISTA EN LAS INSTALACIONES DE CVG BAUXILUM C.A. OPERADORA MATANZAS"**. Consideramos que dicho trabajo cumple con los requisitos exigidos. A tal efecto, lo declaramos **APROBADO**.

En Ciudad Guayana, Puerto Ordaz a los 13 días del mes de octubre de dos mil quince (2015).

_____	_____
Msc. Ing. Iván Turmero	Ing. Neyla Sayago
Tutor Académico	**Tutor Industrial**
_____	_____
Ing. Ysheel Cabello	Ing. Félix Martínez
Jurado Evaluador	**Jurado Evaluador**

"No existen más que dos reglas para escribir:

Tener algo que decir y decirlo".

Oscar Wilde (1854-1900).

DEDICATORIA

Este proyecto de Trabajo de Grado se lo dedico primeramente a DIOS todopoderoso por guiarme por el camino del bien, fortalezas para seguir adelante y voluntad para culminar este proyecto y ser mi fiel amigo.

A mis tres Madres, mi Mama María Gomez, Mi Tía Beatriz Gomez y Mi Abuela Aurora Figueroa, por su crianza, por apoyarme, por guiarme, por estar presente en las buenas y en las malas, aconsejarme y brindarme los recursos económicos necesarios para llevar a cabo esta gran carrera llamada Ingeniería Industrial, Las Amo!.

A mi Abuelo Rafael Gomez, por hacer el papel de padre en toda mi vida, por estar siempre a mi lado y ensenarme el mundo, por cuidarme, jugar, disfrutar, y a pesar que siempre discutimos, siempre nos estamos riendo, Te Amo Mucho.

A mi Hermanita Saelimar, por ser mi hermanita que tanto quiero, que a pesar discutimos siempre nos queremos y nos extrañamos, te amo demasiado!

A mi novia Anabell Hernández, por tu amor, por tu apoyo incondicional, tus grandes ideas, tus risas, por apoyarme en la elaboración y estar en cada momento junto a mí, Te Amo Demasiado Vida!

A mi Tutor Académico Profesor Iván Turmero, por ser mi guía y asesor en la elaboración de este Trabajo Final de Grado, por motivarme a seguir adelante pese a los problemas que se pudieran presentar y estar siempre dispuesto a aclarar mis dudas, muchísimas gracias!!! :D

A mi Tutora Industrial Ing. Neyla Sayago, por sus grandes recomendaciones, ayuda y por demostrar que un Ingeniero Industrial es apto para trabajar en cualquier área que involucre en la ingeniería.

AGRADECIMIENTOS

Primero y principal, le doy el agradecimiento a esta Casa de Estudios U.N.E.X.P.O, por cada paso en nuestra vida académica, que fueron felicidad, risas, lágrimas, orgullo, y por llegar a ser un gran Ingeniero Industrial.

Al departamento de Ingeniería Industrial, por ayudar a cada estudiante a lograr su meta.

A la Señora Loira Belmonte, por su gran cariño y sonrisa, su apoyo y ayudarme en mis problemas, gracias :D.

Al Profesor Félix Martínez, por ser un gran profesor, excelente amigo, su gran paciencia para ensenar, y estar ahí presente en el momento que más se necesita! Profe eres lo máximo :D

A la Profesora Natasha Alarcón, por su gran alegría que llegaba a darnos clase, por ensenarnos las claves para ser ingenieros industriales en las empresas, y por su gran cariño hacia mí, Gracias profe :D.

A los nuevos integrantes de mi familia, mi suegra Ana Silva y a mi cuñado Rubén Hernández, por ayudarme y compartir en mi vida :D.

A mi gran amigo Julián Domínguez, que a pesar que se consiguió una novia y desapareció del mapa, siempre compartimos grandes momentos desde que nos inscribimos en la universidad hasta este momento que nos estamos graduando, gracias :D.

A todos mis amigos, que de una y otra forma han formado parte de mi vida desde que entre en la universidad y que están conmigo en este gran momento.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD NACIONAL EXPERIMENTAL POLITÉCNICA
"ANTONIO JOSÉ DE SUCRE"
VICERRECTORADO PUERTO ORDAZ
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL
TRABAJO DE GRADO

Autor: Rodríguez Gomez, Rafael José
Tutor Académico: Msc. Ing. Iván Turmero
Tutor Industrial: Ing. Neyla Sayago.
Fecha: Octubre, 2015

RESUMEN

La siguiente investigación fue realizada en CVG BAUXILUM C.A, ubicada en la Zona Industrial Matanzas de Puerto Ordaz, específicamente en la División Identificación y Control de Acceso, adscrita a la Gerencia Seguridad Patrimonial, en donde se revisó, evaluó y diseñó un nuevo sistema de control de acceso, en vista a que el actual sistema manual presentaba debilidad y carencias a la hora de ingresar el personal contratista a la empresa, mediante el uso de diagramas de procesos y de Ishikawa. Fue de tipo no experimental: debido a que se identificaron los problemas y debilidades sin alterar ninguna de las variables presente en los procesos; descriptiva, porque se procuró conocer la situación y su entorno. Campo, debido a que se realizó un análisis sistemático de los problemas que afectan a la División Identificación y Control. Aplicada, porque surge la necesidad de obtener la documentación adecuada para optimizar los procesos y Evaluativa, permitió indagar en todos los aspectos referidos al diseño del sistema automatizado. Se dio a conocer las diferentes tecnologías existentes en el mercado nacional requerido para el diseño del proyecto. El resultado de este estudio estableció la adecuación y las mejores pertinentes.

Palabras claves: CVG Bauxilum, identificación, control de acceso, biometría, huella dactilar.

ÍNDICE GENERAL

CONTENIDO **Pág.**

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

Pág.

INTRODUCCIÓN

La empresa C.V.G. BAUXILUM, tutelada por la Corporación Nacional del Aluminio y está adscrita al Ministerio del Poder Popular para Industrias, es una empresa integrada para la producción de alúmina la cual incluye la extracción de bauxita en los Pijiguaos y su transformación en alúmina a través del proceso Bayer en planta en la zona industrial matanzas.

En la Gerencia Seguridad Patrimonial, tiene como principal objetivo, el garantizar la protección patrimonial de la Empresa, asegurando la prevención y resguardo de los bienes e instalaciones, y la protección física de los trabajadores de CVG BAUXILUM.

La División Identificación y Control De Acceso Alúmina, adscrita a la Gerencia Seguridad Patrimonial, tiene como función la de garantizar la administración y funcionamiento del Sistema Integrado de Seguridad Patrimonial del proceso de Identificación y Control de Acceso de las instalaciones de la Empresa en Matanzas, estableciendo los niveles de seguridad de acceso electrónico y la implementación de planes y acciones de mantenimiento preventivo, que aseguren el resguardo de bienes, activos e instalaciones y la protección física de los trabajadores de CVG BAUXILUM C.A.

En el 2002, se plantean las posibles debilidades y amenazas en la empresa en materia de seguridad y por ende se plantean crear un sistema que se ha denominado Sistema Integrado de Seguridad Patrimonial (S.I.S.P.), ya que se van a desarrollar e integrar varios subsistemas de seguridad para proteger a las instalaciones de Bauxilum.

El sistema de identificación que utilizan en C.V.G Bauxilum es por medio de tarjetas RFID (siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia) que es un sistema de almacenamiento y recuperación de datos remotos mediante ondas de radio utilizando la ID única de las tarjetas pasivas de la marca HID Proximity. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (Automatic IDentification, o identificación automática).

La importancia de esta investigación es que se orientó a incrementar la seguridad automatizando el control de acceso del personal contratista, mediante un sistema biométrico, sin la necesidad de hacer uso de las tarjetas RFID, reduciendo significativamente los costos de las mismas, utilizando un identificador que no se pudiese perder, cambiar o falsificar.

Para garantizar un correcto diseño del sistema se realizó el estudio de factibilidad, que es un instrumento que sirve para orientar la toma de decisiones en la evaluación de un proyecto. Formulando con base en información que tiene la menor incertidumbre posible para medir las posibilidades de éxito o fracaso del proyecto de inversión, apoyándose en él se tomará la decisión de proceder o no con su implementación. En conjunto al estudio de factibilidad, se analizaran las distintas tecnologías biométricas (dactilar, iris, facial) mediante el uso de software para entender el impacto que tendrá el nuevo sistema para la empresa; en caso de proceder dicho proyecto, se efectuara su planificación de proyecto llevando con sus ítems: Ingeniería Básica, Ingeniería de Detalles, Procura, Ejecución del Proyecto, Cierre Técnico y Cierre de Proyecto.

Esta investigación se llevó a cabo en la División Identificación y Control De Acceso Alúmina, adscrita a la Gerencia Seguridad Patrimonial en la Empresa C.V.G. Bauxilum, cuya estadía en la planta fue desde 25 de mayo de 2015 hasta el 18 de septiembre de 2015, desde los sistemas de identificación de tarjetas RFID (Fichas), pasando por la autorización de control de acceso

manual, hasta llegar al servidor y sistemas automatizados de control de acceso.

La investigación está estructura de la siguiente manera:

- **Capítulo I, El Problema**: Se formula el Problema a resolver con su respectiva Justificación y Alcance, se establecen el Objetivo Genera y los Objetivos Específicos a solucionar y las Limitaciones del proyecto.
- **Capítulo II, Marco Teórico**: Se hace énfasis en las Bases Teóricas, Identificación y Descripción de la Empresa, en conjunto al área donde se ejecuta la investigación.
- **Capítulo III, Marco Metodológico**: Se hace mención de los Aspectos Procedimentales, Técnicas y Procedimiento Metodológico que se llevaran a cabo para la ejecución de esta investigación.
- **Capítulo IV, Situación Actual:** Se lleva a cabo una descripción detallada de la situación actual de la empresa, a través de la realización de una descripción minuciosa del actual proceso de identificación utilizado en el control de acceso de contratistas.
- **Capítulo V, Análisis y Resultados:** Se establece los problemas que presenta el actual sistema de control de acceso, se muestran las tecnologías, sistema propuesto, estudio de factibilidad técnico, operativo y económico.
- **Conclusiones y Recomendaciones:** Se expone las conclusiones que se llegó con esta investigación.

CAPÍTULO I

EL PROBLEMA

En el presente capítulo se presenta el Planteamiento del Problema, la Situación Actual, el Objetivo General y los Objetivos Específicos, el Alcance, Justificación, Importancia y Limitaciones de la investigación.

PLANTEAMIENTO DEL PROBLEMA

En el Estado Bolívar se encuentra instalada la empresa C.V.G. Bauxilum C.A., empresa tutelada por la Corporación Nacional del Aluminio y adscrita al Ministerio del Poder Popular para Industrias, esta empresa está conformada por dos (02) operadoras, la primera ubicada en Los Pijiguaos que se encarga de la explotación de las minas y extracción del mineral de bauxita, el cual es trasladado por vía fluvial hacia la otra operadora ubicada en la zona industrial matanza en Puerto Ordaz, en donde se encarga de transformar la bauxita mediante el proceso Bayer, y así obtener alúmina en grado metalúrgico.

En la Gerencia Seguridad Patrimonial, mediante el Sistema Integrado de Seguridad Patrimonial (S.I.S.P.), cuentan con una plataforma de control de acceso mediante el uso de tarjetas de proximidad RFID para el personal fijo y temporal de la empresa, enmarcado como parte de las estrategias y lineamientos en materia de prevención y resguardo de la seguridad del recurso humano y los bienes materiales de la empresa.

Adscrita a la Gerencia de Seguridad Patrimonial, se encuentra la División de Identificación y Control de Acceso Alúmina, tiene como principal objetivo el administrar el Sistema Integrado de Seguridad Patrimonial (S.I.S.P.), estableciendo y controlando los niveles de seguridad electrónica del control de acceso y permanencia de personas, vehículos, bienes materiales a las instalaciones y perímetros de la Empresa. El sistema de control de acceso es monitoreado en el Centro de Control (CECON) del Sistema Integrado de Seguridad Patrimonial de CVG BAUXILUM C.A, con la finalidad de mejorar la supervisión y control de los mecanismos de seguridad.

Como resultado de un estudio de seguridad elaborado en el año 1999, por especialistas de la Gerencia de Protección Industrial de CAVSA, se identificaron las amenazas y debilidades, determinándose la necesidad de desarrollar un sistema para la mitigación de los riesgos encontrados y a los cuales está sometido el patrimonio de la empresa y el recurso humano.

En el 2002, se inicia el procedimiento que se ha denominado **Sistema Integrado de Seguridad Patrimonial (S.I.S.P.)**, ya que se van a desarrollar e integrar varios subsistemas de seguridad para proteger las instalaciones de la empresa Bauxilum.

La plataforma tecnológica del **Sistema Integrado de Seguridad Patrimonial (S.I.S.P.)** está compuesta por:

- Control de Acceso
- Intrusión en edificaciones (No se desarrolló)
- Circuito Cerrado de Televisión (C.C.T.V.)

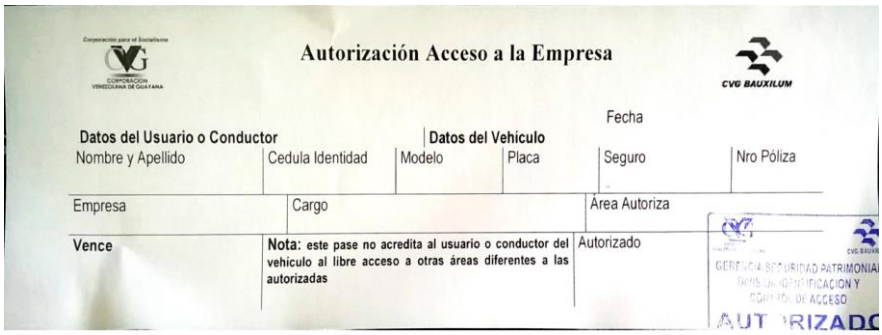
Gracias a este Sistema, la empresa cuenta con los siguientes beneficios en materia de seguridad:

- Control en la entrada, permanencia, tránsito y egreso del personal dentro de la planta.
- Minimizar la perdida por hurtos o robos.
- Limitar el acceso a áreas claves a personal no autorizado.
- Monitorear y registrar en tiempo real las acciones que se desarrollen dentro de las instalaciones.
- Disminución del absentismo laboral.
- Uso no autorizado de los comedores.
- Control de materiales, equipos y herramientas.

El Control de Acceso a la empresa se hace mediante el uso de las tarjetas pasivas RFID de la marca HID Proximity, se enfoca básicamente en aperturas de sistemas de paso peatonal o vehicular tales como torniquetes, puertas electromagnéticas, barrera vehicular o basculante. Todo esto se efectúa bajo la tecnología RFID que están compuestas por tarjetas y lectoras, donde la lectora emite una carga por inducción de corto alcance (125khz para el caso de las tarjetas HID) y la tarjeta emite su ID al lector, donde este es descodificada y la envía al servidor OnGuard de Lenel, donde recibe, interpreta y luego envía la respuesta hacia el lector en el cual apertura el acceso si está autorizado o lo bloquea si no está autorizado.

En la actualidad, debido los elevados costos para adquirir estas tarjetas de identificación, se ha visto obligado a la empresa a usar soluciones alternativas a la hora de identificar al personal contratista, perdiendo la esencia de seguridad que ofrece el control de acceso.

Hoy en día se utiliza una hoja de autorización firmado y sellado por la división de identificación y control de acceso a la empresa para llevar el control de acceso al personal contratista y los visitantes que vienen a la empresa (ver figura 1.1).



Autorización Acceso a la Empresa

CVG BAUXILUM

Fecha

Datos del Usuario o Conductor		Datos del Vehiculo			
Nombre y Apellido	Cedula Identidad	Modelo	Placa	Seguro	Nro Póliza
Empresa	Cargo			Área Autoriza	
Vence	Nota: este pase no acredita al usuario o conductor del vehiculo al libre acceso a otras áreas diferentes a las autorizadas			Autorizado	

GERENCIA SEGURIDAD PATRIMONIAL
DIVISIÓN DE IDENTIFICACIÓN Y CONTROL DE ACCESO
AUTORIZADO

Figura 1.1: Autorización para el Acceso a la empresa.

Fuente: División de Identificación y Control.

En la actualidad, las tarjetas RFID y los sistemas alternativos que están utilizando en la empresa presentan los siguientes problemas a la hora de brindar seguridad a la empresa:

- Las Tarjetas RFID pueden ser transferibles: A diferencia del personal fijo, las tarjetas RFID de los pasantes están sin identificar que muy fácil pueden caer en manos maliciosas.
- Si se pierde una tarjeta, roba o se le queda en casa, representa una pérdida para la empresa por el material, además que al personal se le marcara en el sistema como inasistente.
- Las tarjetas también se dañan: A pesar de ser tarjetas de proximidad que funcionan bajo inducción, estas se dañan por el uso.
- En el sistema Lenel no disponen de un registro con foto del personal contratista, pasante ni visitante, solo se disponen de dicho registro en el personal fijo

En la siguiente investigación se dio respuesta a la siguiente problemática: automatizar el sistema de identificación para el personal contratista, en donde se utilice un método de identificación biométrica, con el principal objetivo de ofrecer una mayor seguridad a la hora de ingreso a la planta y de reducir los altos costos de las tarjetas RFID.

JUSTIFICACIÓN

La investigación se orientó a incrementar la seguridad en el control de acceso al personal contratista, mediante el uso de dispositivos de control de acceso basado en la biometría humana sin la necesidad de hacer uso de las tarjetas RFID, reduciendo significativamente los costos de las mismas. Las técnicas de la biometría se aprovechan del hecho de que las características del cuerpo humano son únicas y fijas. Los rasgos faciales, el patrón del iris del ojo, los rasgos de la escritura, la huella dactilar, y otros muchos son los que se utilizan para estas funciones, incluyendo el ADN, y para la presente investigación explicaremos las bondades del sistema biométrico como método de identificación.

ALCANCE

Este estudio se realizó en la División Identificación y Control de Acceso Alúmina adscrita a la Gerencia Seguridad Patrimonial en la Empresa CVG Bauxilum, la investigación abarcara los siguientes parámetros: el reconocimiento de las debilidades y amenazas que presenta el actual sistema de identificación utilizado por la empresa, estudiar las diferentes tecnologías existentes en el mercado, realizar el estudio de factibilidad técnica, operativa y económica para el proyecto a ejecutar, planificar el proyecto y analizar los distintos escenarios utilizando un software especializado de simulación para evaluar el impacto que generara el nuevo sistema.

OBJETIVOS

Con el desarrollo de este estudio se logrará los siguientes objetivos:

OBJETIVO GENERAL:

Diseñar un sistema automatizado para la identificación y el control de acceso del personal contratista en las instalaciones de la Empresa CVG BAUXILUM.

OBJETIVOS ESPECÍFICOS:

1. Diagnosticar el actual proceso de identificación utilizado en el control de acceso de contratistas de CVG Bauxilum.
2. Evaluar los diferentes procedimientos tecnológicos de identificación y control de acceso disponible en el mercado nacional.
3. Realizar estudios de Factibilidad Técnica de las diferentes tecnologías que existen en el mercado venezolano, evaluando sus especificaciones técnicas y procurando que sea compatible con la infraestructura ya implementada en la Empresa.
4. Desarrollar estudios de Factibilidad Operativa con el fin de evaluar cuál será el impacto que tendrá dicho sistema.
5. Elaborar el estudio de Factibilidad Económica mediante el uso de análisis de costos/beneficio, todos los costos y beneficios de adquirir y operar cada sistema alternativo, identificando y realizando una comparación de ellos.

CAPÍTULO II

MARCO TEÓRICO

En este capítulo se da a conocer los diferentes términos necesarios para la comprensión plena de los temas presentados en capítulos posteriores. Así como también el identificar el área de trabajo y describir la empresa haciendo mención en: Misión, Visión, Ubicación, Objetivos, Funciones, Estructura, entre otros.

DESCRIPCIÓN DE LA EMPRESA

C.V.G BAUXILUM es la empresa resultante de la fusión entre Bauxiven (fundada en 1979) e Interalúmina (fundada en 1977) en marzo de 1994. Está conformada por las operadoras Bauxita y Alúmina.

La Operadora Bauxita se encarga de la explotación de los yacimientos del mineral en la zona de Los Pijiguaos, correspondiente al Municipio Cedeño del Estado Bolívar, tiene una capacidad instalada de 6 millones de TM al año.

Inició sus operaciones oficialmente en 1983, enviando las primeras gabarras con mineral de bauxita, a través del río Orinoco, desde el puerto El Jobal hasta el muelle de la Operadora de Alúmina en Matanzas. La Operadora de Alúmina cuyo objetivo es transformar la bauxita procedente de Los Pijiguaos, por medio del Proceso Bayer, en alúmina en grado metalúrgico y su capacidad instalada es de 2 millones de TM al año. Inició oficialmente sus operaciones el 24 de abril de 1983. Su capacidad instalada inicial fue de

1.000.000 TM al año y en 1992, mediante la implementación del plan de ampliación, fue aumentada su capacidad a 2 millones de TM al año.

La bauxita y la alúmina constituyen la principal materia prima para la obtención de aluminio primario. Tanto las ventas de bauxita como de alúmina se dirigen fundamentalmente al mercado nacional, básicamente para alimentar a las empresas C.V.G Alcasa y C.V.G Venalum, productoras de Aluminio, destinándose un porcentaje de la producción al mercado internacional.

UBICACIÓN GEOGRÁFICA DE LA EMPRESA

C.V.G. Bauxilum, Matanzas, se encuentra ubicada al Sur Oriente del país, en Ciudad Guayana, Estado Bolívar, en la Zona Industrial Matanzas, parcela 523-01-02, Avenida Fuerzas Armadas, frente a la Empresa C.V.G. Venalum; sobre el margen derecho del Rio Orinoco, aproximadamente a 350 kilómetros de su desembocadura y a 17 kilómetros de su confluencia con el río Caroní. Cubre un área de 841.000 metros cuadrados, ver figura 2.1, 2.1 y 2.3 respectivamente.

Figura 2.1: Ubicación Geográfica.

Fuente: Google Earth.

Figura 2.2: Instalaciones CVG Bauxilum.

Fuente: Google Earth.

Figura 2.3: Vista Superior de la Planta de CVG Bauxilum.

Fuente: Google Earth.

MISIÓN

"Impulsar el crecimiento sustentable de la industria nacional, satisfaciendo la demanda de bauxita y alúmina en forma competitiva y rentable, promoviendo el desarrollo endógeno, como fuerza de transformación social y económica".

VISIÓN

"Constituirnos en una empresa socialista, contribuyendo al desarrollo sustentable de la industria nacional del aluminio, a los fines de alcanzar la soberanía productiva, con un tejido industrial consolidado y desconcentrado, con nuevas redes de asociación fundamentadas en la participación y la inclusión social rumbo al Socialismo Bolivariano".

OBJETIVOS DE LA EMPRESA

OBJETIVO GENERAL:

El objetivo básico de C.V.G. Bauxilum es garantizar la producción y abastecimiento de Bauxita y Alúmina de grado metalúrgico, en términos de calidad, oportunidad y costos, para satisfacer los requerimientos de los principales consumidores de alúmina del país como lo son C.V.G. Alcasa y C.V.G. Venalum, así como también, del mercado internacional.

OBJETIVOS ESPECÍFICOS

Dentro de los objetivos específicos de la empresa por área se encuentran los siguientes:

1. **Producción**: Optimizar la producción y la eficiencia del proceso productivo en concordancia con la capacidad instalada y de acuerdo con las exigencias de los mercados internacionales con relación a la calidad, costos y oportunidades.
2. **Mercadeo y ventas:** Maximizar los ingresos de la empresa mediante la venta de productos de la industria del aluminio, cumpliendo oportunamente a los clientes con la calidad requerida y a precios competitivos.
3. **Procura:** Certificar la adquisición de materias primas, equipos, insumos y servicios de calidad y oportunidad requerida a costos competitivos**.**
4. **Tecnología:** Lograr el dominio tecnológico de los procesos productivos e impulsar el desarrollo de nuevas tecnologías que incrementen la competitividad de la empresa en la industria mundial del aluminio.
5. **Finanzas:** Mantener una adecuada estructura financiera que contribuya a mejorar la competitividad y el valor de la empresa**.**
6. **Organización:** Disponer de una adecuada estructura organizativa de los sistemas de soporte que faciliten el cabal cumplimiento de los objetivos de la empresa.
7. **Recursos Humanos:** Disponer de un recurso humano competente, identificado con la organización y con alta motivación que satisfaga la competitividad de la empresa.
8. **Imagen:** Idear a C.V.G. Bauxilum como empresa rentable y competitiva vinculada con el desarrollo Nacional y Regional.

POLÍTICA DE CALIDAD, AMBIENTE, SALUD Y SEGURIDAD DE LA EMPRESA.

Fomentar el desarrollo, la participación del Recurso Humano y el mejoramiento continuo, en los procesos de explotación de Bauxita y producción de Alúmina, cumpliendo con las normas de Calidad, Ambiente, Salud y Seguridad Laboral para satisfacer los requerimientos y expectativas de nuestros clientes, con altos niveles de rentabilidad, competitividad y responsabilidad social.

OBJETIVOS DE CALIDAD, AMBIENTE, SALUD Y SEGURIDAD DE LA EMPRESA

1. Satisfacer los requerimientos de bauxita y alúmina de la industria nacional.

Promover el desarrollo endógeno impulsando las potencialidades de la empresa, la economía popular y el cooperativismo.

Mejorar la eficacia de los procesos operativos y administrativos.

Incrementar los niveles de producción.

Optimizar el uso de la tecnología de información**.**

FUNCIÓN DE LA EMPRESA

C.V.G Bauxilum, a través de sus dos operadoras tiene como tarea la extracción del mineral de bauxita en los Pijiguaos y su transportación a Ciudad Guayana, para ser refinada; obteniendo alúmina metalúrgica que posteriormente es transformada en aluminio primario.

ORGANIGRAMA DE LA EMPRESA

En la figura 2.4, se muestra la estructura organizativa de CVG BAUXILUM MATANZA, aprobada desde el 13 de junio de 2014.

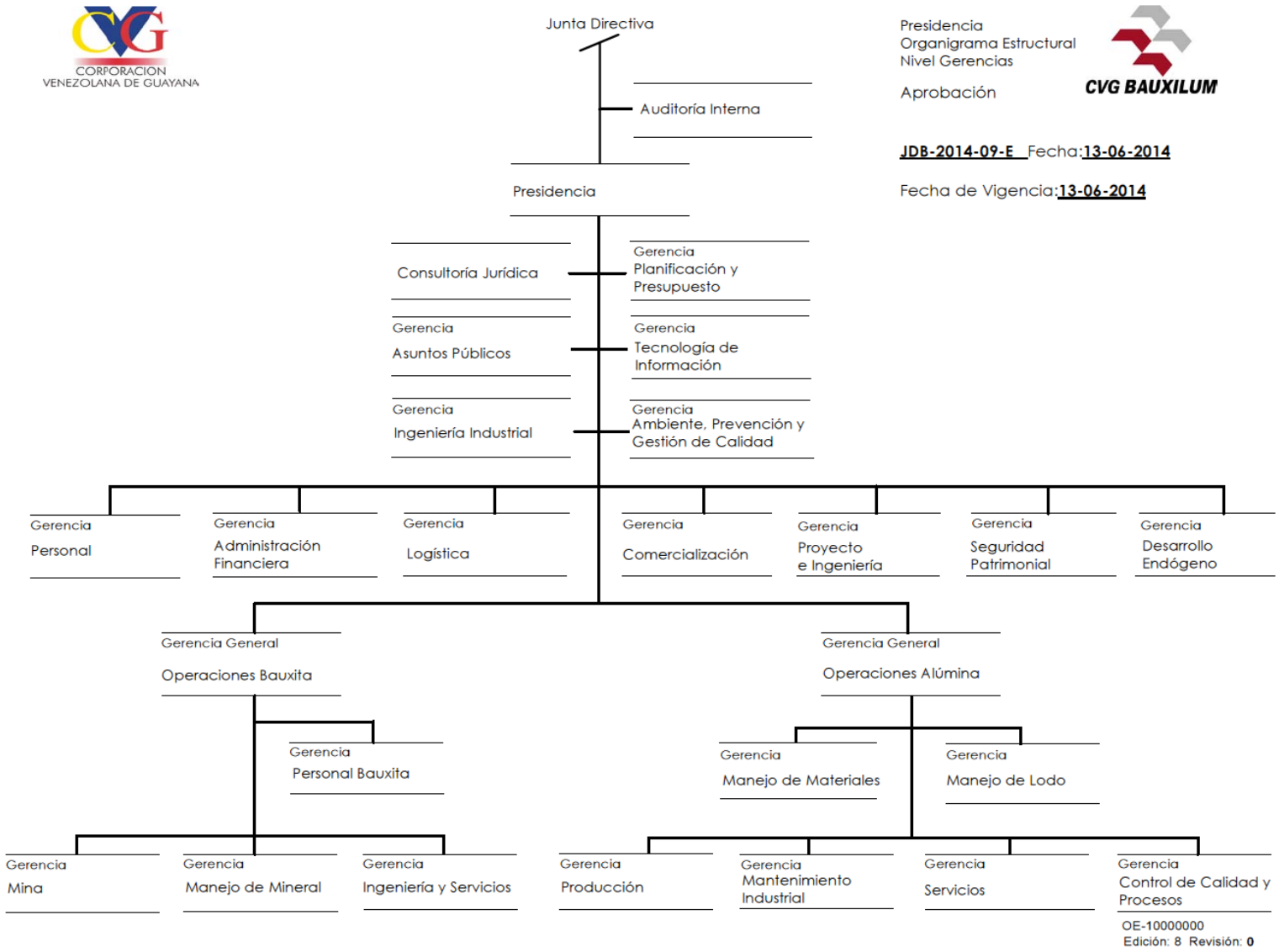


Figura 2.4. Estructura Organizativa de C.V.G Bauxilum.

Fuente: Bauxilum SDI (Sistema de Documentación Interna).

DIVISIÓN DONDE SE REALIZARÁ LA INVESTIGACIÓN

La División Identificación y Control De Acceso Alúmina, enmarcada en el plano funcional que contribuye directamente con los objetivos de la Gerencia. Estableciendo planes y programas de monitoreo permanentes que garanticen el desarrollo de medidas preventivas y la atención oportuna ante hechos delictivos o situaciones de riesgos al personal, instalaciones y áreas estratégicas de la Empresa, en Matanzas, en la figura 2.5 se puede apreciar el organigrama estructural de la gerencia.

GERENCIA SEGURIDAD PATRIMONIAL

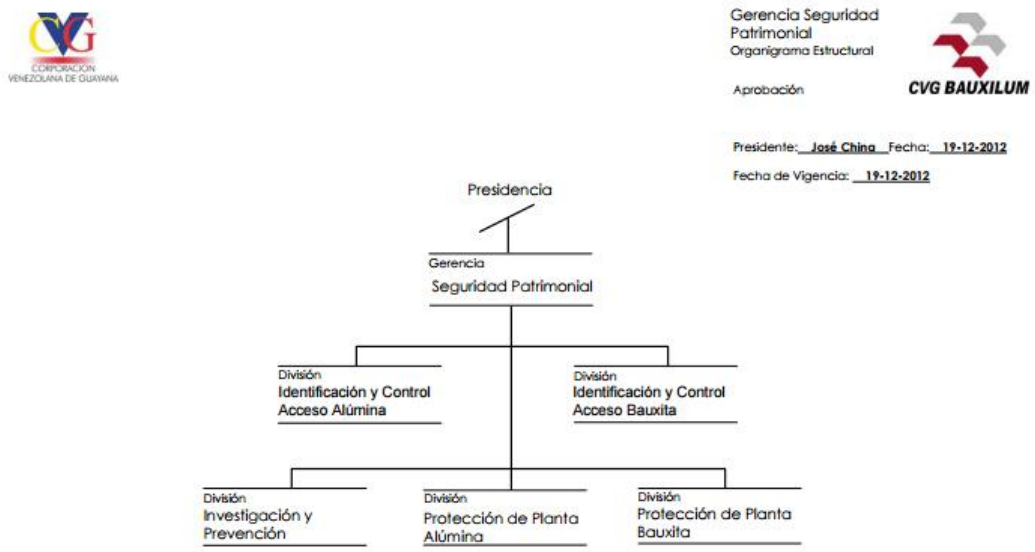


Figura 2.5: Estructura Organizativa de la Gerencia Seguridad Patrimonial.
Fuente: Bauxilum SDI (Sistema de Documentación Interna).

ÁREA DE INVESTIGACIÓN

Por medio de la División Identificación y Control (adscrita a la Gerencia Seguridad Patrimonial) se asignó el siguiente proyecto: Diseño del sistema de automatización para la identificación y control de acceso del personal contratista en las instalaciones de CVG BAUXILUM Operadora Matanzas; este proyecto estará comprendido por los siguientes ítems:

- Diagnosticar el actual proceso de identificación utilizado en el control de acceso de contratistas de CVG Bauxilum.
- Evaluar los diferentes procedimientos tecnológicos de identificación y control de acceso disponibles en el mercado nacional.
- Realizar estudios de Factibilidad Técnica de las diferentes tecnologías que existen en el mercado Venezolano, evaluando sus especificaciones técnicas y procurando de que sea compatible con la infraestructura ya implementada en la Empresa.
- Desarrollar estudios de Factibilidad Operativa con el fin de evaluar cuál será el impacto que tendrá dicho sistema.
- Elaborar el estudio de Factibilidad Económica mediante el uso de análisis de costos/beneficio, todos los costos y beneficios de adquirir y operar cada sistema alternativo, identificando y realizando una comparación de ellos.

GLOSARIO DE TÉRMINOS

- **Planificación:** Es el proceso de establecer metas y elegir medios para alcanzar dichas metas, y es un proceso continuo que refleja

los cambios del ambiente en torno a cada organización y busca adaptarse a ellos.

- **Microsoft Project:** Es un software de administración de proyectos diseñado, desarrollado y comercializado por Microsoft para asistir a administradores de proyectos en el desarrollo de planes, asignación de recursos, tareas, dar seguimiento al progreso, administrar presupuesto y analizar cargas de trabajo.
- **Recursos**: En un proyecto se refieren a personas, material y equipo necesario para completar las tareas en un proyecto.
- **Factibilidad:** Se refiere a la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas. Generalmente la factibilidad se determina sobre un proyecto. Estos resultados se entregan a la gerencia, quienes son los que aprueban la realización del sistema informático.
- **Factibilidad Económica**: Se refiere a que se dispone del capital en efectivo o de los créditos de financiamiento necesario para invertir en el desarrollo del proyecto, mismo que deberá haber probado que sus beneficios a obtener son superiores a sus costos en que incurrirá al desarrollar e implementar el proyecto o sistema; tomando en cuenta la recesión económica y la inflación para determinar costos a futuro.
- **Factibilidad Técnica:** Indica si se dispone de los conocimientos y habilidades en el manejo de métodos, procedimientos y funciones requeridas para el diseño y desarrollo del proyecto. Además indica si se dispone del equipo y herramientas para llevarlo a cabo, y de no ser así, si existe la posibilidad de generarlos o crearlos en el tiempo requerido por el proyecto.
- **Factibilidad Operativa:** La Factibilidad Operativa permite predecir, si se pondrá en marcha el sistema propuesto, aprovechando los beneficios que ofrece, a todos los usuarios

involucrados con el mismo, ya sean los que interactúan en forma directa con este, como también aquellos que reciben información producida por el sistema.

- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "el servidor".
- **Microsoft Visio:** Es un software de dibujo vectorial para Microsoft Windows. Las herramientas que lo componen permiten realizar diagramas de oficinas, diagramas de bases de datos, diagramas de flujo de programas, UML, y más, que permiten iniciar al usuario en los lenguajes de programación.
- **Tarjeta de proximidad:** Es el nombre genérico dado a la tarjeta inteligente "sin contacto" que se utiliza para el acceso seguro o como un sistema de pago. Las tarjetas utilizadas en C.V.G. Bauxilum son tarjetas RFID de la marca HID Proximity, del modelo HID ProxCard® II que funcionan bajo una frecuencia de activación de 125 kHz y estas son tarjetas de solo lectura. La de tarjeta de proximidad funciona a una distancia entre 5 y 10 cm en la mayoría de los casos, lo que permite que el usuario los lleve en la billetera o la cartera.
- **Tarjeta RFID de Solo Lectura:** El código de identificación que contiene es único y es personalizado durante la fabricación de la tarjeta.
- **Etiquetas Pasivas:** Las etiquetas pasivas no poseen alimentación eléctrica. La señal que les llega de los lectores induce una corriente eléctrica pequeña y suficiente para operar el circuito integrado CMOS de la etiqueta, de forma que puede generar y transmitir una respuesta.

- **Lector de RFID:** Compuesto por una antena, un transceptor y un decodificador. El lector envía periódicamente señales para ver si hay alguna etiqueta en sus inmediaciones. Cuando capta una señal de una etiqueta (la cual contiene la información de identificación de esta), extrae la información y se la pasa al subsistema de procesamiento de datos.
- **Transceptor:** Es un dispositivo que cuenta con un transmisor y un receptor que comparten parte de la circuitería o se encuentran dentro de la misma caja.
- **Lenel:** Empresa dedicada a la seguridad y control de acceso, fundada en 1991.
- **OnGuard:** Es una aplicación de control de acceso avanzado que incluye características del módulo de monitoreo de alarmas. Controladores habilitados para IP que permiten la aplicación de ampliar fácilmente a todas las partes de la empresa con el grado adecuado de seguridad en la puerta.
- **Biometría:** Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos como lo son las huellas dactilares, la retina, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano.
- **Lector de Huella Digital:** Es un dispositivo de seguridad encargado de detectar los relieves del dedo por medio de luz o por medio de sensores eléctricos, posteriormente genera una imagen digital la cuál es enviada a la computadora y almacenada en una base de datos en los que se le asocia con la información de una persona.

DIAGRAMA DE PROCESO

El diagrama de proceso, es una forma gráfica de presentar las actividades involucradas en la elaboración de un bien y/o servicio terminado.

Es un diagrama detallado, además se utilizan todos los símbolos y se aplica para trabajo directo e indirecto, determina costos ocultos, con la utilización de este diagrama se le puede hacer seguimiento al personal, equipo o materia prima.

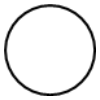
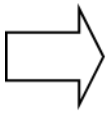
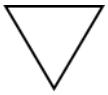
OPERACIÓN		Modificación intencional que se le hace a un objeto en cualquiera de sus características físicas o químicas.
INSPECCIÓN		Verificación de la calidad y/o cantidad de la parte.
TRANSPORTE		Indica movimiento de los trabajadores, materiales o equipos de un lugar a otro.
DEMORA		Ocurre cuando las condiciones no permiten la inmediata realización de la acción planeada (evitable o inevitable).
ALMACENAJE		Tiene lugar cuando un objeto se mantiene y protege contra un traslado no autorizado (temporal o permanente).

Tabla 1: Símbolos para elaborar diagramas

Fuente: Msc. Ing. Iván Turmero.

Simbología que se debe tomar en cuenta para la elaboración de diagramas, aplicados en el estudio mediante diagramas de procesos para mostrar una visión más clara de la situación actual de la empresa y la propuesta.

ANÁLISIS FODA

El Análisis FODA es una metodología de estudio de la situación competitiva de una empresa (situación externa) y de las características internas (situación interna) de la misma, a efectos de determinar sus Debilidades, Oportunidades, Fortalezas y Amenazas. La situación interna se compone de dos factores controlables: fortalezas y debilidades, mientras que la situación externa se compone de dos factores no controlables: oportunidades y amenazas.

MÉTODO DE LAS 6 M

Las empresas hoy en día deben manejar adecuadamente las 6M, que consiste en lo siguiente:

- **Materia prima**: Implica buscar los proveedores más adecuados, certificados de manera tal que permitan lograr la calidad o satisfacción del proceso.
- **Mano de obra**: La mano de obra que trabaje en un proceso, debe estar instruida y entrenada en las operaciones, sabiendo diferenciar un producto bueno de uno que no lo es. Deben conocer cómo reaccionar ante una no conformidad, y llevar los registros correspondientes a la operación.
  Según sea su grado de conocimiento y experiencia, pueden variar desde personal en entrenamiento con fuerte supervisión, a personal con vasta experiencia y suficiente conocimiento como para entrenar a otro operario nuevo.
- **Maquinaria:** estar constantemente dando mantenimiento preventivo de modo tal que no lleguemos a tener alguna contingencia o problema.
- **Medio ambiente:** Se refiere al orden y a la limpieza del sector laboral, y porque no a la seguridad de los operadores, y al trabajo

sostenido en un clima agradable de colaboración y respeto mutuo.

- **Medición:** contar con un adecuado control de la calidad, equipos, calibración, planes de muestro, aseguramiento de la calidad.
- **Métodos:** Las operaciones no deben hacerse de cualquier manera, sino que debe haber una forma pautada e indicada en las hojas de operaciones, que lleve a la repetitividad de acciones, de manera de asegurar la uniformidad en el resultado. El método indica la secuencia de acciones dentro de la operación, y el número de operarios involucrados.

TECNOLOGÍAS DE IDENTIFICACIÓN Y CONTROL DE ACCESO DISPONIBLES EN EL MERCADO.

En el mercado, existen diversas tecnologías para realizar un control de acceso para las empresas, entre ellos tenemos la captura de datos manual, el reconocimiento ópticos (Códigos de barras), bandas magnéticas, tarjetas inteligentes (Smart Cards), RFID y reconocimiento de características biométricas.

El uso de cada método depende en gran medida del proceso en particular que se desee automatizar (acceso peatonal y acceso vehicular), en este objetivo tendrá como finalidad entender claramente la tecnología, ventajas y desventajas así como las aplicaciones comunes en las cuales se utilizan.

Finalmente nos enfocaremos a automatizar la problemática real seleccionando entre todas las opciones actuales de Identificación Automática de Captura de Datos (AIDC, por sus siglas en inglés: Automatic Identification Data Capture), la captura de información a través de características

Biométricas, que por sus características en el registro de asistencia y control de acceso se considera la forma ideal de captura por su precisión e imposibilidad de suplantación de identidad.

1. SISTEMA DE CÓDIGO DE BARRAS

El Código de Barras es un arreglo en paralelo de barras y espacios que contiene información codificada en las barras y espacios del símbolo. Esta información puede ser analizada por dispositivos ópticos, los cuales envían la información leída hacia un servidor como si la información se hubiera tecleado.

1.1 HISTORIA

El primer sistema de código de barras fue patentado el 20 de octubre de 1949 por Norman Woodland y Bernard Silver.

Norman Joseph Woodland (6 de septiembre 1921- 9 de diciembre 2012) aprendió el código morse como Scout, el impulso que le daría alas a su idea cuando, en 1948, el encargado de un supermercado de Filadelfia se acercó al campus de la Universidad Drexel para entrevistarse con el Decano y ver si la Universidad podría ayudarle a desarrollar un sistema con el que poder automatizar el cobro de los productos en la línea de cajas.

Dicho de otra forma, el gerente del supermercado buscaba un método de codificación de los productos que permitiese aligerar el cobro de estos. Si bien al Decano de la Universidad no le hizo mucha gracia esta petición, Bernard Silver (un compañero de estudios de Joseph Woodland, 21 de septiembre 1924 – 28 de agosto 1963) escuchó parte de la conversación y fue a buscar a Woodland para ver si ellos eran capaces de solventar el problema y, quizás, encontrar una idea de negocio viable.

Woodland, convencido de que la solución era simple, utilizó el único código que conocía, el morse, pero convertido en un sencillo gráfico.

Reflexionando sobre la idea en una playa puso los dedos sobre la arena y dibujó una secuencia de 4 líneas verticales, segundos después, volvió a mover sus dedos en la arena y los giros formando un círculo.

El primer boceto de código de barras era circular, así consta en la patente de 1952 puesto que en este primer momento se pensó en la omnidireccionalidad del sistema, es decir, que se pudiese leer en cualquier dirección (de ahí el hacerlo circular). Se trataba de un "blanco" (bull's eye code) hecho mediante una serie de círculos concéntricos.

El primer prototipo del escáner dependía de un haz de luz de 500 vatios de potencia, un hecho que lo hacía inviable para una posible explotación comercial e hizo que Silver y Woodland vendiesen su patente (ver figura 2.6) a la empresa Philco por 15.000 dólares de la época y ésta la vendiese a RCA posteriormente (con un intento de explotar la tecnología comercialmente durante los años 60). Se trataba de un "blanco" (bull's eye code) hecho mediante una serie de círculos concéntricos.

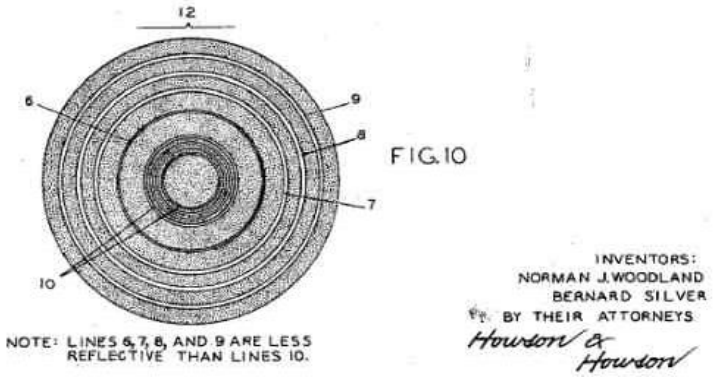


Figura 2.6: Patente US 2612994 A.

Fuente: United States Patent And Trademark Office.

1.2 EVOLUCIÓN DE LOS CÓDIGOS DE BARRAS

- 1961 es el año de aparición del primer escáner fijo de códigos de barras instalado por Sylvania General Telephone. Este aparato

leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles.

- Para 1967 la Asociación de Ferrocarriles de Norteamérica (EEUU) aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de adecuado mantenimiento de las etiquetas conteniendo los códigos.
- En 1967 la sucursal de Cincinnati (Ohio, EEUU) instala el primer sistema de "Retail" (Supermercados) basado en códigos de barras. Al cliente que encontraba un código que no se podía escanear correctamente se le ofrecía cupones de compra gratis.
- 1969, el láser hace su aparición. Usando luz de gas de Helio-Neón, el primer escáner fijo es instalado. Su costo: $10 000 USD. Hoy por hoy el mismo tipo de escáner estaría costando menos de $ 2,000 USD.
- En 1969, Rust-Oleum fue el primero en interconectar un lector de códigos con una computadora. El programa ejecutaba funciones de mantenimiento de inventarios e impresión de reportes de embarque.
- En 1970 aparece el primer terminal portátil de datos fabricado por Norand. Este utilizaba un "Wand" o lápiz de contacto.
- El código Plessey hace su aparición en Inglaterra (The Plessey Company, Dorset, Inglaterra), para control de archivos en organismos militares en 1971. Su aplicación se difundió para control de documentos en bibliotecas.
- CodaBar (ver figura 2.7) aparece en 1971 y encuentra su mayor aplicación en los bancos de sangre, donde un medio de identificación y verificación automática eran indispensables.

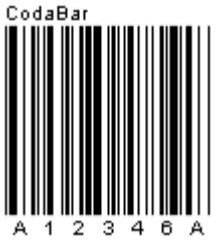


Figura 2.7: Código CodaBar.
Fuente: http://www.codabar.es/.

- Buick (la fábrica de automóviles) utilizó identificación automática en las operaciones de ensamble de transmisiones, también por los años 70. El sistema era utilizado para conteo de los diferentes tipos de transmisión ensamblados diariamente.
- ITF marca su aparición en 1972, creado por el Dr. David Allais, en ese entonces de Intermec (empresa dedicada a la fabricación y desarrollo de tecnología de captura de datos) Ver figura 2.8.

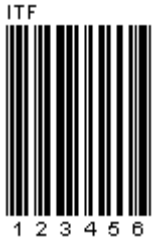


Figura 2.8: Código ITF.
Fuente: http://www.gs1gt.org.

- En el año 1973 se anuncia el código U.P.C. (Universal Product Code) que se convertiría en el estándar de identificación de productos en Estados Unidos de Norteamérica. De esta forma la actualización automática de inventarios permitía una mejor y más oportuna compra y reabastecimiento de bienes.

- En 1974, Europa se hace presente con su propia versión de U.P.C., el código EAN (European Article Number), la asociación recibe el mismo nombre y se pueden observar cuyas diferencia en la figura 2.9.

Figura 2.9: Código UPC y EAN.
Fuente: http://www.gs1.org/.

- En 1974, nuevamente el Dr. Allais conjuntamente con Ray Stevens de Intermec inventa el código 39, el primero de tipo alfanumérico. (Ver figura 2.10).

Figura 2.10: Código 39.
Fuente: http://www.gs1.org/.

- En 1977 por la internacionalización de la Asociación y derivado de la alta aceptación de utilizar este tipo de simbologías, el organismo cambia el nombre de EAN por EAN Internacional, ahora GS1. Actualmente existen 104 organizaciones miembro representadas en 145 países. Estas organizaciones

proporcionan el apoyo total y la información a sus compañías locales. Más de un millón de compañías a nivel mundial se benefician de usar el Sistema GS1. AMECE es el organismo que representa a México. Al ingresar a esta asociación se conoce a detalle la forma de uso de los códigos de barras y las regulaciones pertinentes.

- En 1978 Aparece el primer sistema patentado de verificación de códigos de barras por medio de láser.
- En 1980 El código PostNet (Ver figura 2.11), aparece como consecuencia de un requerimiento particular del Servicio Postal de los EEUU de automatizar los procesos de entrega y recolección de mensajería.

Figura 2.11: Código PostNet.
Fuente: http://www.gs1.org/.

- En 1981 aparece la tecnología de lectura CCD (Charge Coupled Device) es aplicada en un escáner, En la actualidad este tipo de tecnología tiene bastante difusión en el mercado asiático, mientras que el láser domina en el mundo occidental. En ese año también aparece el código 128 (ver figura 2.12), de tipo alfanumérico.

Figura 2.12: Código 128.

Fuente: http://www.gs1.org/.

- Aparece la norma ANSI MH10.8M que especifica las características técnicas de los códigos 39, CodaBar, e ITF (Interleaved Two of Five).
- El Dr. Allais es incansable. En 1987 desarrolla el primer código bidimensional, el código 49. Le sigue Ted Williams (Laser Light Systems) con el código 16K (1988).
- En 1990 se publica la especificación ANS X3.182, que regula la calidad de impresión de códigos de barras lineales.

1.3 CÓDIGOS BIDIMENSIONALES.

En el año 1990, Symbol Technologies (empresa líder en la fabricación y desarrollo de tecnología de captura de datos y que fue adquirida por Motorola en el año de 2007) presenta el código bidimensional PDF417y QR.

- **Código PDF 417**: Estándar de código de barras bidimensional, este tipo de código está compuesto por 3 a 90 filas de símbolos de código de barras lineales. Tiene una gran capacidad de codificar datos hasta 1800 caracteres de texto o 2710 dígitos. Se emplea en diversas industrias para codificar información de documentos, mercancías y materiales. Se pueden apreciar sus características en las figuras 2.13 y 2.14.

Figura 2.13: Código Bidireccional PDF417.
Fuente: Symbol Technologies.

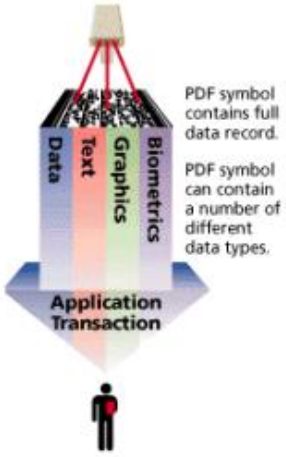


Figura 2.14: Symbol Technologies que presenta el Código PDF.
Fuente: Symbol Technologies http://www.gs1.org/.

- **Código QR**: Su nombre viene de “Quick Response” y es una simbología que provee lecturas muy rápidas, de forma omnidireccional y cuenta con buenos algoritmos de corrección de error. Sin embargo, al igual que la simbología anterior, los patrones de identificación se encuentran en las orillas, lo que puede traer problema de lectura cuando las condiciones del código no son óptimas. Debido a la ubicación del patrón de referencia, también se requieren áreas en blanco circundantes para que pueda ser correctamente decodificado. (Ver figura 2.15)

Figura 2.15: Código QR.
Fuente: Symbol Technologies.

1.4 MÉTODOS DE IMPRESIÓN DE CÓDIGOS DE BARRAS.

- **Impresión Directa**: El Código de Barras puede ser impreso como parte de la cara comercial del producto y se utiliza cualquier sistema de impresión convencional (offset, serigrafía, roto grabado, flexografía, litografía, etc.). Se necesita de una "película maestra" para que el impresor pueda hacer su trabajo.
- **Impresión a Solicitud**: Si no es posible o no se desea que el Código de Barras sea impreso como parte del empaque, éste puede ser fijado en una etiqueta (auto adherible, colgante, cosida, etc.). Generalmente las etiquetas son impresas en transferencia térmica, térmicas o láser. Estos sistemas no requieren de una película maestra.
- **Impresión Térmica**: Este proceso de impresión generalmente se usa en impresoras de etiquetas. Muchas impresoras de etiquetas pueden usar un medio de transferencia térmica directa o transferencia térmica. Básicamente, la impresión térmica directa tiene impresas barras de color negro intenso. El problema es que solamente el ojo humano puede ver el negro intenso. Para el lector, generalmente tienen una apariencia algo gris. Para mejorar esto, debe cambiarse el material ya que el valor de reflejo para las barras depende de los químicos sensibles al calor del papel.

1.5 APLICACIONES.

Las aplicaciones del código de barras cubren prácticamente cualquier tipo de actividad humana, tanto a la empresa, como también para los comercios, instituciones educativas, instituciones médicas, gobierno, etc.

- Control de acceso y Control de asistencia.

- Control de material en proceso.
- Control de Inventario.
- Punto de Venta (POS).
- Control de calidad.
- Embarques y recibo de mercancía.
- Control de documentos.
- Facturación.
- Bibliotecas.
- Bancos de sangre.
- Hospitales.

1.6 VENTAJAS:

- Se imprime a bajos costos.
- Porcentajes muy bajos de error.
- Mayor velocidad de captura.
- Los equipos de lectura e impresión de código de barras son flexibles y fáciles de conectar e instalar.

1.7 DESVENTAJAS:

- Problemas de lecturas debido a que debe estar en línea de visión con el láser y en modo horizontal.
- Los lectores de códigos de barras no pueden leer etiquetas que estén arrugadas, sucias, manchadas o dañadas.
- El costo de los equipos utilizados como control de acceso son elevados.

2. TARJETA CON BANDA MAGNÉTICA

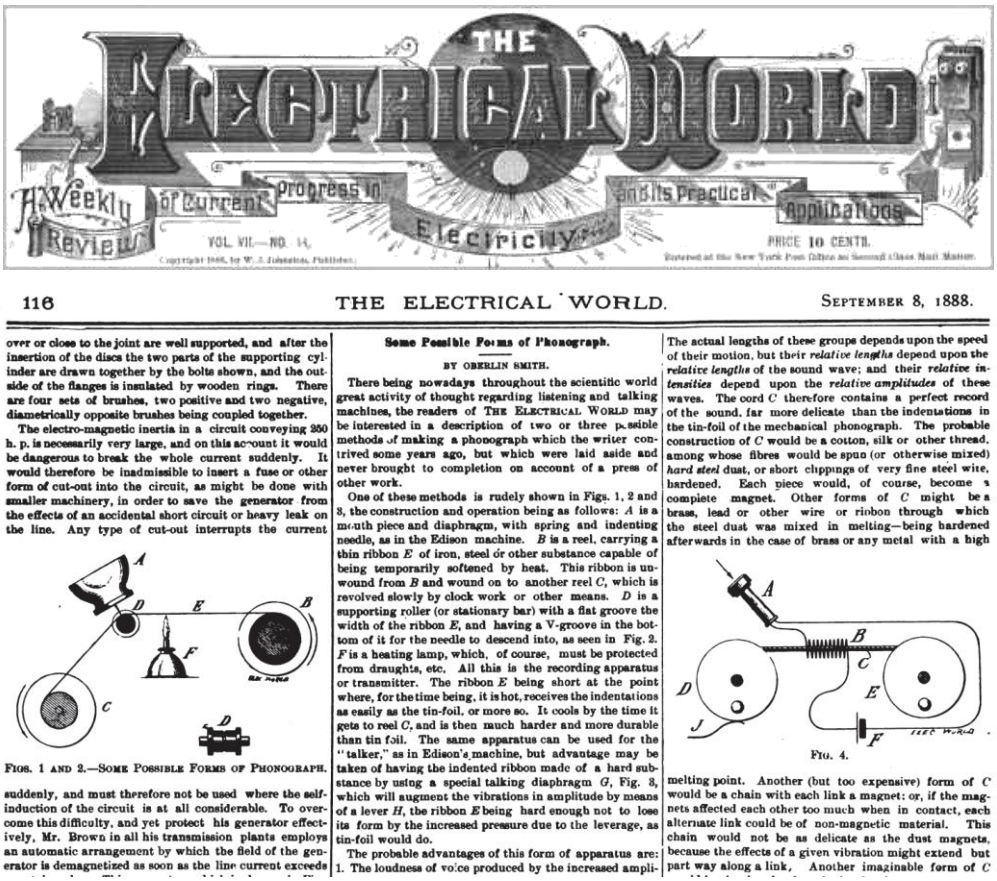
La banda magnética en tarjetas de plástico es un método, de bajo costo, que te permite hacer una lectura rápida y confiable de ciertos datos con los que identificas dicha tarjeta.

Es comúnmente usada en métodos de control de acceso, cajeros automáticos, tarjetas de alimentación, certificados de regalo, llaves electrónicas, entre otras.

2.1 HISTORIA

Oberlin Smith (22 de marzo de 1840 - 19 de julio de 1926) puede ser considerado el padre de la grabación magnética analógica de sonido desde el punto de vista teórico. En sus investigaciones descubrió las propiedades de las partículas ferromagnéticas en interacción con un electroimán. Se considera como uno de los pioneros de la radiodifusión. A pesar de que hay poca información sobre su persona, su aportación es un eslabón fundamental que ha de ser tomado en consideración.

Oberlin Smith publica en la revista Electrical World del 8 de septiembre de 1888 un artículo (Ver figura 2.16) donde explicaba los principios básicos para grabar señales en un soporte magnético.



THE ELECTRICAL WORLD

A Weekly Review of Current Progress in Electricity and its Practical Applications

VOL. VII.—NO. 14. PRICE 10 CENTS.

Entered at the New York Post Office as Second Class Mail Matter.

over or close to the joint are well supported, and after the insertion of the discs the two parts of the supporting cylinder are drawn together by the bolts shown, and the outside of the flanges is insulated by wooden rings. There are four sets of brushes, two positive and two negative, diametrically opposite brushes being coupled together.

The electro-magnetic inertia in a circuit conveying 350 h. p. is necessarily very large, and on this account it would be dangerous to break the whole current suddenly. It would therefore be inadmissible to insert a fuse or other form of cut-out into the circuit, as might be done with smaller machinery, in order to save the generator from the effects of an accidental short circuit or heavy leak on the line. Any type of cut-out interrupts the current

FIGS. 1 AND 2.—SOME POSSIBLE FORMS OF PHONOGRAPH.

suddenly, and must therefore not be used where the self-induction of the circuit is at all considerable. To overcome this difficulty, and yet protect his generator effectively, Mr. Brown in all his transmission plants employs an automatic arrangement by which the field of the generator is demagnetized as soon as the line current exceeds

Some Possible Forms of Phonograph.

BY OBERLIN SMITH.

There being nowadays throughout the scientific world great activity of thought regarding listening and talking machines, the readers of THE ELECTRICAL WORLD may be interested in a description of two or three possible methods of making a phonograph which the writer contrived some years ago, but which were laid aside and never brought to completion on account of a press of other work.

One of these methods is rudely shown in Figs. 1, 2 and 3, the construction and operation being as follows: *A* is a mouth piece and diaphragm, with spring and indenting needle, as in the Edison machine. *B* is a reel, carrying a thin ribbon *E* of iron, steel or other substance capable of being temporarily softened by heat. This ribbon is unwound from *B* and wound on to another reel *C*, which is revolved slowly by clock work or other means. *D* is a supporting roller (or stationary bar) with a flat groove the width of the ribbon *E*, and having a V-groove in the bottom of it for the needle to descend into, as seen in Fig. 2. *F* is a heating lamp, which, of course, must be protected from draughts, etc. All this is the recording apparatus or transmitter. The ribbon *E* being short at the point where, for the time being, it is hot, receives the indentations as easily as the tin-foil, or more so. It cools by the time it gets to reel *C*, and is then much harder and more durable than tin foil. The same apparatus can be used for the "talker," as in Edison's machine, but advantage may be taken of having the indented ribbon made of a hard substance by using a special talking diaphragm *G*, Fig. 3, which will augment the vibrations in amplitude by means of a lever *H*, the ribbon *E* being hard enough not to lose its form by the increased pressure due to the leverage, as tin-foil would do.

The probable advantages of this form of apparatus are: 1. The loudness of voice produced by the increased ampli-

The actual lengths of these groups depends upon the speed of their motion, but their *relative lengths* depend upon the *relative lengths* of the sound wave; and their *relative intensities* depend upon the *relative amplitudes* of these waves. The cord *C* therefore contains a perfect record of the sound, far more delicate than the indentations in the tin-foil of the mechanical phonograph. The probable construction of *C* would be a cotton, silk or other thread, among whose fibres would be spun (or otherwise mixed) *hard steel* dust, or short clippings of very fine steel wire, hardened. Each piece would, of course, become a complete magnet. Other forms of *C* might be a brass, lead or other wire or ribbon through which the steel dust was mixed in melting—being hardened afterwards in the case of brass or any metal with a high

FIG. 4.

melting point. Another (but too expensive) form of *C* would be a chain with each link a magnet; or, if the magnets affected each other too much when in contact, each alternate link could be of non-magnetic material. This chain would not be as delicate as the dust magnets, because the effects of a given vibration might extend but part way along a link. Another imaginable form of *C*

Figura 2.16: Principios básicos para grabar señales en un soporte magnético. Fuente: The Electrical World.

El sistema de grabación magnética de Smith se basaba en un electroimán y una cuerda cubierta de limaduras de hierro. Se conserva un diagrama de cómo debía realizarse la grabación, pero si Smith construyó algún tipo de prototipo, éste no se conserva en la actualidad, ni ninguna grabación que pudiese haberse realizado con él. Oberlin Smith no siguió con estas investigaciones, porque era empresario en otro campo que poco tenía que ver con la radiodifusión.

2.2 EVOLUCIÓN DE LA CINTA MAGNÉTICA

- En 1898 cuando Valdemar Poulsen invento un grabador eléctrico sobre una tira de material flexible cubierta de polvo imantado, antecesor de la cinta magnetofónica actual y fue patentado en Estados Unidos bajo la patente US661619 (Ver figura 2.17).

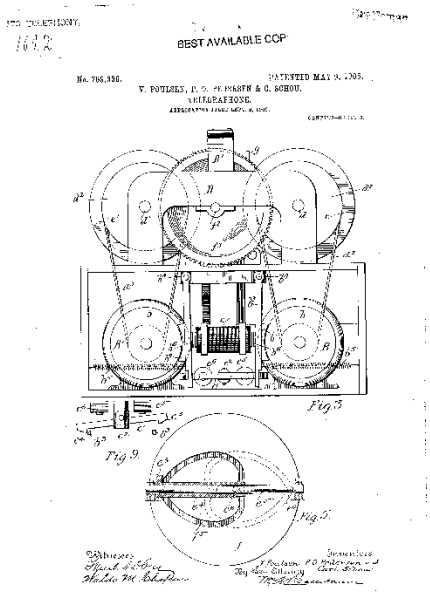


Figura 2.17: Patente US661619.

Fuente: United States Patent And Trademark Office.

- Las primeras tarjetas con banda magnética fueron usadas desde principios de los sesentas en el transporte público, London Transit Authority instaló un sistema de tarjeta con banda magnética en el sistema de tren London Underground, en Londres.
- A nivel de entidades financieras se empezaron a usar en 1951, a finales de los sesentas implementaron la tarjeta plástica con banda magnética como se aprecian a continuación en la figura 2.18.

Figura 2.18: Primeras tarjeta plástica con banda magnética.
Fuente: https://www.americanexpress.com.

- En 1970 cuando se establecieron los estándares internacionales (ISO/IEC 7811 Identification cards - Recording technique) el uso de la banda magnética se masificó y se extendió su uso a nivel mundial.
- En 1971 The American Banking Association en Estados Unidos aprobó el uso de la banda magnética a nivel bancario.
- El 16 de enero de 1973 Robert E. Lawhend y William E. Steele patentaron una impresora para tarjetas con banda magnética, que fue asignada a Internacional Business Machines Corp. (IBM) con la patente No. 3711359 en Estados Unidos.

2.3 LA BANDA MAGNÉTICA

La banda magnética es una banda negra o marrón, esta banda está hecha de finas partículas magnéticas en una resina. Las partículas pueden ser aplicadas directamente a la tarjeta o pueden ser hechas en forma de banda magnética y después ser adherida a la tarjeta, en la figura 2.19 se puede apreciar dicha banda sometida a un microscopio.

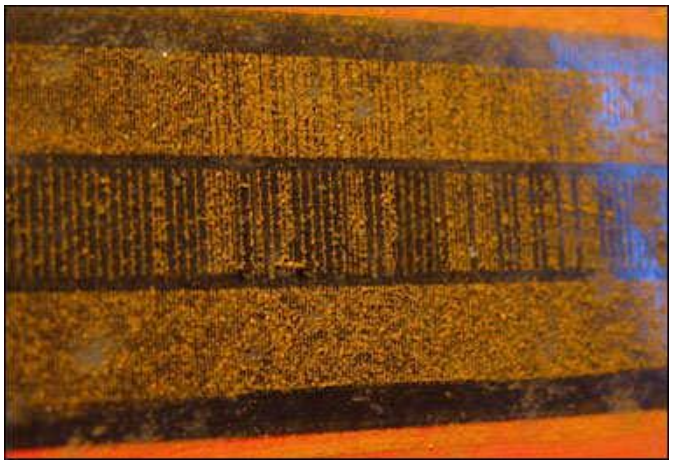


Figura 2.19: Polvo de óxido de hierro sobre la banda magnética.

Fuente: http://www.tetherdcow.com/.

La banda magnética tiene una característica muy particular y es el material en que fue construida, puede ser de baja coercitividad Lo-CO o Bajo Costo (banda marrón) hecha de óxido de hierro, o de alta coercitividad Hi-CO o Alto Costo (banda negra) hecha de ferrita de bario.

El estándar ISO/IEC 7811 define la amplitud de señal para las tarjetas que son usadas en un ambiente de intercambio de información. La densidad de bits de información es seleccionada basada en los requerimientos del usuario. El estándar ISO/IEC 7811 establece los requerimientos de densidad de bits para las tarjetas en un ambiente de intercambio figura 2.20.

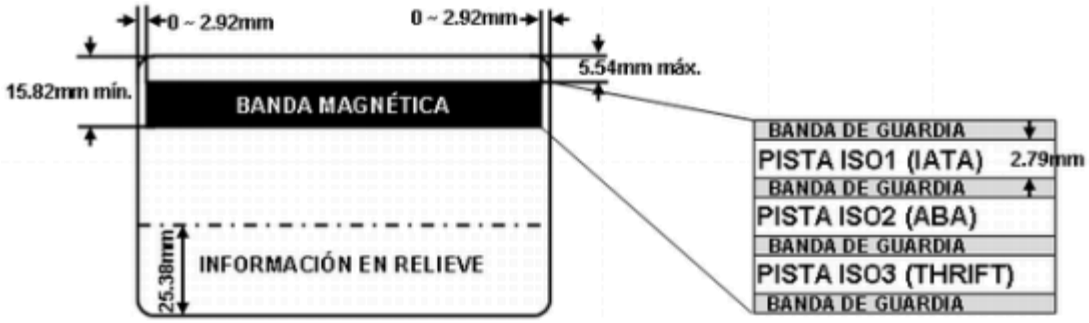


Figura 2.20: Estándar ISO/IEC 7811.

Fuente: http://www.iso.org/.

2.4 VENTAJAS

- Clave privada no sale de tarjeta.
- Cifrado de información.
- Posibilidad de tener varias contraseñas.
- Certificados y claves portátiles.
- Facilidad de uso.
- Comodidad para usuario.
- Estándares específicos.
- Capacidad de memoria.

2.5 DESVENTAJAS

- PIN es muy vulnerable.
- Se puede extraviar fácilmente.
- Recuperación de información de tarjeta robada o perdida.
- Clonación de la tarjeta.
- Sensible a fluidos.
- Necesaria infraestructura.
- Coste de producción.
- Desgaste por uso.

3. SISTEMAS DE TARJETAS INTELIGENTES (SMARTCARD).

Las Smart Cards son unas tarjetas de plástico con un tamaño definido normalmente por la razón que incluye un microchip (Estándar ISO 7816, Electronic Identification Cards With Contacts SmartCard). Mucha gente considera que las tarjetas inteligentes son un invento reciente, sin embargo llevan usándose desde los años 70.

3.1 EVOLUCIÓN DE LA SMART CARDS

- 1974: Roland Moreno de Francia registra la patente original para las IC Cards (tarjetas de circuito integrado), más tarde adoptada por las Smart Card.
- 1977: Tres fabricantes comerciales, Bull CP8, SGS Thomson, y Schlumberger empezaron a desarrollar el producto IC Card.
- 1979: Motorola desarrolla el primer microcontrolador uni-chip seguro, para uso en la banca francesa.
- 1982: La prueba de campo de las tarjetas de teléfono con memoria serie tuvo lugar en Francia – La primera y mayor prueba de IC cards del mundo.
- 1984: El proceso de las tarjetas bancarias ATM con chip, tuvo un comportamiento exitoso.
- 1986: En marzo, 14,000 tarjetas equipadas con el Bull CP8 se distribuyeron a clientes del Banco de Virginia y del Banco Nacional de Maryland. Además, 50,000 tarjetas Casio se distribuyeron a clientes del Banco Nacional Primero de Palm Beach y del banco Mall.
- 1987: La primera aplicación a gran escala de Smart Card es implementada en los Estados Unidos con la tarjeta de marketing del maní a nivel nacional del departamento de agricultura de los EE.UU.
- 1991: Primer proyecto de Smart Card de transferencia de beneficios electrónicos (EBT). El proyecto es lanzado en Wyoming para el programa de nutrición especial suplementaria para mujeres, bebés y niños.
- 1992: Un proyecto de tarjeta de Prepago (monedero electrónico) se inicia a nivel nacional en Dinamarca y Venezuela (Ver figura 2.21).

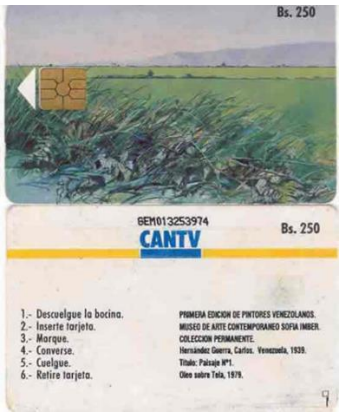


Figura 2.21: Tarjeta Prepago para telefonía pública CANTV.
Fuente: http://www.cantv.net/.

- 1993: Prueba de campo de aplicaciones de Smart Card multi-funcion en Rennes, Francia. La función Telecarte (para teléfonos públicos) se habilitó en Smart Card bancarias.
- 1994: Europay, MasterCard, y Visa (EMV) publicaron especificaciones compartidas para Smart Card bancarias globales. Alemania inicia una expedición con 80 millones de Smart Cards de memoria como tarjetas de salud del ciudadano
- 1995: Más de 3 millones de usuarios de teléfono móvil empiezan a entablar y tarificar llamadas con Smart Cards.
- 1996: Más de 1.5 millones de tarjetas de valor almacenado VISACash se expidieron para las olimpiadas de Atlanta.
- MasterCard y Visa empezaron el patrocinio del consorcio de competición para trabajar en la solución de problemas de interoperabilidad de las Smart Cards; dos soluciones diferentes fueron desarrolladas: La JavaCard respaldada por VISA, y el sistema operativo multi-aplicación (MULTOS) respaldado por Mastercard.
- 1998: En septiembre, la administración de servicios generales del gobierno de los EE.UU. y la marina de los EE.UU. unieron

fuerzas e implementaron un sistema Smart Card de nueve aplicaciones y una solución para la gestión de tarjetas. El propósito primordial evaluar la integración de Smart Cards multi-aplicación con otro tipo de tecnologías, buscando sistemas hábiles para el uso de gobierno federal.

- Microsoft anunció su Nuevo sistema operativo Windows para Smart Card. Francia inició el reparto de Smart Cards sanitarias para sus 50 millones de habitantes.
- 2004: Se extiende el uso de las Smart Cards para su uso en el transporte público. Se implanta en ciudades como Chicago, Londres, Boston…
- 2006: Comienza en España el despliegue del DNI electrónico o Cedula de Identidad (Ver Figura 2.22).

Figura 2.22: DNI Electrónico.

Fuente: http://www.dnielectronico.es/.

- 2009: Inicia la migración de las tarjetas bancarias en Venezuela, pasando del estándar de barras magnéticas a utilizar las Smart Cards utilizando las especificaciones EMV con el fin de eliminar el fraude y clonación de tarjetas.

3.2 TECNOLOGÍA

Las Smart Cards las podemos clasificar según sus componentes como Memory Cards y Chip Cards (con procesador).

3.3 MEMORY CARDS

Son las Smart Cards más comunes y baratas. Su objetivo es almacenar datos. El contenido de una Memory Card es:

- **EEPROM (Electrically Erasable Programmable Read-Only Memory):** Es un dispositivo que almacena datos dónde todas las aplicaciones pueden escribir. El tamaño de la EEPROM oscila entre 2KB y 8KB. El acceso a los datos de la EEPROM pueden ser bloqueados con un PIN. Por ejemplo, en una tarjeta de teléfono la EEPROM puede mantener el valor del saldo que nos queda.
- **ROM (Read-Only Memory):** Los datos que almacena no se pueden alterar nunca. Siguiendo el mismo ejemplo de la tarjeta de teléfono, en la ROM guardaría el número de la tarjeta, el nombre dela empresa, entre otros.

3.4 CHIP CARDS

Estas tarjetas incorporan un microprocesador. Los principales componentes del chip de una tarjeta son:

- **ROM (Read-Only Memory):** La ROM almacena el sistema operativo que se escribe solamente una vez (durante la fabricación de la tarjeta). Los tamaños de la ROM suelen estar comprendidos entre 8KB y 32KB, dependiendo del sistema operativo que se vaya a usar. Tal como su nombre indica, estas tarjetas son escritas una vez y ya no se puede cambiar su contenido almacenado.
- **EEPROM (Electrically Erasable Programmable Read-Only Memory):** En la EEPROM se almacenan las aplicaciones de la tarjeta y sus datos. En esta memoria se permite libre acceso

(inserción, extracción y borrado). Los tamaños varían desde 2KB a 32KB.

- **RAM (Random Access Memory):** Es la memoria volátil usada por el procesador para ejecutar las funciones pertinentes. La memoria es borrada cuando la alimentación se anula. El tamaño típico de la RAM ronda los 256 bytes, debido a que se le reserva un área muy pequeña, restringida a 25 mm^2
- **CPU (Central Processing Unit):** Es el corazón de la tarjeta. Normalmente se usan microprocesadores de 8 bits basados en la arquitectura CISC con una frecuencia de reloj de 5 Mhz. Aunque muchas ya implementan microprocesadores con arquitectura de 32 bits debido a las tarjetas Java.

Las Chip Cards son algo más caras que las Memory Cards. El nivel de seguridad que ofrecen estas tarjetas es muy alto. Si dividimos el tipo de tarjeta según la interfaz obtenemos las tarjetas de contacto y las tarjetas sin contacto.

Las tarjetas de contacto deben ser insertadas dentro del lector mientras que las tarjetas sin contacto son procesadas mediante una señal de radio y no requiere la inserción en un lector. También existen unas tarjetas que permiten ambos métodos de procesamiento.

3.5 TARJETAS DE CONTACTO

Requieren la inserción en un lector de tarjetas para ser procesadas. El chip contiene de 6 a 8 contactos físicos. El contacto físico puede ser establecido por deslizamiento o por presión. La alimentación de la tarjeta la recibe del lector. Un ejemplo (Figura 2.23) de chip que cumpla el formato estándar ISO 7816 es el siguiente:

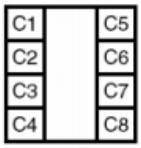


Figura 2.23: Chip estándar ISO 7816.

Fuente: http://www.iso.org/.

Los contactos están indicados por Cx. La función de cada contacto está definida como:

- C1: Vcc Suministra el voltaje
- C2: RST Reset
- C3: CLK Señal de Reloj
- C4: RFU Reservado para futuro uso
- C5: GND Tierra
- C6: Vpp Voltaje de Programación
- C7: I/O Entrada y salida de datos
- C8: RFU Reservado para futuro uso

La apariencia física y las propiedades de una Smart Card se encuentran definidas en la ISO 7816, parte 1. La ISO 7816 es el documento que establece el estándar para la industria de Smart Cards como se puede apreciar en la siguiente figura 2.24.

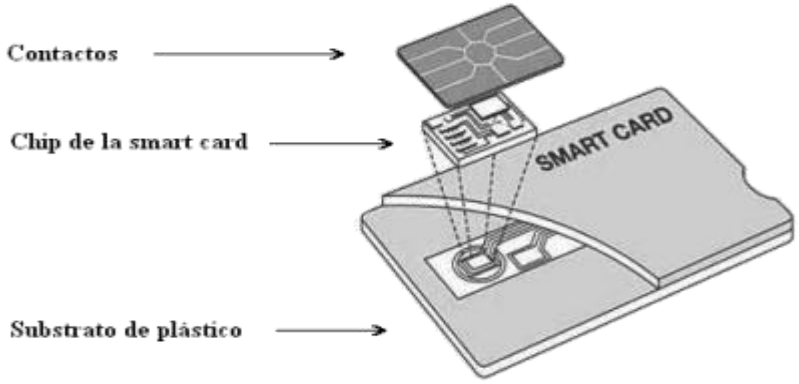


Figura 2.24: Apariencia física de una Smart Card según Estándar ISO 7816.

Fuente: http://www.iso.org/.

Normalmente una Smart Card no contiene una fuente de alimentación, o un display ni un teclado. Para comunicarse con el mundo exterior, la tarjeta se debe colocar dentro o cerca de un dispositivo que acepte estas tarjetas (CAD = Card Acceptance Device) y que está conectado a un ordenador.

Las tarjetas inteligentes también pueden ser clasificadas según su sistema operativo. En el mercado existen muchos sistemas operativos para tarjetas inteligentes. Algunos de los principales son:

- Java Card.
- MultOS.
- Chrysalis.
- Cosmo.

3.6 VENTAJAS

- Altos niveles de seguridad.
- Clave privada no sale de tarjeta.
- Cifrado de información.
- Posible tener varias contraseñas.
- Certificados y claves portátiles.
- Facilidad de uso.
- Estándares específicos.
- Capacidad de memoria.
- Capacidad de procesamiento.

3.7 DESVENTAJAS

- PIN es muy vulnerable.
- Extraviada fácilmente.
- Intercambiable.

- Recuperación de información de tarjeta robada o perdida.
- Sensible a fluidos.
- Necesaria infraestructura.
- Coste de producción.

4. TARJETAS DE PROXIMIDAD RFID.

Estas tarjetas no requieren la inserción dentro de un lector. Solamente deben ser pasadas cerca de una antena para llevar a cabo la operación. La distancia de lectura oscila entre escasos centímetros a 150 cm. Las tarjetas sin contacto son más caras, aunque poseen una vida más larga.

RFID: La identificación por radiofrecuencia o RFID por sus siglas en inglés (Radio Frequency Identification), es una tecnología de identificación remota e inalámbrica en el cual un dispositivo lector o reader vinculado a un servidor, se comunica a través de una antena con un transponder (también conocido como tag o etiqueta) mediante ondas de radio (Ver figura 2.25).

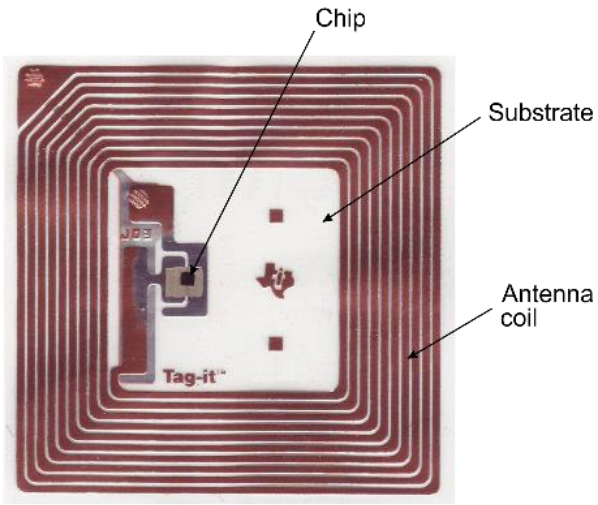


Figura 2.25: Tag RFID.

Fuente: http://www.gs1ve.org/.

4.1 HISTORIA

RFID, tecnología conocida desde hace más de seis décadas y que unida al resto de elementos anteriormente descritos ha tomado un papel fundamental en el desarrollo de la Auto identificación electrónica de productos basada en el código electrónico del producto EPC (Electronic Product Code).

La tecnología que forma la base de RFID fue primeramente desarrollada durante la segunda guerra mundial para identificar aeroplanos. En ese tiempo fue llamada tecnología de amigos o enemigos y usada por la Real Fuerza Aérea Británica.

La Tecnología RFID tuvo un sentido como herramienta de espionaje que fue inventado por Léon Theremin para el gobierno soviético en 1945. Su propósito era utilizar un dispositivo de escucha secreto pasivo y no como una etiqueta de identificación como se utiliza en la actualidad.

El ejército alemán descubrió que si los pilotos balanceaban sus aviones al volver a la base cambiaría la señal de radio reflejada de vuelta. Este método hacia así distinguir a los aviones alemanes de los aliados y se convirtió en el primer dispositivo RFID pasivo.

Las primeras patentes solicitadas en relación a la tecnología RFID se remontan a principios del año 1973 cuando Mario W. Cardullo se presentó con una etiqueta RFID activa que portaba una memoria rescribible. El mismo año, Charles Walton recibió la patente para un sistema RFID pasivo que abría las puertas sin necesidad de llaves. Una tarjeta con un transponedor comunicaba una señal al lector de la puerta que cuando validaba la tarjeta desbloqueaba la cerradura

El gobierno americano también trabajaba sobre esta tecnología en los años 70 y montó sistemas parecidos para el manejo de puertas en las centrales nucleares, cuyas puertas se abrían al paso de los camiones que portaban materiales para las mismas que iban equipados con un transponedor.

También se desarrolló un sistema para el control del ganado que había sido vacunado insertando bajo la piel de los animales una etiqueta RFID pasiva con la que se identificaba los animales que habían sido vacunados y los que no.

Con la evolución de la tecnología y la creación de los semiconductores las etiquetas RFID abrieron paso a ser un producto de consumo masivo gracias a su bajo costo, a su vez se subdividía en 3 categorías o tipos de funcionamiento: RFID pasivo cuando no tenían una fuente de alimentación propia, RFID semi-pasivo cuando utilizaban una pequeña batería asociada y RFID activo cuando tenían su propia fuente de alimentación.

Luego llegaron los sistemas de acceso basados en RFID. Estos se desarrollaron primero en la década de los 70 y 80. Unos permitían desbloquear el automóvil a varios metros de distancia, otros ahorraban el tiempo de buscar las llaves de la puerta de la oficina sólo con acercar una tarjeta.

Las investigaciones en sistemas de etiquetado de bajo coste convirtieron al RFID en un sistema extendido a finales de los 90. En ese momento las empresas empezaron a experimentar con aplicaciones que permitiesen pagar el pasaje de autobús con el teléfono móvil (NFC) o en la detección de contrabando, evitando la entrada de productos medicinales potencialmente peligrosos.

En la actualidad la tecnología RFID es utilizada por gobiernos en aplicaciones civiles y militares, en asuntos de seguridad nacional (pasaportes electrónicos), pagos inalámbricos y controles de acceso. También hacen uso de esta tecnología las grandes empresas para el seguimiento de sus productos, desde el inicio de su manufacturación hasta su destino final en los almacenes y tiendas.

Un sistema de RFID está formado por dispositivos llamados "transponders" o "tags" que contiene el EPC, y lectores electrónicos o "reader"

que se comunican con ellos. Estos sistemas se comunican vía señales de radio que transportan información de manera uni o bidireccional (distinguiendo así los tags de sólo lectura de los de escritura que permiten almacenar en el propio tag datos de interés).

Es decir, cuando un tag entra a una zona de lectura, que puede ser radial (a diferencia de los lectores de código de barras), su información es capturada por el lector y puede ser utilizada (Ver figura 2.26).

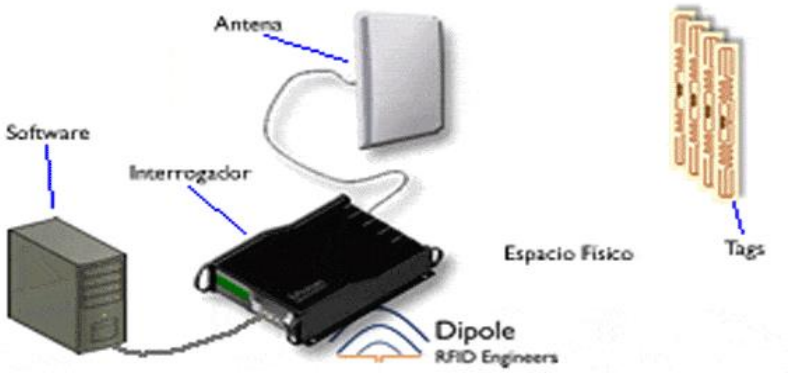


Figura 2.26: Tag RFID.
Fuente: http://www.gs1ve.org/.

4.2 TIPS DE TAGS

Existen "tags" activos y pasivos.

- **Los tags activos** tienen batería propia por lo que de forma activa pueden informar de su presencia o activar cambios en otros dispositivos. Las distancias de lectura en estos casos son mayores. La vida útil de una batería puede fluctuar entre los 5 y 7 años, y puede ser renovada.
- **Los tags pasivos** no tienen batería propia, y sólo informan de su presencia cuando son preguntados por el lector. A través de una antena, el microchip recibe la energía emitida por el lector, con lo que puede enviar y recibir información.

En la Empresa CVG BAUXILUM, su principal método de identificación, es utilizando el sistema de tarjetas de proximidad o tags, utilizando específicamente las del formato HID ProxCard II cuya frecuencia de uso es de 125khz, emite un código de identificación único y los lectores o readers de la marca HID cuyo modelo son ProxPro 5355, ProxPro II 5455 y MiniProx 5365.

4.3 ESTÁNDARES DE CODIFICACIÓN

El código electrónico de producto o EPC por sus siglas en inglés es la evolución del código de barras ya que utiliza la tecnología RFID para identificar de manera única a los productos en sus distintas unidades de empaque, pieza, caja y tarima (item, case y pallet) agregando un número de serie a la información sobre su tipo y fabricante. Los códigos electrónicos de producto son administrados a nivel mundial por EPCglobal, filial de GS1.

Figura 2.27: Código electrónico de identificación RFID.
Fuente: http://www.gs1ve.org/.

La red EPC Network, al igual que un código de barras, el EPC de 96 bits utiliza una cadena de números para identificar al fabricante de un artículo y su categoría de producto. El EPC añade un tercer grupo de dígitos, que es un número de serie exclusivo para cada artículo. Este número es todo lo que se almacena en el microchip de la etiqueta RFID, pero el EPC se puede asociar con una gran cantidad de información en una base de datos, creando así unas posibilidades de explotación gigantescas. Por ejemplo, el lugar y la fecha de fabricación del producto, su fecha de caducidad, el lugar al que se debe enviar,

etc. Además, la información se puede actualizar en tiempo real para seguir los movimientos o los cambios del artículo.

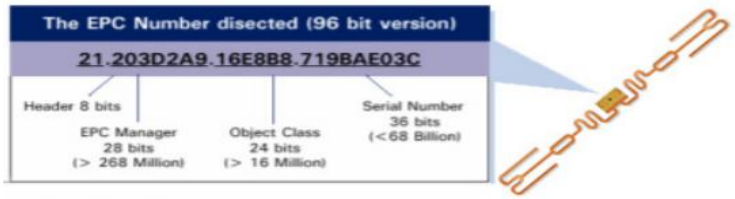


Figura 2.28: Código EPC con tecnología RFID.
Fuente: Auto-ID Center.

4.4 APLICACIONES

- **Control de acceso:** Sistemas de alta seguridad con registro de actividades almacenado en un sistema de información local o en los mismos transponders. Ideal para instituciones como escuelas, instalaciones de seguridad o empresas en general.
- **Identificación vehicular:** Sistemas de identificación automática de vehículos para casetas de cobro y control vehicular con tags pasivos y activos.
- **Manufactura y control de procesos:** La tecnología RFID aplicada a procesos de manufactura, permite obtener trazabilidad y control de producción en proceso WIP (Work In Process) en distintos tipos de industria.
- **Control de activos:** Identifique y mantenga un control eficiente de los inventarios de computadoras, maquinaria y otras piezas de activo fijo como vehículos y equipo portátil mediante tecnología RFID.
- **Autentificación de medicamentos:** EEUU y las dependencias del sector salud en América Latina requieren de mayores controles para asegurar el abasto y custodia de la cadena de suministro de medicamentos y combatir la falsificación. Con ello

se requiere codificar el producto desde su fabricación a fin de insertar un tag de RFID que permita darle trazabilidad al mismo.

4.5 VENTAJAS.

- Lecturas más rápidas y más precisas.
- Tarjetas (Tags) personalizadas.
- Seguimiento del personal o producto.
- Altos estándares de seguridad y cifrado, depende del modelo de tarjeta.

4.6 DESVENTAJAS.

- Altos Costos.
- Se pueden extraviar.
- Intercambiable.
- Se pueden clonar sin la necesidad de hacer contacto.
- No son resistentes.

5. SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO.

Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas. Las características básicas que un sistema biométrico para identificación personal debe cumplir son: desempeño, aceptabilidad y fiabilidad. Las cuales apuntan a la obtención de un sistema biométrico con utilidad práctica.

5.1 HISTORIA Y TIPOS DE BIOMETRÍA

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos físicos

intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

La biometría, una de las diez tecnologías emergentes según un estudio (2001) del Massachussets Institute of Technology (MIT), es una ciencia que emplea métodos de identificación no tradicionales como la impresión de huella dactilar, la biometría dinámica de firma, la geometría del rostro o de la mano, el iris, la retina, así como el tipo de sangre y de ADN. En la actualidad debido a su sencilla implementación y bajo costo/beneficio, la biometría de huella dactilar es el método más utilizado y conocido; se emplean programas de lectura de huellas digitales, controles de asistencia utilizando el control biométrico o programas de control de ausentismo por lectura biométrica, estos sistemas son aquellos que utilizando lectores de huellas digitales integrados a una red de computadoras o bien lectores autónomos de huellas dactilares permiten verificar el ingreso, salida, ausentismo y otras situaciones relacionadas con el control de personal.

Los principios en los que se basa están relacionados con la traducción de la información contenida en la huella digital (utilizan un mapa de puntos clave de una huella dactilar) a algoritmos únicos y personales que se emplean para identificar al usuario y relacionar esta información con sus datos personales. Estos sistemas de lectura de huellas digitales por biometría utilizan menos de un segundo para captar e identificar al poseedor de la impresión dactilar.

5.2 MÉTODOS DE IDENTIFICACIÓN BIOMÉTRICA

Existen diferentes métodos de identificación y autenticación de los seres humanos a través de características fisiológicas y de comportamiento los cuales pueden dividirse en:

- **Fisiológicos**: Geometría de la mano, iris, retina, reconocimiento facial, huella digital
- **Comportamiento**: Firma, voz, dinámica de teclado

5.2.1. IDENTIFICACIÓN POR HUELLAS DACTILARES

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones.

Las salientes se denominan crestas papilares y las depresiones surcos inter papilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

5.2.2. CLASIFICACIÓN

Los patrones de huellas digitales están divididos en 4 tipos principales (Ver figura 2.29), todos ellos matemáticamente detectables. Esta clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente.

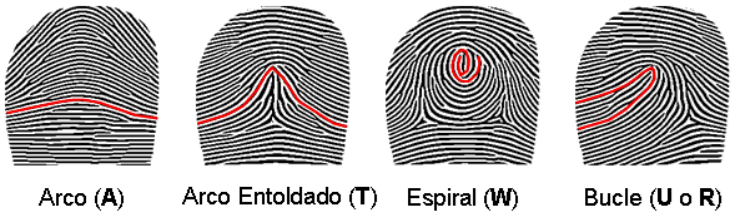


Figura 2.29: Patrones de huellas digitales.

Fuente: http://www.biometria.gov.ar/.

En la figura 2.30 aparecen 7 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 (por ejemplo 10 horquillas, 12 empalmes, 15 islotes, etc.). A estos puntos también se llaman minucias, término utilizado en la medicina forense que significa “punto característico”.

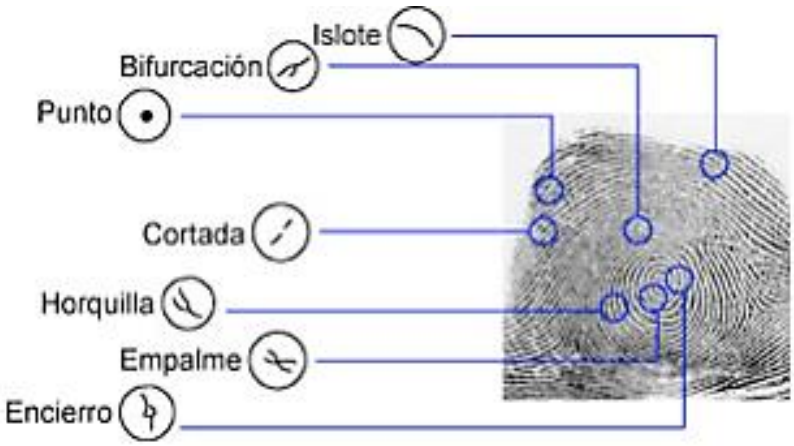


Figura 2.30: Características de la Huella Digital.

Fuente: http://www.biometria.gov.ar/.

5.2.3. PROCEDIMIENTO

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, según se muestra en la siguiente

figura, el mismo se almacena en una base de datos, con la debida referencia de la persona que ha sido objeto del estudio.

Para ello, la ubicación de cada punto característico o minucia se representa mediante una combinación de coordenadas (x, y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible.

Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes.

			
El dedo es leído por un lector de huellas.	El dedo es codificado.	Una plantilla matemática es generada.	El lector guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Figura 2.31: Procedimiento de lectura de la Huella digital.

Fuente: http://www.biometria.gov.ar/.

5.2.4. DISPOSITIVO PARA IDENTIFICACIÓN

El Sistema de Identificación Automatizada de Huellas Dactilares, tiene un índice de seguridad del 99.9% ya que verifica la identidad de una persona, basada en las características de sus huellas digitales.

Para tratar los datos de la huella se utiliza un algoritmo que permite asociar la huella que se desea identificar, con otras de similares características, almacenadas en la base de datos.

Existen dos maneras distintas usar los datos de una huella.

- **VERIFICACIÓN ¿ES LA PERSONA QUIEN DICE SER?**

Se suele pedir un código, una lectura de tarjeta y comparar esa huella almacenada con la huella puesta en el lector, la verificación es un proceso un poco más molesto porque se le pide una información o una acción adicional al usuario, pero como ventaja tiene que es más rápido y más seguro.

- **IDENTIFICACIÓN. ¿QUIÉN ES LA PERSONA?**

En este proceso directamente se compara una huella capturada contra todas las que están almacenadas en el ordenador, es un proceso algo más lento, pero la interacción con el usuario es mínima.

Es importante remarcar que la mayoría de los lectores dactilares, no guardan la imagen de la huella, solo almacenan los datos matemáticos explicados anteriormente.

5.2.5. TIPOS DE SENSORES

En el mercado actual existen muchos tipos de sensores biométricos, lectores capaces de convertir una huella en una imagen procesable por un algoritmo.

Existen diversos tipos, la mayoría experimentales y nunca han llegado realmente al mercado, los que se puede encontrar se dividen en las siguientes categorías:

a) LECTORES ÓPTICOS

- **Ventajas**: Bajo costo, rapidez de captura, resolución de la imagen, velocidad.
- **Desventajas**: Dependiendo del modelo se utiliza en interiores debido a la luz solar, modelos más avanzados solucionan este problema.

b) LECTORES CAPACITIVOS

- **Ventajas**: Reducido tamaño ideal para dispositivo de uso personal, móviles, etc.
- **Desventajas**: Muy sensibles a la humedad, poca calidad de imagen.

c) LECTORES TÉRMICOS

- **Ventajas**: Tamaño pequeño, uso en exteriores, dispositivos personales.
- **Desventajas**: sensibles a la temperatura, dificultad de uso, necesita un cierto aprendizaje.

d) LECTORES ULTRASONIDOS

- **Ventajas**: No requiere de contacto, mucha seguridad.
- **Desventajas**: Precio alto, tamaño, requiere mantenimiento continuo.

5.3 RECONOCIMIENTO FACIAL.

El reconocimiento facial es una tecnología con mucho futuro, en la actualidad no está muy extendida, puesto que requiere de unas condiciones muy concretas, sobre todo de luz, además suele requerir cámaras de un coste bastante alto. La seguridad en la actualidad es alta, porque incorpora dos cámaras (una infrarroja y una cámara estándar, ver figura 2.32) utilizando técnicas de 3D con el objetivo de evitar falsos positivos o fraudes a la hora del acceso, por los momentos la tecnología se encuentra en una temprana etapa de desarrollo.

Figura 2.32: Lector Facial para control de Acceso FaceStation.
Fuente: Suprema Inc.

5.4 RECONOCIMIENTO POR VOZ.

Similar al reconocimiento facial, no es suficientemente seguro como sistema biométrico, pero puede ayudar a otros sistemas.

El Reconocimiento Automático del Habla (RAH) o Reconocimiento Automático de voz es una parte de la Inteligencia Artificial que tiene como objetivo permitir la comunicación hablada entre seres humanos y computadoras electrónicas.

El problema que se plantea en un sistema de RAH es el de hacer cooperar un conjunto de informaciones que provienen de diversas fuentes de conocimiento (acústica, fonética, fonológica, léxica, sintáctica, semántica y pragmática), en presencia de ambigüedades, incertidumbres y errores inevitables para llegar a obtener una interpretación aceptable del mensaje acústico recibido.

5.2.6. USOS Y APLICACIONES

Aunque en teoría cualquier tarea en la que se interactúe con una computadora puede utilizar el reconocimiento de voz, actualmente las siguientes aplicaciones son las más comunes:

- **Dictado automático**: El dictado automático es, en el 2007, el uso más común de las tecnologías de reconocimiento de voz. En algunos casos, como en el dictado de recetas médicas y diagnósticos o el dictado de textos legales, se usan corpus especiales para incrementar la precisión del sistema.
- **Control por comandos**: Los sistemas de reconocimiento de habla diseñados para dar órdenes a un computador ("Abrir Google Chrome", "cerrar ventana") se llaman Control por comandos. Estos sistemas reconocen un vocabulario muy reducido, lo que incrementa su rendimiento.
- **Telefonía**: Algunos sistemas PBX permiten a los usuarios ejecutar comandos mediante el habla, en lugar de pulsar tonos. En muchos casos se pide al usuario que diga un número para navegar un menú.
- **Sistemas portátiles**: Los sistemas portátiles de pequeño tamaño, como los relojes o los teléfonos móviles, tienen unas restricciones muy concretas de tamaño y forma, así que el habla

es una solución natural para introducir datos en estos dispositivos.

- **Sistemas diseñados para discapacitados**: Los sistemas de reconocimiento de voz pueden ser útiles para personas con discapacidades que les impidan teclear con fluidez, así como para personas con problemas auditivos, que pueden usarlos para obtener texto escrito a partir de habla. Esto permitiría, por ejemplo, que los aquejados de sordera pudieran recibir llamadas telefónicas.

5.5 ESCÁNER DE IRIS O ESCÁNER DE RETINA.

Tecnología altamente segura, pero hoy en día una tecnología bastante cara, solo para sitios de muy alta seguridad, los usuarios son reticentes a poner el ojo cerca de una cámara que es totalmente inocua, sin embargo algunas cámaras necesitan luz roja que puede ser visible o invisible (Infrarroja) en el caso de la luz visible el usuario siente que es una acción intrusiva y prefiere no exponerse.

Hay dos formas de escanear los ojos. Un escáner de retina mide el patrón de venas en el fondo del ojo, que se obtiene proyectando una luz infrarroja a través de la pupila.

Figura 2.33: Retina.

Fuente: http://www.hertasecurity.com/.

El escáner de iris se realiza utilizando una videocámara y examinando los patrones de color únicos de los surcos de la parte coloreada de nuestros ojos. Los escáneres de iris están empezando a utilizarse en la seguridad de los aeropuertos, control de asistencia, oficinas, etc.

Figura 2.34: Iris.
Fuente: http://www.hertasecurity.com/.

Los escáneres de retina son bastante invasivos y menos habituales, pero se siguen utilizando para restringir el acceso a instalaciones militares, laboratorios de investigación y otras áreas de alta seguridad.

CAPÍTULO III

DISEÑO METODOLÓGICO

En el siguiente capítulo se presentaran los lineamientos metodológicos relacionados con el tipo de estudio y diseño de la investigación, así como también la técnica de recolección de datos, el cual representa la guía para obtener la información necesaria, para el tratamiento de la información y los procedimientos para el análisis, serán documentales, debido a que esta investigación se fundamentara con autores y leyes relacionadas a este estudio, por último se presentara el procedimiento haciendo énfasis en el análisis de los datos que fueron analizados para el desarrollo de la investigación.

DISEÑO Y TIPO DE ESTUDIO

El estudio se desarrollara bajo la aplicación de una investigación con diseño no experimental, del tipo Descriptivo, Campo, Evaluativo y Aplicado.

- **INVESTIGACIÓN DE DISEÑO NO EXPERIMENTAL:** Debido a que se identifican los problemas y debilidades sin alterar ninguna de las variables presente en los procesos, estos solo se analizan.

Como señala Kerlinger (1979, p. 116).

> *"La investigación no experimental o expost-facto es cualquier investigación en la que resulta imposible manipular variables o asignar aleatoriamente a los sujetos o a las condiciones".*

Esto quiere decir, la investigación No Experimental es observar fenómenos tal y como se dan en su contexto natural, para después estudiarlos, en este caso, será analizar el escenario utilizados como control de acceso que tendrá el personal contratista al ingresar a la empresa.

- **TIPO DESCRIPTIVA:** Se procuró conocer la situación y su entorno, para tener una idea clara y objetiva de las características de la situación actual que presenta la División.

Describe Tamayo y Tamayo (2001).

> *"Corresponde a la descripción, registro, análisis e interpretación de la naturaleza actual de los fenómenos. El enfoque se hace sobre como una persona, grupo o cosa funciona en el presente" (pág. 46).*

Esta investigación se basa en una formulación de tipo descriptiva, debido a que determina cual es la situación actual, describiendo, analizando e interpretando las condiciones actuales en las cuales se realizan los diferentes modelos de control de acceso, con el fin de identificar los aspectos e impactos que se puedan estar generando y buscar posibles soluciones, que mejore la seguridad y reduzca los costos que generan las tarjetas de identificación y los pases a planta en la Empresa CVG Bauxilum.

- **TIPO CAMPO:** Se realiza un análisis sistemático de los problemas que afectan a la División Identificación y Control, Gerencia Seguridad Patrimonial y a la Empresa BAUXILUM, con el propósito bien sea de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus causas y efectos, o predecir su ocurrencia, haciendo uso de métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo.

Según los autores Santa Palella y Feliberto Martins (2010), define:

> *"La Investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta. (Pág. 88)"*

Es decir, los datos de interés son recogidos en forma directa de la realidad, en este caso, las autorizaciones suministrados a los contratistas y el procedimiento que utilizan para el proceso de verificación; en este sentido, se trata se realiza investigaciones a partir de datos que son suministrado mediante la recolección para su posterior análisis mediante procedimientos estadísticos, modelos matemáticos, econométricos o de otro tipo.

- **TIPO EVALUATIVA:** La investigación evaluativa permitió en esta investigación, indagar en todos los aspectos referidos al diseño del sistema automatizado y realizar una medición del impacto que tendrá en la población para adaptarse a la nueva tecnología, tomando en consideración la opinión del personal de la Gerencia Seguridad Patrimonial.

El autor Weiss (1980), indican:

> *"Medir los efectos de un programa por comparación con las metas que se propuso alcanzar, a fin de contribuir a la toma de decisiones subsiguientes acerca del programa y para mejorar la programación futura. (Pág. 17)".*

Esto quiere decir, ayuda a la contribución de toma de decisiones y al mejoramiento de la programación, además de que hace más preciso y objetivo el proceso de juzgar, da criterios claros y específicos para el éxito. Reúne pruebas y testimonios de muestras representativas de la población a la cual se hace referencia. Por lo general, se traduce las pruebas y testimonios en números reales y los compara con criterios que se habían establecido. Al final saca conclusiones acerca del éxito y la eficacia de lo que se está estudiando.

- **TIPO APLICADA:** Concentra su atención en las posibilidades reales de llevar a la práctica las teorías generales, y destina sus esfuerzos a resolver los problemas y necesidades que se plantean los hombres en sociedad en un corto, mediano o largo plazo.

Según Pedro Venegas (2006).

> *"La investigación aplicada es también conocida como investigación práctica, se realiza con fines prácticos, tanto para resolver un problema, como para tomar decisiones, evaluar programas y general para mejorar un producto o proceso"*

La investigación se considera aplicada porque permitirá obtener los elementos indispensables para la elaboración, dar respuesta efectiva y fundamentada al problema detectado con el anterior sistema de control de acceso. Además, destina sus esfuerzos a resolver los problemas y necesidades que se plantean en un corto, mediano o largo plazo.

- **REVISIÓN DE DOCUMENTOS:** Esta técnica se utilizará con la finalidad de recoger toda la documentación disponible y necesaria para el desarrollo del proyecto. De esta manera, se recopilo toda la información requerida para la evaluación de los procesos administrativos de la División Identificación y Control a través de informes de pasantías y tesis que se encuentran en el SDI, internet, prácticas administrativas, entre otros documento de contenido informativo.

Según Arias (2006),

> *"La revisión documental consiste en una recopilación de ideas, posturas de autores,*

conceptos y definiciones, que sirven de base a la investigación".

- **Reunión con Tutor Industrial y Jefe de División de la Unidad Control de Acceso:** Establecido los métodos alternativos para el control de acceso, se procedió a realizar una reunión para establecer las necesidades, carencias, mejoras y alternativas para el diseño del nuevo sistema y estudiar el impacto que generaría a la gerencia.

POBLACIÓN

Para la obtención de información o datos que permitieron la evaluación del estado actual del objeto de estudio de la presente investigación, se consideró una población de 10 dispositivos de control de acceso automatizado.

MUESTRA

Se utilizó como muestra los dispositivos de control de acceso biométricos utilizando el sistema de huellas dactilares, por ser una tecnología de alta tasa de aceptación por los usuarios, tener costos accesibles, tener una facilidad de uso y una alta seguridad para la empresa.

INSTRUMENTOS

Durante las pruebas que se realizarán para determinar, se utilizaran los siguientes materiales y equipos:

- **Tarjeta RFID:** Marca HID Proximity, utilizado en la actualidad por el personal fijo impreso con sus datos personales y fotos, y los pasantes sin imprimir
- **Lectora de Tarjeta RFID:** Marca HID Proximity, utilizadas en la manga de identificación (molinetes), portón de acceso, puertas de edificios, entre otros puntos de acceso de riesgos establecido por el S.I.S.P
- **Tarjeta PVC:** Tarjeta que se utilizara en modo de prueba para impresión de código de barras y/o código bidimensional QR.
- **Generador de Código de Barra y/o QR:** Se utilizara un generador de código de barra open source para la generación de códigos de barra y/o QR.
- **Lector Código de Barra y/o Código Bidimensional QR:** Método alternativo para el control de acceso que consta de un lector óptico o laser para hacer las lecturas de las tarjetas ya impresas.
- **Lectores Biométricos de Huellas Dactilares:** Método alternativo para utilizar en el control de acceso a la empresa, que consta de un lector biométrico de huellas dactilares con soporte simultaneo de tarjetas RFID compatible con las tarjetas HID ProxCard II, certificado con la norma IP-68 (Ingress Protection; 6= Protección fuerte contra polvo; 8=Inmersión completa y continua en agua).
- **Software de Control de Acceso:** Software centralizado, basado en interfaz web y estará compuesto por con la base de datos el personal contratista, pasante y visitante basado en MySQL, este equipo estará bajo un servidor paralelo al servidor Lenel.
- **Equipos Clientes:** 2 Workstation ubicados en el módulo de identificación, contaran con 2 lectores biométricos y con el acceso al software para el proceso de registro y verificación del personal.

- **Cronómetro:** Utilizado para medir el tiempo que se genera con el actual sistema desde el momento que se realiza el pase para el personal hasta el momento que logra ingresar a la planta, y utilizado para medir con los sistemas alternativos (código de barra y biométricos).
- **Software Microsoft Office 2013:** Se utilizó la suite ofimática para realizar este trabajo, utilizando como procesador de datos la aplicación Microsoft Word; Hojas de Cálculo la aplicación Excel; Microsoft PowerPoint para el diseño de las diapositivas; Microsoft Project para la planificación, control del proyecto y el cronograma de actividades y Microsoft Visio, utilizado para diseñar los diagramas utilizados en el presente trabajo.
- **Intranet (Tramen, Bucare-SDI):** Servidor http-ftp donde se almacenan los manuales de procedimientos, instructivos y diversos documentos de la empresa.
- **Laptop:** Equipo portátil con procesador Intel Core i7 a 2.8ghz, memoria RAM 8Gb, con Sistema Operativo Microsoft Windows 10, con suite Ofimática Microsoft Office 2013, Microsoft Project 2013, Microsoft Visio 2013 y Software Arena.
- **Computador:** Computadora de escritorio Pentium 4 a 2.0ghz, memoria RAM 768mb, con sistema operativo Windows XP, suite ofimática Microsoft Office 2003, Microsoft Project 2003, sin software de retro compatibilidad de para archivos Microsoft Office 2007 a 2003 y no permite el acceso para utilizar pendrive ni disco duro portátil.
- **Impresora Samsung ML-2165.**
- **Hojas.**

PROCEDIMIENTO METODOLÓGICO

- **Diagnosticar el actual proceso de identificación utilizado en el control de acceso de contratistas.**

    - Revisión de los Antecedentes del Proyecto de Identificación ya establecido para el personal fijo (Sistema RFID)
    - Realizar entrevistas no estructuradas a los Analistas de Identificación y al personal.
    - Establecer mediantes diagramas de procesos, la series de pasos que debe efectuar el personal contratista a la hora de ingresar a la empresa
    - Indagar y realizar un Diagrama de Ishikawa con el fin de identificar cuáles son las posibles causas y cuál es su efectos que impiden la expansión de la tecnología RFID ya implementada en la empresa
    - Investigar las diferentes tecnologías de identificación y control de acceso disponibles en el mercado.

- **Investigar las diferentes tecnologías de identificación y control de acceso disponibles en el mercado.**

    - Investigar los dispositivos de Control de Acceso que sean compatibles con las instalaciones existentes.
    - Revisión de los diferentes proveedores en la zona.
    - Comprobar la capacidad de expansión tecnológica que cuenta la actual infraestructura.

- **Realizar estudios de Factibilidad Técnica** de las diferentes tecnologías que existen en el mercado Venezolano, evaluando sus especificaciones técnicas procurando de que sea compatible con la infraestructura ya implementada en la Empresa.
- **Desarrollar estudios de Factibilidad Operativa** con el fin de evaluar cuál será el impacto que tendrá dicho sistema, indicando que no debe

representar peligro alguno para los usuarios por lo cual deberá ser un sistema de fácil uso y que inspire confianza a los usuarios finales.

- **Elaborar el estudio de Factibilidad Económica** mediante el uso de análisis de costos/beneficio, todos los costos y beneficios de adquirir y operar cada sistema alternativo, identificando y realizando una comparación de ellos.

CAPÍTULO IV

SITUACIÓN ACTUAL

Se lleva a cabo una descripción detallada de la situación actual de la Empresa CVG Bauxilum C.A. a través de la realización de una descripción minuciosa del actual proceso de identificación utilizado en el control de acceso de contratistas, diagramas de procesos y diagramas de causa-efecto los cuales permiten evaluar de forma concreta el problema existente.

ACTUAL PROCESO DE IDENTIFICACIÓN UTILIZADO EN EL CONTROL DE ACCESO DE CONTRATISTAS.

El Sistema Integrado de Seguridad Patrimonial (S.I.S.P.), surge como le resultado del estudio de seguridad y análisis de riesgo realizado por especialistas de la Unidad de Protección Industrial de C.V.G. Bauxilum Matanzas y Los Pijiguaos, en el que se identificaron y evaluaron las amenazas y debilidades que afectan la gestión de Protección Patrimonial. Este proyecto de ingeniería ha sido concebido bajo una visión holística.

ANÁLISIS FODA

El análisis de Fortalezas, Oportunidades, Debilidades y Amenazas (FODA), si bien no permite directamente la toma de decisiones, sí puede servir de orientación para estudiar la problemática actual en la empresa en el sentido de proporcionar una presentación sintética de los factores positivos y negativos

del sistema manual utilizado por el personal contratista y el sistema RFID utilizado en el personal fijo, con objeto de proporcionar una visión panorámica que permita tener una primera idea acerca de la conveniencia de acometer su realización.

A continuación, se realiza un análisis FODA sobre el actual sistema manual utilizado para el control de acceso del personal contratista a la empresa.

- **FORTALEZAS.**
  - Sistema económico frente al sistema automatizado RFID ya implantado.
- **OPORTUNIDADES.**
  - Disponibilidad de nuevas tecnologías.
  - Personal y equipos apto para incorporar nuevas tecnología.
- **DEBILIDADES.**
  - Error al crear los pases diarios al personal.
  - Falta de equipos automatizados.
  - Servicio lento y deficiente.
  - No utiliza el sistema automatizado RFID ya implementado.
- **AMENAZAS.**
  - Acceso del personal a áreas no autorizadas.
  - No se realiza seguimiento al contratista.
  - No hay control de hora de ingreso, estadía y salida de planta.
  - Dificultad para acceder a los expedientes.

Se puede apreciar, el actual sistema tiene un alto margen de debilidades y amenazas para la empresa, por utilizar un sistema obsoleto y vulnerable.

Se procede a realizar un análisis FODA sobre el actual sistema automatizado RFID utilizado para el control de acceso del personal fijo a la empresa.

- **FORTALEZAS.**
  - No se necesita contacto directo ni visual del tag con el lector.
  - Actualización de datos en línea.
  - Control de hora exacta de ingreso, estadía y salida de planta.
  - Control de acceso personal en múltiples puntos.
- **OPORTUNIDADES.**
  - Disponibilidad de nuevas tecnologías.
  - Personal y equipos apto para incorporar nuevas tecnología.
- **DEBILIDADES.**
  - Altos costos de las Tarjetas (Tags) RFID HID.
  - Tiempo de vida útil de la tarjeta RFID.
  - No es compatible con otro formato de tarjeta, bien sea EM, MiFare.
  - Servidor limitado por licencias.
  - Falta de actualización con la tecnología
  - Servidor con licencia obsoleta
- **AMENAZAS.**
  - Magnetismo de ciertas áreas de la empresa dañan las tarjetas.

- Trafico no cifrado en la red de datos
- Cortes de energía eléctrica.

En este análisis, el actual sistema automatizado de tarjetas RFID tiene un alto margen de debilidades debido a la obsolescencia de los equipos utilizados, altos costos de las tarjetas (tags) y amenazas para la empresa como el tráfico no encriptado de datos hasta los cortes de energía eléctrica en el servidor.

Para el proceso actual se tiene que le personal contratista llega al portón 1, donde espera 8 minutos donde realiza una cola, se desplaza 6 metros hasta llegar a la taquilla de identificación, posteriormente saluda al analista y le entrega su cedula de identidad laminada y su autorización de acceso a la empresa vencida, espera 1 minuto mientras el analista realiza una nueva autorización de acceso, posteriormente la recibe, verifica que sus datos estén correctos, se traslada 4 metros hacia los molinetes de acceso, luego pasa al área de acceso y se desplaza 3 metros hacia el vigilante, le entrega la cedula de identidad y la autorización de acceso, espera 1 minuto mientras el vigilante valida los datos y por ultimo ingresa a la empresa.

DIAGRAMA DE PROCESOS

Diagrama: De proceso.

Proceso: Identificación y control de acceso al personal contratista a la empresa CVG Bauxilum.

Inicio: Llega al portón 1.

Fin: Pasa a la empresa.

Fecha: 09/10/2015.

Método: Actual.

Seguimiento: Al personal contratista.

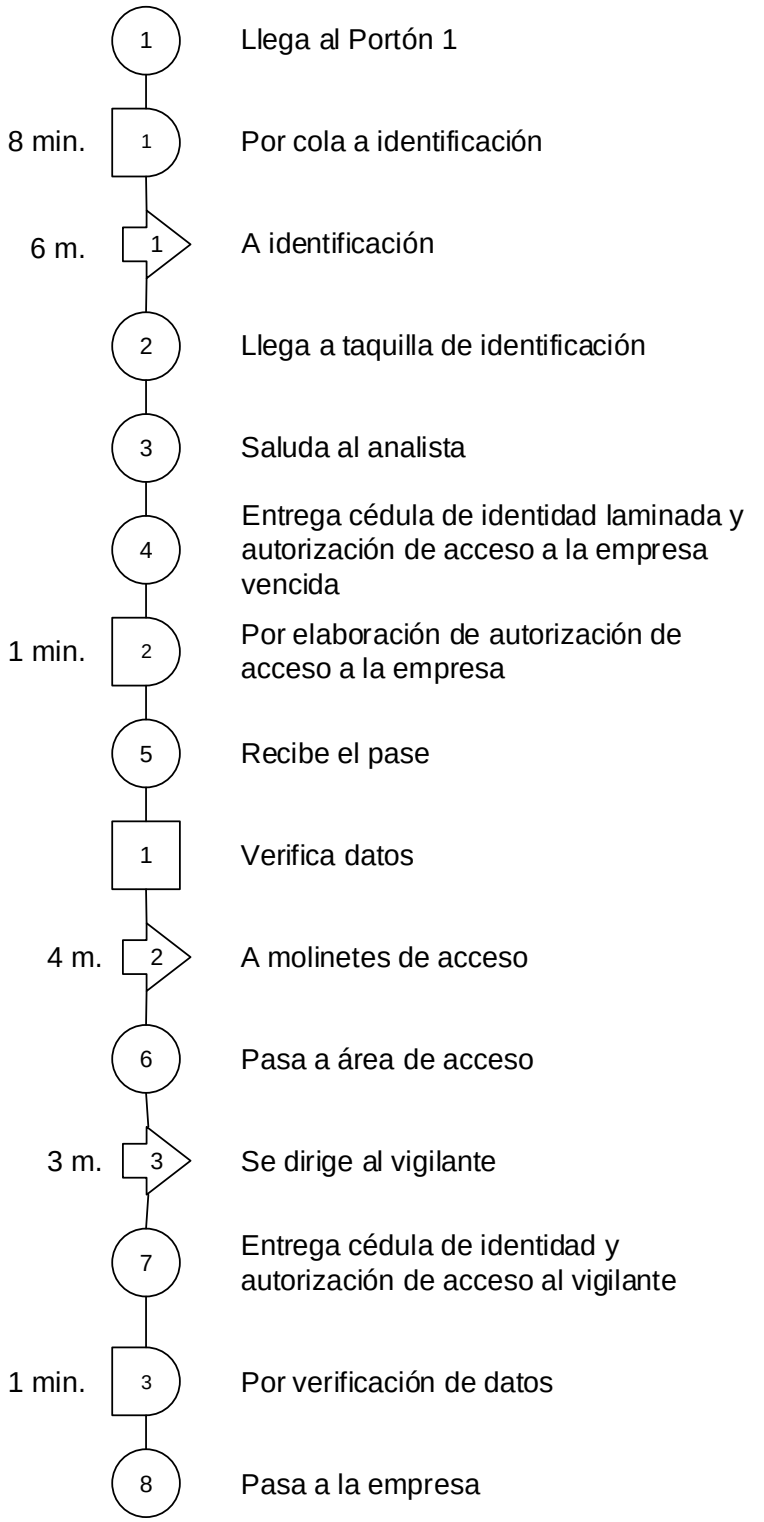
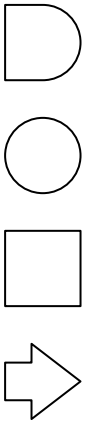


Figura 4.1: Diagrama de proceso del personal contratista

Fuente: Autor.

Resumen:



._ 3 (8min. + 1min. + 1min.) = 10 min.

._ 8

._ 1

._ 3 (6m. + 4m. + 3m.) = 13m.

Total : 15

Figura 4.2: Resumen de diagrama de proceso del personal contratista
Fuente: Autor

Según los resultados obtenidos se puede evidenciar en el diagrama de procesos que el personal contratista demora aproximadamente 10 minutos en acceder a la empresa, y se debe trasladar aproximadamente 13 metros, medidas que se podrían reducir considerándose innecesarias, pudiendo decir que es un proceso engorroso para algo tan sencillo como la identificación y el acceso del personal contratista a la empresa.

Posteriormente se estudió la situación actual del proceso de identificación y acceso del personal fijo y contratado, se tiene que el empleado llega al portón 1, se desplaza 4 metros hacia los molinetes de acceso, marca la ficha o tarjeta RFID, espera 2 segundos mientras el sistema lo identifica y por último le da acceso a la empresa.

Diagrama: De proceso.

Proceso: Identificación y control de acceso al personal fijo y contratado a la empresa CVG Bauxilum.

Inicio: Llega al portón 1.

Fin: Pasa a la empresa.

Fecha: 09/10/2015.

Método: Actual.

Seguimiento: Al personal fijo y contratado.

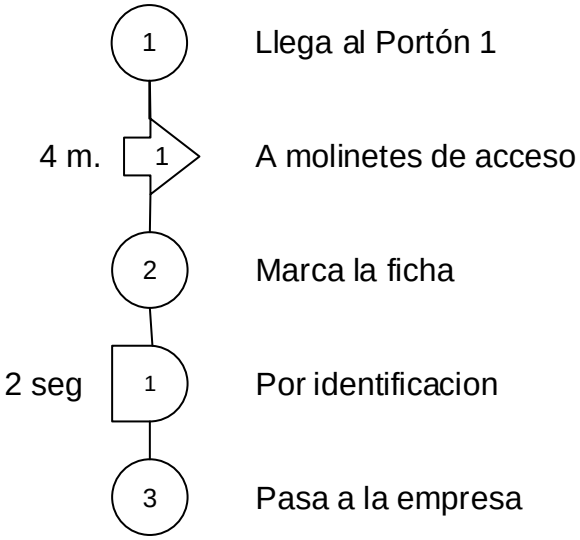
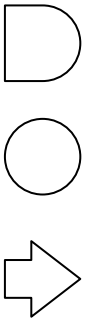


Figura 4.3: Resumen de diagrama de proceso del personal fijo y contratado.

Fuente: Autor

Resumen:



._ 1 (2seg.)

._ 3

._ 1 (4m.)

Total : 5

Figura 4.4: Resumen de diagrama de proceso del personal fijo y contratado.
Fuente: Autor

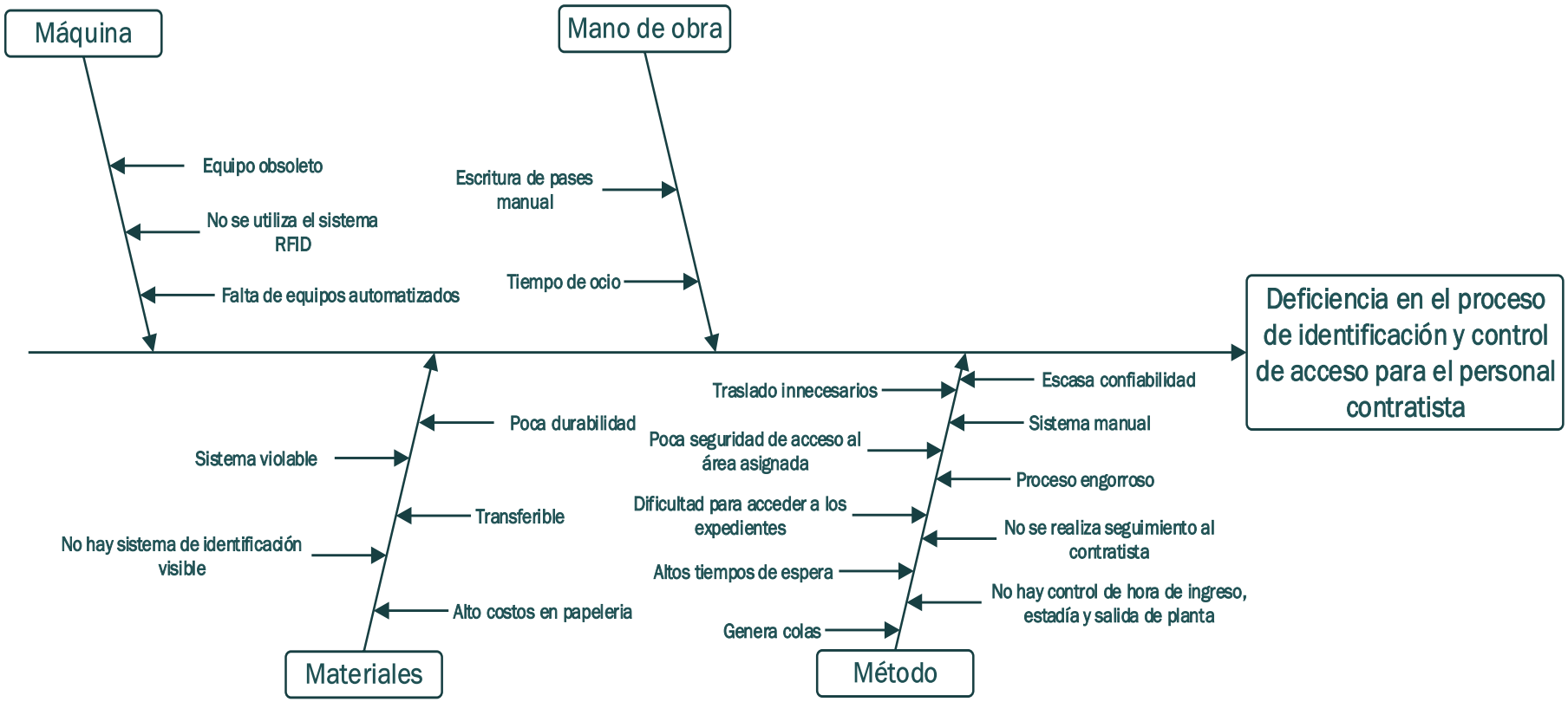
En cuanto a la identificación y control de acceso para el personal fijo y contratado es más eficiente en cuanto al tiempo de demoras y traslados innecesarios, sin embargo es un sistema altamente costoso, por lo que se estudió la factibilidad de implementar un sistema equivalente que genere menos gastos.

DIAGRAMA CAUSA-EFECTO

Para efectos del estudio se decidió organizar las diferentes teorías propuestas sobre la causa del problema central con el fin de organizar y mostrar gráficamente según el método de las 6M cuáles son las áreas o subcampos con mayor incidencia en la identificación y acceso del personal contratista a la planta CVG Bauxilum C.A. operadora Matanzas.

Para esto se realizó un diagrama causa-efecto donde se evaluaron todas las causas que conllevan al problema actual en cuanto al sistema de identificación y control de acceso del personal contratista, mediante un estudio basado en la recopilación de datos y observación directa se determinó que los problemas más relevantes en la actualidad son los siguientes:

- Es un sistema manual
- Posee elevados costos de papelería
- Genera altos tiempos de espera
- Produce largas colas
- Ocasiona traslados innecesarios
- Es un proceso engorroso
- Genera dificultad para acceder a los expedientes de cada trabajador contratista.
- Otorga tiempo de ocio a los contratistas.
- Existe poca seguridad de acceso al área asignada.
- No se realiza un seguimiento al contratista, es decir, se desconoce su ubicación exacta en la planta luego de acceder a la misma.
- Escasa confiabilidad.
- Sistema violable.
- Permiso transferible.
- Poca durabilidad.
- Maquinaria obsoleta.
- La maquinaria implementada no marca la hora de entrada ni de salida de planta.
- No hay control de hora de ingreso, estadía y salida de planta.
- Falta de equipos automatizado.
- No se utiliza el sistema RFID.



Gráfica 1: Diagrama de Ishikawa, deficiencia del proceso de acceso al personal contratista

Fuente: Autor

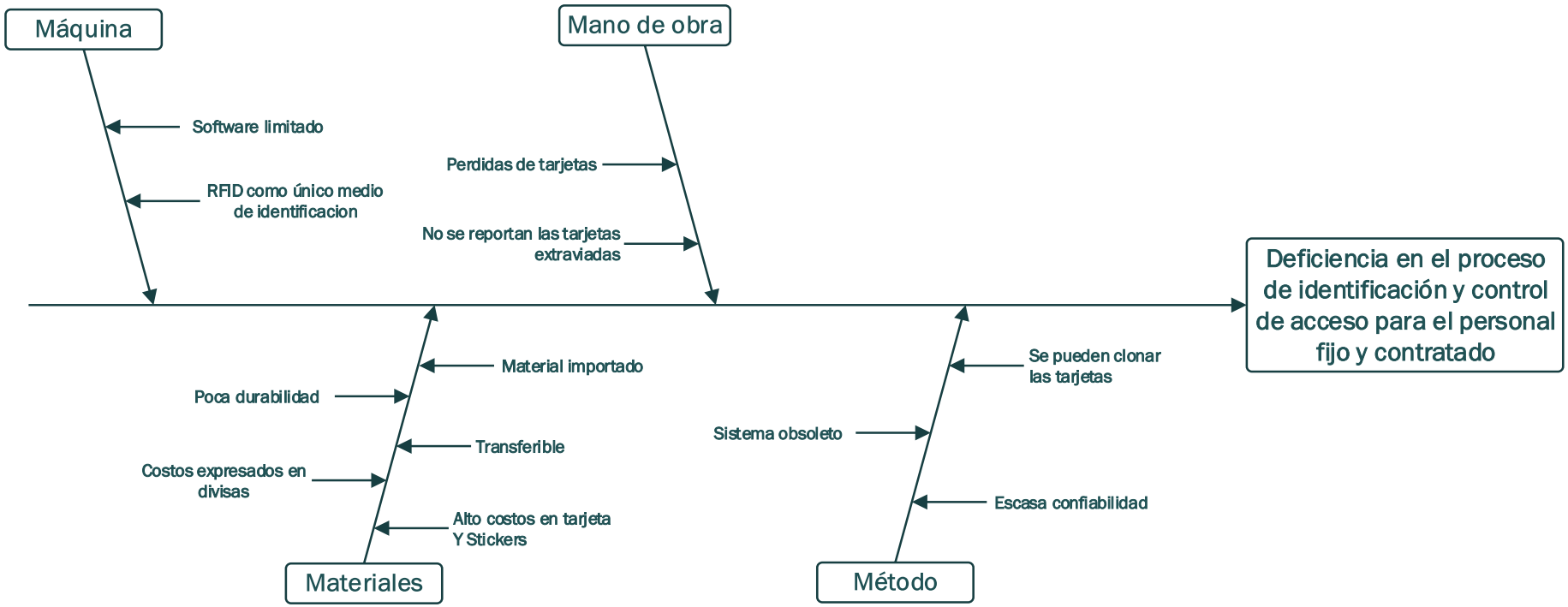
Posteriormente al realizar un análisis apoyado en un diagrama causa-efecto se determinó que los factores que tienen mayor incidencia en la deficiencia del proceso de identificación y control de acceso para el personal contratista se debe al método empleado actualmente por la empresa por lo cual se recomienda sustituirlo por un método más eficaz.

Las normas y procedimientos establecidas para la identificación y acceso a la planta en la actualidad son violadas, es decir, el procedimiento de identificación y acceso usado para el personal contratista no es el establecido por la planta, ya que la norma archivada bajo el código 03.01.01 establece que el personal contratista, fijo, visitante y demás debe ser identificado para posteriormente acceder a planta de igual forma siguiendo el procedimiento actual que solo se emplea para el personal fijo, haciendo uso del carnet de identificación el cual contiene información relacionada a la Gerencia de adscripción, cargo actual, apellidos y nombres, número de personal, tipo de sangre, número de la cédula de identidad, foto actual, tipo de nómina y áreas permitidas.

La identificación y acceso del personal fijo se realiza de forma automatizada haciendo uso de tarjetas de proximidad RFID, se cree que no es el sistema más eficiente ya que al realizar un estudio se detectó que existen ciertos problemas que afectan el sistema actual, entre los cuales se pueden mencionar los siguientes:

- Las tarjetas RFID son transferibles
- Emplean un software limitado
- Es un sistema obsoleto
- Genera altos costos a la compañía
- Tarjetas poco resistentes

- Se pueden clonar sin la necesidad de hacer contacto, es decir, es un sistema violable
- Tarjeta RFID importada
- Arroja costos expresados en divisas
- Los trabajadores las pierden con frecuencia, es decir, se extravían con facilidad
- En caso de hurto los trabajadores no suelen reportar las tarjetas para que sean eliminadas del sistema
- Al ser transferible genera inseguridad en la planta
- RFID como único medio de identificación



Gráfica 2: Diagrama de Ishikawa, deficiencia del proceso de acceso al personal fijo y contratado.

Fuente: Autor

Al realizar un análisis haciendo uso de un diagrama causa-efecto se determinó que los factores que tienen mayor incidencia en la deficiencia del proceso de identificación y control de acceso para el personal fijo y contratado se deben a los materiales empleados para la fabricación de la tarjeta RFID, método empleado actualmente por la empresa se considera obsoleto por lo cual se recomienda sustituirlo por un método más eficaz como también se recomienda actualizar la maquinaria empleada y capacitar a los obreros para hacer un uso adecuado del nuevo método a implementar.

CAPÍTULO V

ANÁLISIS Y RESULTADOS

A continuación se presentan los resultados de la investigación.

8.1.1 SELECCIÓN DE LA TECNOLOGÍA

Un sistema biométrico es un sistema de reconocimiento en el que la identidad de un individuo es determinada a partir de algunas de sus características fisiológicas o de comportamiento. Se añade así un nuevo paradigma a la identificación personal, ya que la autenticación se realiza por medio de algo que la persona es, ya sea un rasgo fisiológico personal, en este caso, la huella dactilar.

Los métodos tradicionales de autenticación presentan el gran inconveniente de no poder discriminar de manera fiable entre los individuos legítimos y los individuos impostores, debido a que el método de identificación o bien sea tarjeta RFID o pase de acceso a la empresa que la persona tiene puede ser sustraída, pérdida, falsificada, clonada, etc. En cambio, los métodos basados en la autenticación de la entidad por medio de los rasgos biométricos de un individuo proporcionan una mayor fiabilidad en la identificación personal.

En la siguiente tabla se pueden apreciar las características de cada tecnología biométrica, donde se resaltó el impacto entre los usuarios, su funcionamiento y posibles incidencias en el mismo.

Tecnología	Huella dactilar	Geometría de la mano	Retina	Iris	Geometría Facial	Voz	Firma
Como Trabaja	Captura y compara patrones de la huella dactilar	Mide y compara dimensiones de la mano y dedos	Captura y compara los patrones de la retina	Captura y compara los patrones del iris	Captura y compara patrones los patrones faciales	Captura y compara las cadencia, pitch y tono de la voz	Captura y compara el ritmo, aceleración y presión de la firma
Tamaño de la plantilla (bytes)	250-1000	9	96	512	84-1300	10000-20000	1000-3000
Fiabilidad	Muy alta	Baja	Baja	Baja	Baja	Alta	Alta
Facilidad de uso	Alta	Alta	Baja	Baja	Baja	Media	Media
Posibles incidencias	Ausencia de miembro	Edad, ausencia de miembro	Lentes	Luz	Edad, Cabello, luz, densidad de vello facial	Ruido, temperatura y condiciones meteorológicas	Edad, enfermedad, analfabetismo
Costo	Bajo	Bajo	Alto	Muy Alto	Medio	Alto	Alto
Aceptación del usuario	Alta	Alta	Baja	Baja	Baja	Media	Media

Tabla 2: Equipos biométricos.

Fuente: Autor

Se puede evidenciar que la tecnología de control de acceso biométrico por uso de huella dactilar es recomendable por ser una tecnología con alta tasa de aceptación por los usuarios, tener costos accesibles, tener una facilidad de uso y una alta seguridad para la empresa.

ESTUDIO DE FACTIBILIDAD TÉCNICA, OPERATIVA Y ECONÓMICA DEL PROYECTO DISEÑADO.

El presente proyecto se considera factible, porque según la investigación de campo realizada se determinó que el actual sistema de identificación manual para el personal contratista como el sistema automatizado por RFID para el personal fijo se encuentra obsoleto y generando un gasto excesivo a la empresa, además no permite controlar de forma eficaz y precisa la entrada y salida del personal contratista y a su vez del personal fijo que dejo su ficha en su casa o la perdió. Dicho esto, se propone con el proyecto de identificación biométrico mediante huellas dactilares los siguientes beneficios:

- Automatizar los procedimientos manuales
- No depender de una ficha para ingresar a la empresa
- Reducir el pago innecesario por jornadas no laboradas
- Reducir errores y mejorar la precisión a la hora de elaborar los reportes de entrada y salidas del personal que labora en las distintas áreas (Fijo, Contratistas, Pasantes, Visitantes y Jubilados).

Además, en la empresa se cuenta con una serie de objetivos que determinan la posibilidad de Factibilidad del proyecto de un sistema automatizado sin ser limitativos. Estos objetivos son los siguientes:

- Automatización optima de procedimiento manual.
- Reducción de errores y mayor precisión en los procesos.
- Reducción de costos mediante la optimización o eliminación de recursos no necesarios.
- Integración en todas las áreas y subsistemas de la empresa.
- Incrementar la seguridad en el control de acceso.
- Aceleración en la recopilación de datos.

- Obtener información rápida y veraz en caso de requerirla la división de Investigación y Prevención.
- Reducción en el tiempo de procesamiento y ejecución de tareas.

En todos los proyectos se debe evaluar un estudio de factibilidad, con el propósito de determinar los recursos necesarios para la realización de los mismos, por lo que dicho estudio se ha evaluado a través de 3 fases, la Factibilidad Técnica, Económica y Operativa las cuales son detalladas a continuación:

FACTIBILIDAD TÉCNICA.

Por medio de la investigación de campo realizada en la empresa CVG BAUXILUM, se determinó que dicha empresa cuenta con un servidor de aplicación para el control de acceso, servidor con la base de datos en MySQL, la infraestructura cableada requerida, además se dispone por parte de la empresa la capacidad de mejorar el sistema y adquirir los nuevos equipos de control de acceso biométricos de huella dactilar que se utilizaran para el diseño del sistema automatizado para el control de entrada y salida del personal.

8.1.2 HARDWARE

Existen una amplia variedades de hardware que pueden ser utilizados en el diseño del sistema, pero la elección del hardware ideal asegurará el óptimo funcionamiento y rendimiento del sistema.

Para el diseño del sistema, como ya se mencionó, será necesario que se cuente con el hardware necesario para su buen funcionamiento, a continuación se detallan los dispositivos que serán necesarios para el proyecto.

8.1.3 ESTACIÓN DE TRABAJO / WORKSTATION.

Cualquier computadora de escritorio o estación de trabajo puede ser utilizada en cada nodo de una red, por lo tanto, se hace necesario que para el diseño del proyecto se cuente con al menos con una computadora de escritorio.

Basado en el estudio realizado, se determinó que en la empresa cuentan con computadoras de escritorio en óptimas condiciones que no están siendo utilizadas en la actualidad en el área de identificación, que anteriormente se utilizaban para la activación de fichas bajo el Sistema Lenel.

A continuación se detallan las características técnicas mínimas necesarias con las que tiene que contar una computadora ubicada en el área de recepción para que el sistema propuesto funcione de una forma óptima.

- Procesador Intel Celeron 1.8 GHz.
- Disco Duro de 80 GB.
- Memoria RAM 512 MB.
- Tarjeta de Red 10/100mbps.
- Monitor.
- Teclado.
- Mouse.
- Sistema Operativo (Windows, Linux).
- Navegador Web que soporte HTML 5 (Mozilla Firefox, Google Chrome, Microsoft Edge, entre otros).
- Lector de huellas USB (solo utilizado en la taquilla de identificación).

8.1.4 SERVIDOR

El sistema propuesto tiene la capacidad de trabajar de forma simultánea en el actual servidor donde está establecido el software Lenel con la ventaja de no interferir el uno con el otro y en donde compartirán la actual base de datos

de todos los trabajadores en la empresa. De todos modos, los requisitos mínimos que sugiere el Software BioStar de Suprema son los siguientes:

- Windows XP o superior (Solo 32 bits)
- Procesador Intel Pentium IV 1 GHz o superiores.
- Memoria RAM 512 MB
- Disco Duro de 80 GB
- Tarjeta de Red 10/100mbps.

8.1.5 SELECCIÓN DE HARDWARE DE RED.

Para el sistema propuesto se debe contar con una infraestructura de comunicaciones basada en TCP/IP, que en la actualidad ya se encuentra implementada. A continuación se detallan el hardware de red mínimo necesario para un óptimo funcionamiento.

- Switch Full Duplex (100mbps simultáneos).
- Cable de red UTP Cat. 5e.
- Terminales RJ45.

8.1.6 SELECCIÓN DE DISPOSITIVOS DE RECONOCIMIENTO BIOMÉTRICO.

Los dispositivos de Reconocimiento Biométrico están revolucionando el mercado de sistemas de control de acceso de personal en todas las áreas, debido a que se ahorra dinero en comparación con otros sistemas para el control de asistencia como por ejemplo los sistemas de tarjetas RFID, debido a que se elimina el uso de estas tarjetas o de algún otro dispositivo adicional, también se elimina la marcación de compañeros de trabajo, ésta es una de las principales características porque se evita que los compañeros de trabajo se marquen entre ellos la asistencia, ahorrando así un sin fin de pagos de horas

no laboradas que por la falta de recursos no se sabe a ciencia cierta si esta persona las ha trabajado, este tipo de dispositivos ofrecen la solución más exacta de registros de tiempo y asistencia disponibles.

Los sistemas de reconocimiento de huella digital son la manera más antigua de identificación biométrica que ha sido empleada a lo largo del tiempo; la huella digital es una característica física, única que nos distingue a los seres humanos. La huella digital es el patrón característico de un dedo. Se piensa con fuertes evidencias que cada huella digital es única. Cada persona tiene sus propias huellas digitales con la singularidad permanente. De manera que las huellas digitales han sido usadas durante mucho tiempo para la identificación y la investigación forense.

A continuación se mencionan las características del dispositivo biométrico de reconocimiento recomendado Suprema Inc.

8.1.7 SUPREMA INC.

Suprema es una compañía ubicada en Seongnam-si, Gyeonggi-do, Corea del Sur, que ofrece tecnologías centrales para huellas dactilares para aplicaciones en PC, dispositivos de control de acceso y control de asistencia. La solución de Suprema se representa por la integración la capacidad, del diseño, sistema de algoritmos utilizado en la verificación y autentificación del usuario.

Figura 5.1: Logo de la compañía Suprema Inc.
Fuente: https://www.supremainc.com/.

El algoritmo de huellas dactilares de Suprema probó ser la solución más confiable del mundo al clasificarse No. 1 en la Competencia Internacional de Verificación de Huellas dactilares (FVC) consecutivamente en 2004 y 2006, con desempeño sobresaliente y sin rival. Suprema es la primera compañía de biométrica listada en el mercado de valores de Corea (KOSDAQ) y su capital de mercado excede US$100 millones, y los productos de la compañía se han vendido a más de 100 países en todo el mundo. Sus clientes incluyen compañías como Samsung, Toshiba e Hitachi y en modo local se encuentran el Aeropuerto Internacional Manuel Piar, Clínica Unare, Aserca Airlines, Hotel Eurobuilding, entre otros.

8.1.7.1 SUPREMA BIOENTRY PLUS

BioEntry Plus es un dispositivo de control de acceso de huella dactilar basado en la conexión IP, de fácil instalación y de fácil operación por el usuario. Además de integrar el sistema de huellas dactilar, posee una lectora de tarjetas RFID en sus múltiples versiones, en este caso se utilizara el del estándar de tarjetas de proximidad HID a 125khz, el diseño del equipo se puede observar en la figura 5.2.

Figura 5.2: Suprema BioEntry Plus.
Fuente: https://www.supremainc.com/.

El dispositivo integra las interfaces TCP/IP, RS-485, Wiegand, haciéndolo compatible con el actual sistema Lenel y favoreciendo en el impacto que surgirá en el proceso migratorio del sistema de tarjetas RFID al sistema biométrico. El BioEntry Plus también viene con 2 entradas internas (Sensor de Puerta y botón de emergencia o pánico) y 1 salida interna (Relay) para controlar los dispositivos periféricos o cerraduras eléctricas o por electroimán, en la figura 5.3 se puede observar el modo autónomo del equipo (la conexión LAN es opcional) y en la figura 5.4 el modo de conexión en red.

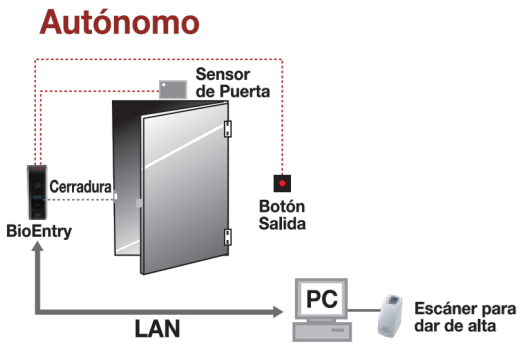


Figura 5.3: Modo autónomo.

Fuente: https://www.supremainc.com/.

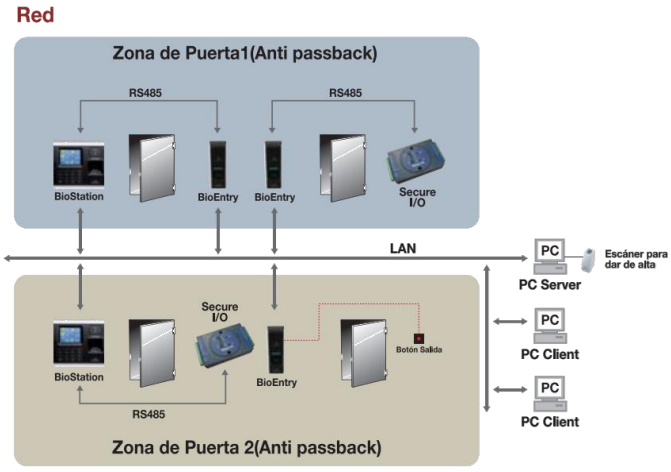


Figura 5.4: Modo red.

Fuente: https://www.supremainc.com/.

8.1.7.1.1 CARACTERÍSTICAS

- CPU de 400mhz.
- Sensor óptico de 500ppp.
- Capacidad de almacenamiento de 5.000 usuarios (10.000 huellas).
- Identificación de 1:2.000 huellas dactilares en 1 segundo.
- Relay integrado para el control de acceso de puertas eléctricas, cerraduras electromagnéticas, molinetes, brazo basculantes entre otros.
- Salida Wiegand configurable hasta los 64 bits.
- Soporte de tarjetas HID 125khz.
- Led multicolor y sonido multitono.
- Alimentación médiate la interfaz PoE.
- Log de memoria interna de 50.000 eventos.
- Opción de dedo pánico.
- Interfaz Ethernet.
- Modo anti-passback.

8.1.7.1.2 USOS

Este equipo puede ser utilizado en zonas de bajas demandas e internas dentro de la empresa debido a que no soporta el uso en intemperie.

8.1.7.2 SUPREMA BIOENTRY W

BioEntry Plus/W dispone de una estructura resistente al vandalismo y con nivel de protección IP65 además de tener su lector de huellas y lector de tarjetas RFID. BioEntry W es ideal para instalaciones en exteriores ya que ofrece durabilidad excepcional bajo condiciones ambientales severas.

Figura 5.5: Suprema BioEntry W.

Fuente: https://www.supremainc.com/.

Al igual que el BioEntry Plus, el BioEntry W integra las interfaces TCP/IP, RS-485, Wiegand. El BioEntry W también viene con 2 entradas internas (Sensor de Puerta y botón de emergencia o pánico) y 1 salida interna (Relay), además de tener las certificaciones IP65 (protección contra polvo y agua) y la IK08 (antivandálico) para controlar los dispositivos periféricos o cerraduras eléctricas o por electroimán, en la figura 5.6 se puede observar el modo autónomo del equipo (la conexión LAN es opcional) y en la figura 5.7 el modo de conexión en red.

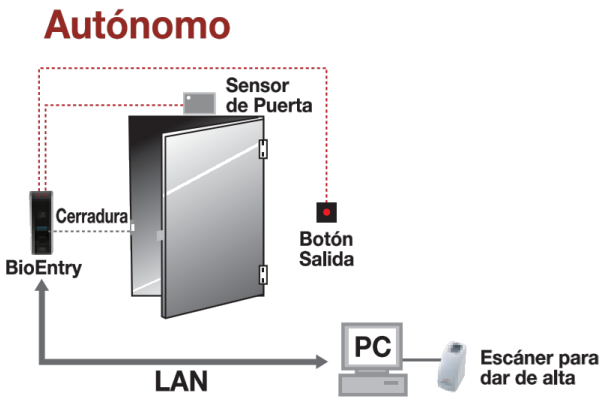


Figura 5.6: Modo autónomo.

Fuente: https://www.supremainc.com/.

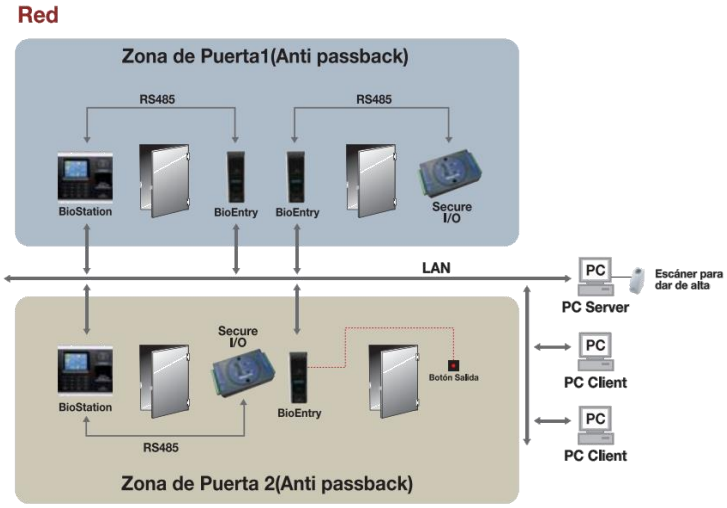


Figura 5.7: Modo red.

Fuente: https://www.supremainc.com/.

8.1.7.2.1 CARACTERÍSTICAS

- Protección IP65 contra Polvo y Agua
- Protección IK08 Antivandálico
- CPU de 400mhz.
- Sensor óptico de 500ppp.
- Capacidad de almacenamiento de 5.000 usuarios (10.000 huellas).
- Identificación de 1:2.000 huellas dactilares en 1 segundo.
- Relay integrado para el control de acceso de puertas eléctricas, cerraduras electromagnéticas, molinetes, brazo basculantes entre otros.
- Salida Wiegand configurable hasta los 64 bits.
- Soporte de tarjetas HID 125khz.
- Led multicolor y sonido multitono.
- Alimentación médiate la interfaz PoE.
- Log de memoria interna de 50.000 eventos.

- Opción de dedo pánico.
- Interfaz Ethernet.
- Modo anti-passback.

8.1.7.2.2 USOS

Este equipo puede ser utilizado en las puertas de los edificios en zonas de bajas demandas gracias a su soporte de intemperie.

8.1.7.3 SUPREMA BIOSTATION 2

El equipo BioStation 2 es un dispositivo de última generación que incorpora un potente procesador y es de alta demanda, además de incorporar un nuevo sensor óptico en donde es capaz de identificar hasta 20.000 huellas en un segundo.

Figura 5.8: Suprema BioStation 2.
Fuente: https://www.supremainc.com/.

8.1.7.3.1 CARACTERÍSTICAS

- Protección IP65 contra Polvo y Agua
- Protección IK08 Antivandálico
- CPU Dual Core de 1.0ghz.
- Sensor óptico de 500ppp.
- Capacidad de almacenamiento de 500.000 usuarios (1.000.000 huellas).
- Pantalla de 2.5” QVGA.
- Identificación de 20.000 huellas dactilares en 1 segundo.
- Relay integrado para el control de acceso de puertas eléctricas, cerraduras electromagnéticas, molinetes, brazo basculantes entre otros.
- Salida Wiegand, TCP/IP, RS485, RS232, TTL I/O, WIFI
- Soporte de tarjetas HID 125khz.
- Led multicolor y sonido multitono.
- Alimentación médiate la interfaz PoE.
- Log de memoria interna de 3.000.000 eventos.
- Opción de dedo pánico.
- Interfaz Gigabits Ethernet.
- Puerto USB.
- Micrófono y altavoz.
- Modo anti-passback.

El equipo BioStation 2 solo es compatible con el Software BioStar 2, el diagrama de conexión se presenta a continuación.

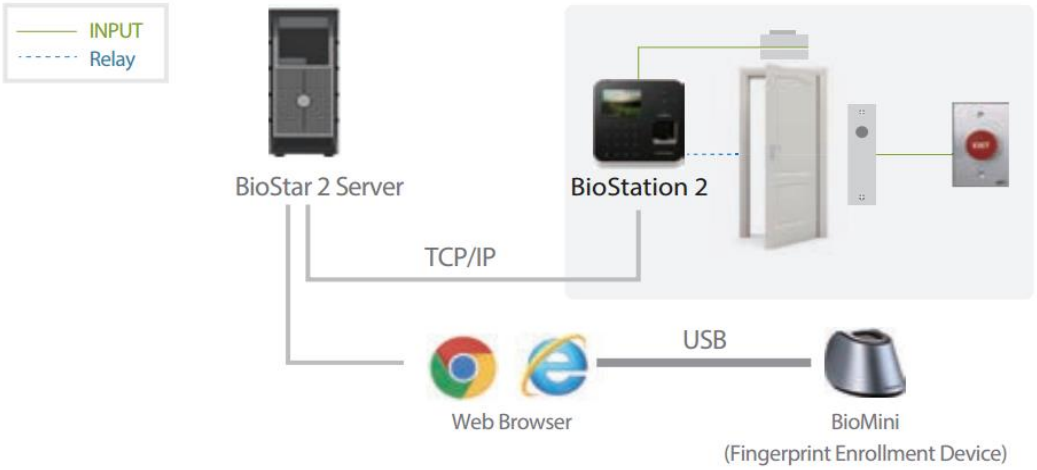


Figura 5.9: Suprema BioStation 2.
Fuente: https://www.supremainc.com/.

8.1.7.3.2 USOS

Debido a la alta velocidad de identificación y verificación, y su alta capacidad de almacenamiento, este equipo puede ser utilizado en las mangas de identificación y es compatible con todas las puertas para un rápido control de acceso.

8.1.7.4 SOFTWARE SUPREMA BIOSTAR 2

BioStar 2 establece el nuevo estándar en seguridad mediante el entorno basado en la nube para el control de acceso biométrico, proporcionando la capacidad de una fácil integración con sistemas de terceros (Lenel) y permite a los desarrolladores de software incorporar nuevas aplicaciones y funciones a BioStar 2. La accesibilidad a BioStar 2 y sus APIs se extienden aún más a través de los servicios basados en la nube.

El software posee un solo nivel de licencia completa en donde la plataforma permite su expansión gracias a sus capacidades de integración y

desarrollo a través de la API BioStar 2 y del SDK de dispositivo BioStar 2 que proporcionan flexibilidad y versatilidad. La revolucionaria aplicación BioStar 2 Mobile junto con la API BioStar 2 permiten una forma completamente nueva de configurar y gestionar el sistema mediante navegadores web (Microsoft EDGE, Google Chrome, Mozilla Firefox, Apple Safari, entre otros). La versión BioStar 2.1 incluye la API BioStar 2, un conjunto de APIs REST que utilizan datos formateados JSON para solicitudes y respuestas para un mejor entendimiento.

El módulo de control de acceso de BioStar 2, incluye varias actualizaciones clave y la usabilidad mejorada permite asignar usuarios a grupos de acceso y configurar el nivel de acceso de manera más simple para un desarrollo más rápido. El módulo también proporciona la función para importar/exportar grupos de usuarios e identificaciones de tarjetas para brindar mayores ventajas al usuario.

La aplicación BioStar 2 Mobile utiliza la nube BioStar 2 a través de la API. Está diseñada para interactuar con el servidor BioStar 2 local a través de la API BioStar 2 y permite a los usuarios acceder de manera remota al servidor y llevar a cabo las operaciones del sistema/usuario y el monitoreo del sistema en cualquier momento y en cualquier lugar. El uso de la API BioStar 2 (Ver figura 5.10) mantiene la integridad de la seguridad del servidor durante el acceso remoto.

Figura 5.10: Uso del API BioStar 2 en un iPhone, también compatible con Android.

Fuente: https://www.supremainc.com/.

A través de la API BioStar Mobile, los administradores pueden agregar, editar o eliminar usuarios fácilmente de manera remota a través de la aplicación. La aplicación también controlará cualquier dispositivo instalado en la red para capturar nuevos datos biométricos del usuario.

La compatibilidad con la nube permite el acceso remoto al servidor BioStar 2 utilizando cualquier aplicación que utilice la API BioStar 2 o la aplicación Suprema BioStar 2 Mobile.

El software también ofrece la sincronización automática de usuario, incorporaciones, eliminaciones y modificaciones de datos de los usuarios en el servidor se sincronizarán automáticamente en los dispositivos configurados en el sistema.

Entre otra de las funciones es que permite que la plataforma detecte todos los dispositivos conectados dentro de la red IP para su configuración e instalación y la notificación de actualización automática vía nube, bien sea del software del servidor o el firmware de los dispositivos

A nivel de seguridad se tienen que las comunicaciones entre el servidor y el cliente están protegidas por el cifrado HTTPS mediante el uso del navegador y la comunicación entre el servidor y el dispositivo está protegida por el cifrado AES de 256 bits. Además en que el software BioStar 2 también protege los datos de los usuarios, tales como huellas digitales, PINs y contraseñas usando normas de cifrado de 256 bits.

8.1.7.4.1 DISPOSITIVOS COMPATIBLES

Figura 5.11: Lista de equipos compatible con el software BioStar 2.

Fuente: https://www.supremainc.com/.

8.1.7.5 TOPOLOGÍA DE RED

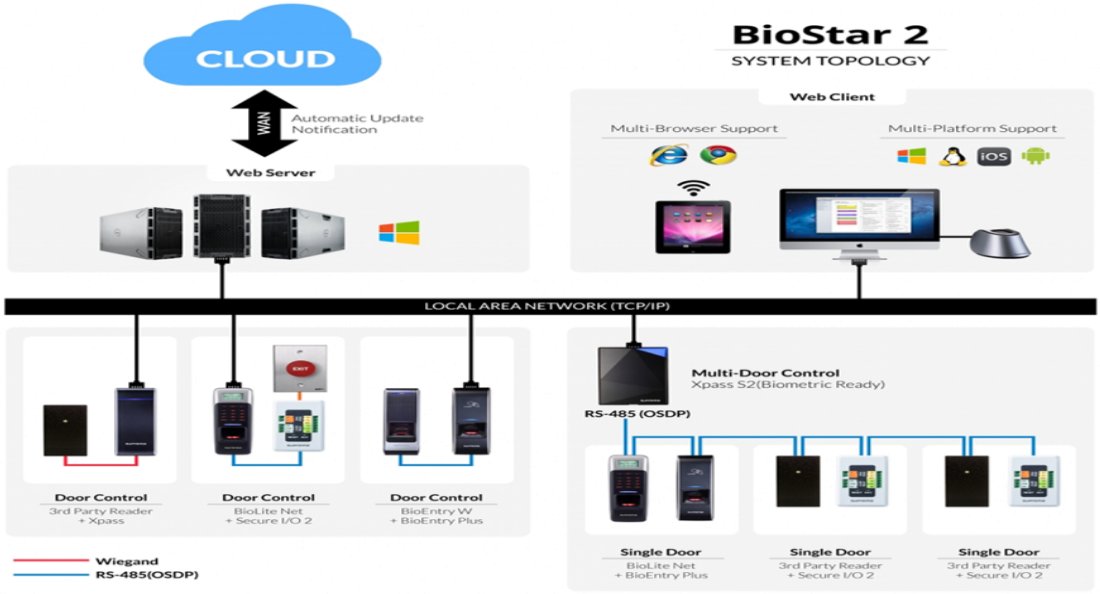


Figura 5.12: Topología de la red, utilizando un Servidor BioStar 2.

Fuente: https://www.supremainc.com/.

La topología establecida es la ideal gracias a su tecnología basada en estrella, ofreciendo eficiencia y facilidad de utilizar el estándar plug and play protocolos de comunicación utilizado donde se conecta el dispositivo al switch y es detectado automáticamente en el sistema.

La configuración de red que dispone la empresa con el sistema Lenel es tipo estrella, cuyas ventajas y desventajas son:

Ventajas:

- Posee un sistema que permite agregar nuevos equipos fácilmente.
- Fácil de prevenir daños y/o conflictos.
- Centralización de la red.

Desventajas:

- Si el switch central falla, toda la red deja de transmitir.
- Es costosa, ya que requiere más cables que las topologías en bus o anillo.
- El cable viaja por separado del concentrador a cada computadora.

8.1.7.6 SUPREMA BIOMINI PLUS

BioMini Plus es un escáner utilizado como dispositivo de enrolamiento de huellas dactilares, está certificado por la categoría PIV Single Finger Capture Devices. La certificación asegura que los dispositivos cumplen con la especificación de calidad de imagen de la Identificación de Próxima Generación (NGI) del FBI.

Figura 5.13: SUPREMA BioMini Plus.
Fuente: https://www.supremainc.com/.

Este dispositivo cuenta con una detección híbrida de dedos en tiempo real que examina tres aspectos de las huellas dactilares: patrones de cambio dinámico, viveza de las características y anormalidad de las características.

Después de un cuidadoso análisis de las tres características, el algoritmo del lector será capaz de rechazar las huellas dactilares que se consideran falsas.

8.1.8 PROVEEDORES

8.1.8.1 BIOIDENTIDAD

Empresa especializada en sistemas biométricos de alto desempeño para el control e identificación de personas.

Brinda consultoría, soluciones y productos en las áreas de biometría, documentos de identidad, tarjetas inteligentes, proximidad, control de acceso, control de asistencia, identificación en radiofrecuencia, PKI, firmas digitales, integración de sistemas, desarrollo de software y equipamiento especializado, así como en normas y estándares técnicos internacionales relacionados.

e-mail: info@bioidentidad.com.ve, Teléfono: 0212-3191926, Caracas, Venezuela.

8.1.8.2 GRUPO MONVE

Es una empresa que trabaja con venta e instalación de equipos biométricos de calidad, está orientado a realizar las instalaciones a medida de acuerdo a las necesidades de sus clientes.

e-mail: crodriguez@grupomonve.com, Teléfono: 0212-3149760, Caracas, Venezuela.

8.1.8.3 WindowGard de Venezuela C.A.

Empresa que está dedicada a proveer soluciones integrales de tecnologías de seguridad para el mercado corporativo.

e-mail: info@windowgard.com, Teléfono: 0286-9524383, Puerto Ordaz, Venezuela.

Al adquirir los equipos, todos los proveedores ofrecen 1 año de garantía contra cualquier falla, asesoría, capacitación (adicional) y un software especializado de control de acceso y asistencia BioStar 1.8 Free.

8.1.9 CRITERIOS MÍNIMOS PARA EL DISEÑO DEL SISTEMA.

Las condiciones óptimas para el diseño del sistema de control de entrada y salida del personal que labora en la empresa área son las siguientes:

a) **Portabilidad:** Es la capacidad que tiene el software de migrar de una plataforma a otra con transferencia de la base de datos.

b) **Conectividad:** Capacidad de traslado o migración de los datos, almacenamiento y rendimiento entre versiones de software.

c) **Soporte Técnico:** Debe existir un proveedor autorizado en el país que brinde soporte técnico al sistema de gestión de la base de datos.

d) **Relacionalidad:** Debe ser relacional el sistema de gestión de base de datos

e) **Integridad:** Es la capacidad de permitir modificaciones en un momento determinado sin afectar el funcionamiento del sistema.

FACTIBILIDAD OPERATIVA

El proyecto es factible porque el personal que opera los sistemas de control de entrada y salida tanto del proceso manual como el automatizado es

controlada por la Gerencia Seguridad Patrimonial y la planilla (pase) es elaborada por los Analistas De Identificación de la Empresa, están conscientes de la necesidad de contar con una herramienta tecnológica que les permita automatizar el proceso y de esta forma mejorar la efectividad y la confiabilidad de la información y a su vez automatizar el proceso de realizar la planilla de ingreso.

La Factibilidad Operativa del nuevo sistema, se comprobó que la empresa será capaz de darle uso al sistema, que cuenta con el personal capacitado para hacerlo y tiene los recursos humanos necesarios para mantener el sistema. Para esto, el sistema contempla cinco puntos importantes al momento de implantarse.

- **El sistema no debe ser complejo**; gracias a la interfaz intuitiva del sistema BioStar, los administradores que operaran el sistema no tendrán que preocuparse darle un uso indebido, y al usuario, gracias a la actual implementación de esta tecnología en los supermercados y farmacias, ya se encuentran adaptados a este sistema logrando simplificar las funciones y dar todo por servido.
- **Evitar que a los usuarios les incomode el nuevo sistema**; el sistema será mucho más fácil que ingresar al sistema Lenel, gracias a que no necesita un software instalado en el pc cliente, solo necesitara disponer de un navegador web o el software descargado en el equipo celular, el sistema se encuentra en el idioma español y es una interfaz intuitiva y amigable. En el caso de los usuarios, a la hora de marcar su acceso ya no tendrán el inconveniente de que se le haya quedado la ficha, extraviado o dañado debido a que su sistema de identificación siempre lo lleva consigo.
- **Un cambio repentino, puede ocasionar un lento aprendizaje**; por ende el proceso de migración y automatización se realizara

de la siguiente manera: 1) Personal contratista, 2) Visitantes, 3) Pasantes, 4) Personal jubilado y 5) Personal fijo y contratado, con el fin de que se vayan familiarizando, capacitando y permitir al personal adaptarse a él con la tranquilidad y apoyo necesario como manuales, charlas y capacitaciones.

- **Posibilidad de la obsolescencia subsecuente**; La tecnología existe, por ende se seleccionó la mejor empresa que ofrece la relación calidad-precio, stock disponible en el mercado venezolano, ofreciendo la última tecnología disponible debido a que es mejor constar con tecnología que esté disponible en el momento (evitando la temprana obsolescencia) y sea fácil de obtener o esté más al alcance de la mano (por si se requieren repuestos o correcciones sea fácil de conseguir).
- **Indicadores para la Gerencia**; Permitirá verificar la información de una fuente confiable y segura, permitiendo así el monitoreo continuo del ingreso, estadía y salida del personal de la planta, además de incrementar los estándares de seguridad en la empresa.

8.1.10 RECURSO HUMANO.

Para el diseño operativo del nuevo sistema automatizado de control de acceso biométrico, se estableció la siguiente disposición para utilizar el sistema.

Número de personal	Cargo
1	Gerente de Seguridad Patrimonial
1	Jefe División Identificación y Control de Acceso

1	Jefe División Investigación y Prevención
1	Administrador del Sistema CECON
1	Analista de Identificación y Control de Acceso
1	Auxiliar de Analista de Identificación y Control de Acceso

Tabla 3: Recursos Humanos.
Fuente: Autor.

Como se puede observar, el recurso humano para ejecutar el sistema será de seis empleados directos, distribuidos en los siguientes cargos: un gerente, dos jefes, un administrador, un analista y un auxiliar.

FACTIBILIDAD ECONÓMICA.

En el diseño de un sistema cualquiera es de suma importancia contar con la estimación de los costos necesarios para llevar a cabo la implementación, en dicha estimación de costos es de suma importancia detallar los costos de los equipos, software adicional así como también los costos por mantenimiento.

8.1.11 COSTOS DE DESARROLLO DEL PROYECTO.

Para la estimación de la inversión que se tiene que realizar para que el sistema de control de entrada y salida se implemente se han separado en 4 diferentes grupos que son:

- Costos de Hardware.
- Costos de Equipo de Red.
- Costos de Dispositivos Biométricos.
- Costos del Diseño y Desarrollo.
- Costos de Licencias para Software.

8.1.11.1 COSTOS DE HARDWARE.

Los costos de hardware se estimaran basados en las especificaciones técnicas mencionadas en el estudio de la factibilidad técnica en ese apartado se determinó que el equipo computacional necesario para la implementación se divide en dos subgrupos. El costo de los Workstation es 0, en vista de que ya se encuentran instalados los equipos pero temporalmente fuera de servicio, los equipos que son indispensables son los accesorios como la webcam, el lector biométrico usb y el ups. En las siguientes tablas se puede apreciar los costos por hardware y accesorios.

COSTO DEL WORKSTATION PARA IDENTIFICACIÓN			
Cantidad	**Especificaciones Técnicas**	**Unidad**	**Total**
2	Procesador Celeron 1.8 GHz	0BsF	0BsF
	Disco Duro de 80 Gb		
	Memoria Ram 512 MB		
	Tarjeta de Red 10/100		
	Monitor 15”		
	Teclado		
	Mouse		
2	UPS 100 Watt	0BsF	0BsF

TOTAL	**0BsF**	**0BsF**

Tabla 4: Costos de los Workstations.

Fuente: Autor

No se generan costos para la implementación de los Workstation en vista de que la empresa ya dispone de las estaciones necesarias.

COSTO DE LOS ACCESORIOS PARA EL WORKSTATION PARA IDENTIFICACIÓN			
Cantidad	**Especificaciones Técnicas**	**Unidad**	**Total**
2	Webcam Microsoft Lifecam Studio HD	34.720BsF	69.440BsF
2	Suprema BioMini Plus USB	114.751BsF	229.502BsF
TOTAL		**149.471BsF**	**298.942BsF**

Tabla 5: Costos de los accesorios a utilizar en los Workstations.

Fuente: Autor

En la tabla se puede apreciar los accesorios necesarios para el diseño del sistema, estos equipos son webcam Microsoft Studio HD utilizada para la captura de la foto del contratista y el lector Suprema USB biométrico de huella dactilar, para la captura y registro del personal contratista.

8.1.11.2 COSTOS DE EQUIPO DE RED.

Los costos de equipo de red se estimaran basados en las especificaciones técnicas mencionadas en el estudio de la factibilidad técnica, en ese apartado se determinó que la empresa ya dispone de la infraestructura tanto el cableado como el hardware para realizar la conexión desde el dispositivo biométrico hasta el servidor, solo se reemplazara la lectora por el biométrico.

COSTO DE EQUIPOS DE RED			
Cantidad	**Especificaciones Técnicas**	**Unidad**	**Total**
1	Cable UTP 5e	0BsF	0BsF

	Switch 10baseT (10mbps)		
	Conectores RJ45		
TOTAL		**0BsF**	**0BsF**

Tabla 6: Costos de equipos de red.

Fuente: Autor

En vista de que la empresa ya dispone de la infraestructura necesaria, únicamente será necesario reemplazar los lectores HID por los lectores biométricos Suprema. Disminuyendo los costos necesarios para la instalación de equipos de red.

8.1.11.3 COSTO DE LICENCIAS PARA SOFTWARE.

Los costos de Software se estimarán basados en las especificaciones técnicas mencionadas en el estudio de la factibilidad técnica, ahí se determinó el software más indicado para que el sistema funcione de forma óptima. A continuación se muestra los costos por concepto de software y licencias.

COSTO DE LICENCIAS PARA SOFTWARE				
Cantidad	Tipo	Especificaciones	Unidad	Total
1	Sistema Operativo	Windows XP	0BsF	0BsF
1	Sistema de control de acceso biométrico y de asistencia con Licencia	BioStar 2	580.533,20BsF	580.533,20BsF
TOTAL			580.533,20BsF	580.533,20BsF

Tabla 7: Costos de las licencias para el servidor.

Fuente: Autor.

La empresa cuenta con un servidor equipado con Windows XP con licencia de Lenel OnGuard 05 y base de datos bajo MySQL, y gracias a la arquitectura del sistema BioStar puede trabajar en simultáneo con el actual sistema a su vez compartiendo la actual base de datos, permitiendo la reducción de costos del servidor y del sistema operativo.

8.1.11.4 COSTOS DE EQUIPO BIOMÉTRICOS.

Los costos del equipo biométrico se estimaron basados en las especificaciones técnicas mencionadas en el estudio de la factibilidad técnica, se determinó que la primera fase como del proyecto contara con cuatro lectoras de alta demanda como propuesta uno o cuatro lectoras de baja demanda como propuesta dos. Debido al amplio número de dispositivos en el mercado a nivel mundial, se propone tomar en cuenta el dispositivo de reconocimiento de huella digital Suprema debido a que es uno el dispositivo que se comercializa en

Venezuela, tiene 1 año de garantía y gracias a sus altos estándares y algoritmos utilizados en la detección de huella lo hace rápido y eficiente. Se establecen 3 propuestas para el análisis de costos de los equipos biométricos, entre ellas tenemos los Suprema Biostation, Bioentry W y Bioentry Plus.

COSTO DE DISPOSITIVO BIOMETRICO			
Cantidad	**Especificaciones**	**Unidad**	**Total**
8	BioStation 2 HID Prox	1.087.637,20BsF	8.701.097,60BsF
TOTAL		**1.087.637,20BsF**	**8.701.097,60BsF**

Tabla 8: Costos de los dispositivos Biométrico BioStation 2.

Fuente: Autor

Se especifica el costo por unidad de dispositivo biométrico BioStation 2, utilizados en áreas de alta demanda, alta capacidad de usuarios registrados y certificación IP65 (resistente al agua y polvo).

COSTO DE DISPOSITIVO BIOMETRICO			
Cantidad	**Especificaciones**	**Unidad**	**Total**
8	BioEntry W HID Prox	677.461,20BsF	5.419.689,60BsF
TOTAL		**677.461,20BsF**	**5.419.689,60BsF**

Tabla 9: Costos de los dispositivos Biométrico BioEntry W.

Fuente: Autor

Se presenta el costo detallado por cada unidad de dispositivo biométrico BioEntry W, utilizados en áreas de baja demanda, alta capacidad de usuarios registrados y certificación IP65 (resistente al agua y polvo).

COSTO DE DISPOSITIVO BIOMETRICO			
Cantidad	Especificaciones	Unidad	Total
8	BioEntry Plus HID Prox	514.672,60BsF	4.117.380,80BsF
TOTAL		514.672,60BsF	4.117.380,80BsF

Tabla 10: Costos de los dispositivos Biométrico BioEntry Plus.

Fuente: Autor

Se establece el costo por unidad de dispositivo biométrico BioEntry Plus, utilizados en áreas de baja demanda, alta capacidad de usuarios registrados, no es resistente al agua ni al polvo.

8.1.11.5 COSTOS DE IMPLEMENTACIÓN.

Para los costos del diseño del sistema se tomaron en cuenta los salarios y también los costos de los servicios que brindan empresas especializadas en las áreas como por ejemplo en el área eléctrica, instructores, etc.

COSTO DE IMPLEMENTACIÓN	
Descripción	**Costos**
Personal para instalaciones física y software	1.266,67BsF
Personal desarrollo del Software	17.874,33BsF
Instructor para capacitación del sistema biométrico	20.000,00BsF
TOTAL	**39.141,00BsF**

Tabla 11: Costos mano de obra para la implementación del sistema.

Fuente: Autor

Al estimar el costo de implementación necesario para la instalación y capacitación del sistema, se generara un costo total de 39.141Bsf

8.1.11.6 ANÁLISIS COSTO-BENEFICIO

Cuando se realiza cualquier proyecto y en especial un sistema de información es necesario tener en cuenta una estimación de los costos para su implementación, analizar los beneficios que le traerá a la empresa implementando dicho sistema, es decir que beneficio le traerá adjudicar una suma de dinero y determinar si será una inversión o si será un gasto.

8.1.11.7 COSTO – BENEFICIO ECONÓMICO

En el costo – beneficio económico se debe hacer una valoración de la inversión inicial, comparar el sistema actual con el sistema propuesto en términos económicos, para determinar la rentabilidad del proyecto.

El resultado económico el sistema Suprema BioStar fue evaluado a través de la información contenida en las siguientes tablas:

- **DETALLE DE INVERSIÓN**

En el detalle de la inversión inicial se tomó en cuenta los costos que se detallaron anteriormente, dando así como resultado una estimación total para el diseño del sistema.

INVERSIÓN PROYECTADA	
Descripción	**Total**
Costo de accesorios de los Workstations	298.942BsF
Costos de equipos de red	0BsF
Costos de dispositivos biométricos BioStation 2	8.701.097,60BsF
Costos de licencias	580.533,20BsF
Costos de diseño	39.141BsF
TOTAL	**9.619.713,80BsF**

Tabla 12: Propuesta 1 utilizando el dispositivo Biométrico BioStation 2.

Fuente: Autor

En la tabla anterior se proyectan los costos totales generados para la implementación del proyecto, tomando en cuenta la propuesta 1 (equipos biométricos BioStation 2).

INVERSIÓN PROYECTADA	
Descripción	Total
Costo de Workstation	298.942BsF
Costos de equipos de red	0BsF
Costos de dispositivos biométricos	5.419.689,60BsF
Costos de licencias	580.533,20BsF
Costos de diseño	39.141BsF
TOTAL	6.338.305,80BsF

Tabla 13: Propuesta 2 utilizando el dispositivo Biométrico BioEntry W.

Fuente: Autor

En la tabla anterior se proyectan los costos totales generados para la implementación del proyecto, tomando en cuenta la propuesta 2 (equipos biométricos BioEntry W).

INVERSIÓN PROYECTADA	
Descripción	Total
Costo de Workstation	298.942BsF
Costos de equipos de red	0BsF
Costos de dispositivos biométricos	4.117.380,80BsF
Costos de licencias	580.533,20BsF
Costos de diseño	39.141BsF
TOTAL	5.035.997,00BsF

Tabla 14: Propuesta 3 utilizando el dispositivo Biométrico BioEntry Plus.

Fuente: Autor

En la tabla anterior se proyectan los costos totales generados para la implementación del proyecto, tomando en cuenta la propuesta 3 (equipos biométricos BioEntry Plus).

COSTO DEL SISTEMA ACTUAL				
Cant.	**Descripción**	**Costo Unitario**	**Costo Mensual**	**Costo Anual**
1	Analista de identificación	25.000BsF	25.000BsF	300.000BsF
1	Analista de identificación	25.000BsF	25.000BsF	300.000BsF
1	Auxiliar de Analista de identificación	18.000BsF	18.000BsF	216.000BsF
50	Tarjetas RFID Marca HID ProxCard II	2.925BsF	146.250BsF	1.755.000BsF
1	Cinta para impresora de carnet	140.000BsF	140.000BsF	1.680.000BsF
50	Sticker para carnet HID ProxCard II	500BsF	25.000BsF	300.000BsF
3	Papelería: Resmas de hojas	3.500BsF	10.500BsF	126.000BsF
1	Papelería: Tóner de Impresora Samsung	16.289,99BsF	16.289,99BsF	195.479,88BsF
3	Papelería: Bolígrafos	25Bsf	75BsF	900BsF
1	Papelería: Tinta para sello	169,99BsF	169,99BsF	2.039,88BsF
TOTAL			**406.284,98BsF**	**4.875.419,76BsF**

Tabla 15: Gastos generados por el sistema actual.

Fuente: Autor

En el actual sistema de identificación y control de acceso para el personal se generan el siguiente costo anual 4.875.419,76BsF, donde se generan los mayores costos en la adquisición de las tarjetas RFID HID, Sticker y cinta para la impresora.

COSTO DEL SISTEMA PROPUESTO				
Cant.	Descripción	Costo Unitario	Costo Mensual	Costo Anual
1	Analista de identificación	25.000BsF	25.000BsF	300.000BsF
1	Auxiliar de Analista de identificación	18.000BsF	18.000BsF	216.000BsF
6	Caja de tarjetas de PVC para carnets de identificación, 500 unidades	55BsF	27.500BsF	165.000BsF
1	Cinta para impresora de carnet	140.000BsF	140.000BsF	1.680.000BsF
TOTAL			210.500BsF	2.526.000BsF

Tabla 16: Gastos generados por el sistema propuesto.

Fuente: Autor

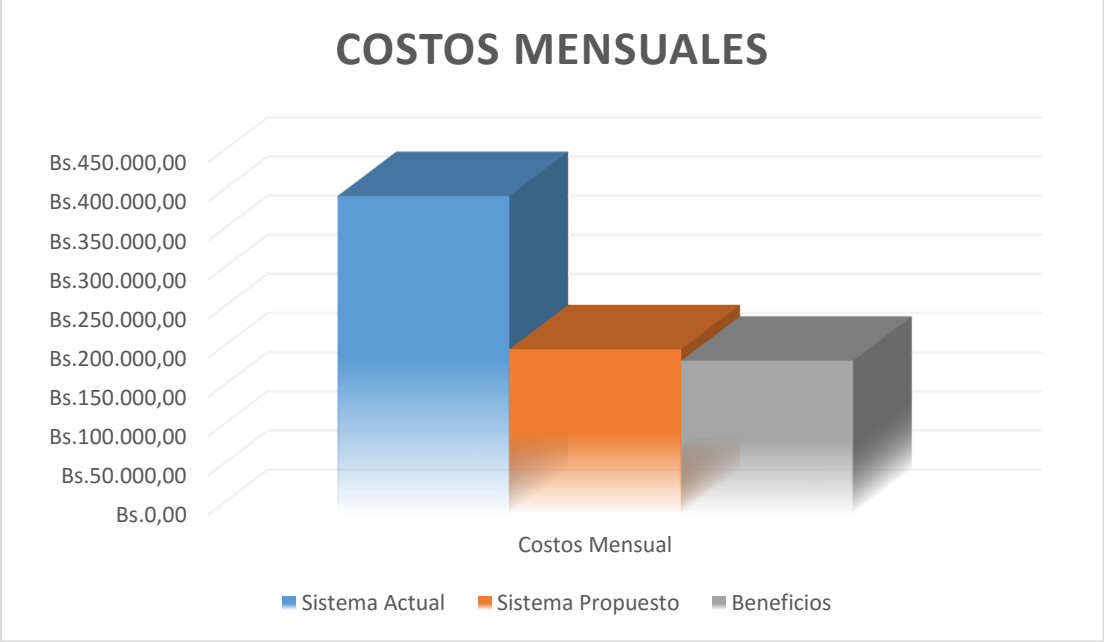
Con el sistema propuesto, se evidencia un gasto total anual de 2.526.000BsF., siendo más económico para la empresa, se puede evidenciar que el mayor gasto recurre en la cinta para impresora de carnets, sin embargo este recurso es indispensable para cualquier sistema de identificación aplicado en la empresa.

BENEFICIO PROYECTADO		
Descripción	Costo Mensual	Costo Anual
Sistema Actual	406.284,98BsF	4.875.419,76BsF
Sistema Propuesto	210.500,00BsF	2.526.000,00BsF
Beneficio en disminución de gastos	195.784,98BsF	2.349.419,76BsF

Tabla 17: Beneficios proyectados por el sistema propuesto.

Fuente: Autor

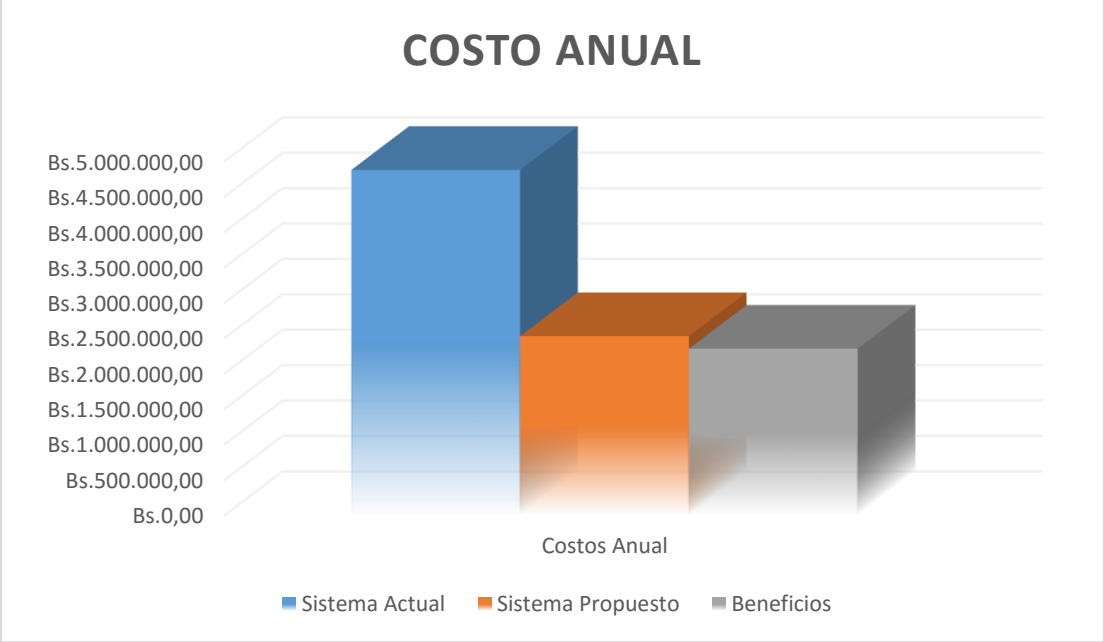
Al comparar el sistema actual con el propuesto se tiene un beneficio de 2.349.419,76BsF, siendo el sistema propuesto la solución más rentable para la identificación y control de acceso al personal.



Gráfica 3: Comparativa de costos mensuales.

Fuente: Autor

Se puede observar que el sistema actual genera costos mensuales mayores a 400.000BsF mientras que el sistema propuesto generaría costos mensuales sobre los 200.000BsF otorgándole a la empresa una reducción de costos de 195.784,98BsF.



Gráfica 4: Comparativa de costos anual.

Fuente: Autor

Se puede interpretar que el sistema actual genera costos anuales sobre los 4.500.000BsF mientras que el sistema propuesto generaría costos anuales sobre los 2.500.000BsF otorgándole a la empresa una reducción de costos 2.349.419,76BsF.

8.1.11.8 REDUCCIÓN DE COSTOS

Es el cálculo de la utilidad que se puede obtener después de un determinado lapso de tiempo, donde la utilidades van absorbiendo la inversión inicial hasta obtener los beneficios netos del proyecto.

En el beneficio mensual es el ahorro que obtiene la empresa al implementar en nuevo sistema más el ahorro en el pago de la renta.

- **PROPUESTA 1, EQUIPO BIOMÉTRICO SUPREMA BIOSTATION**

REDUCCIÓN DE COSTOS			
MES	INVERSIÓN INICIAL	REDUCCIÓN DE COSTOS	ACUMULADO
1	BS.9.619.713,80	BS.195.784,98	BS.9.423.928,82
2	BS.9.423.928,82	BS.195.784,98	BS.9.228.143,84
3	BS.9.228.143,84	BS.195.784,98	BS.9.032.358,86
4	BS.9.032.358,86	BS.195.784,98	BS.8.836.573,88
5	BS.8.836.573,88	BS.195.784,98	BS.8.640.788,90
6	BS.8.640.788,90	BS.195.784,98	BS.8.445.003,92
7	BS.8.445.003,92	BS.195.784,98	BS.8.249.218,94
8	BS.8.249.218,94	BS.195.784,98	BS.8.053.433,96
9	BS.8.053.433,96	BS.195.784,98	BS.7.857.648,98
10	BS.7.857.648,98	BS.195.784,98	BS.7.661.864,00
11	BS.7.661.864,00	BS.195.784,98	BS.7.466.079,02
12	BS.7.466.079,02	BS.195.784,98	BS.7.270.294,04
13	BS.7.270.294,04	BS.195.784,98	BS.7.074.509,06
14	BS.7.074.509,06	BS.195.784,98	BS.6.878.724,08
15	BS.6.878.724,08	BS.195.784,98	BS.6.682.939,10
16	BS.6.682.939,10	BS.195.784,98	BS.6.487.154,12
17	BS.6.487.154,12	BS.195.784,98	BS.6.291.369,14
18	BS.6.291.369,14	BS.195.784,98	BS.6.095.584,16
19	BS.6.095.584,16	BS.195.784,98	BS.5.899.799,18
20	BS.5.899.799,18	BS.195.784,98	BS.5.704.014,20
21	BS.5.704.014,20	BS.195.784,98	BS.5.508.229,22
22	BS.5.508.229,22	BS.195.784,98	BS.5.312.444,24
23	BS.5.312.444,24	BS.195.784,98	BS.5.116.659,26
24	BS.5.116.659,26	BS.195.784,98	BS.4.920.874,28
25	BS.4.920.874,28	BS.195.784,98	BS.4.725.089,30
26	BS.4.725.089,30	BS.195.784,98	BS.4.529.304,32
27	BS.4.529.304,32	BS.195.784,98	BS.4.333.519,34
28	BS.4.333.519,34	BS.195.784,98	BS.4.137.734,36

29	BS.4.137.734,36	BS.195.784,98	BS.3.941.949,38
30	BS.3.941.949,38	BS.195.784,98	BS.3.746.164,40
31	BS.3.746.164,40	BS.195.784,98	BS.3.550.379,42
32	BS.3.550.379,42	BS.195.784,98	BS.3.354.594,44
33	BS.3.354.594,44	BS.195.784,98	BS.3.158.809,46
34	BS.3.158.809,46	BS.195.784,98	BS.2.963.024,48
35	BS.2.963.024,48	BS.195.784,98	BS.2.767.239,50
36	BS.2.767.239,50	BS.195.784,98	BS.2.571.454,52
37	BS.2.571.454,52	BS.195.784,98	BS.2.375.669,54
38	BS.2.375.669,54	BS.195.784,98	BS.2.179.884,56
39	BS.2.179.884,56	BS.195.784,98	BS.1.984.099,58
40	BS.1.984.099,58	BS.195.784,98	BS.1.788.314,60
41	BS.1.788.314,60	BS.195.784,98	BS.1.592.529,62
42	BS.1.592.529,62	BS.195.784,98	BS.1.396.744,64
43	BS.1.396.744,64	BS.195.784,98	BS.1.200.959,66
44	BS.1.200.959,66	BS.195.784,98	BS.1.005.174,68
45	BS.1.005.174,68	BS.195.784,98	BS.809.389,70
46	BS.809.389,70	BS.195.784,98	BS.613.604,72
47	BS.613.604,72	BS.195.784,98	BS.417.819,74
48	BS.417.819,74	BS.195.784,98	BS.222.034,76
49	BS.222.034,76	BS.195.784,98	BS.26.249,78
50	BS.26.249,78	BS.195.784,98	-BS.169.535,20

Tabla 18: Reducción de costos de la propuesta 1.

Fuente: Autor

Al aplicar la propuesta 1, se verá reflejado la reducción de costos luego de 50 meses, es decir, se recupera la inversión realizada transcurrido este lapso de tiempo.

INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO	M	INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO
Bs.9.619.713,80		Bs.9.619.713,80	1		Bs.406.284,98	Bs.406.284,98
	Bs.210.500,00	Bs.9.830.213,80	2		Bs.406.284,98	Bs.812.569,96
	Bs.210.500,00	Bs.10.040.713,80	3		Bs.406.284,98	Bs.1.218.854,94
	Bs.210.500,00	Bs.10.251.213,80	4		Bs.406.284,98	Bs.1.625.139,92
	Bs.210.500,00	Bs.10.461.713,80	5		Bs.406.284,98	Bs.2.031.424,90
	Bs.210.500,00	Bs.10.672.213,80	6		Bs.406.284,98	Bs.2.437.709,88
	Bs.210.500,00	Bs.10.882.713,80	7		Bs.406.284,98	Bs.2.843.994,86
	Bs.210.500,00	Bs.11.093.213,80	8		Bs.406.284,98	Bs.3.250.279,84
	Bs.210.500,00	Bs.11.303.713,80	9		Bs.406.284,98	Bs.3.656.564,82
	Bs.210.500,00	Bs.11.514.213,80	10		Bs.406.284,98	Bs.4.062.849,80
	Bs.210.500,00	Bs.11.724.713,80	11		Bs.406.284,98	Bs.4.469.134,78
	Bs.210.500,00	Bs.11.935.213,80	12		Bs.406.284,98	Bs.4.875.419,76
	Bs.210.500,00	Bs.12.145.713,80	13		Bs.406.284,98	Bs.5.281.704,74
	Bs.210.500,00	Bs.12.356.213,80	14		Bs.406.284,98	Bs.5.687.989,72
	Bs.210.500,00	Bs.12.566.713,80	15		Bs.406.284,98	Bs.6.094.274,70
	Bs.210.500,00	Bs.12.777.213,80	16		Bs.406.284,98	Bs.6.500.559,68
	Bs.210.500,00	Bs.12.987.713,80	17		Bs.406.284,98	Bs.6.906.844,66
	Bs.210.500,00	Bs.13.198.213,80	18		Bs.406.284,98	Bs.7.313.129,64
	Bs.210.500,00	Bs.13.408.713,80	19		Bs.406.284,98	Bs.7.719.414,62
	Bs.210.500,00	Bs.13.619.213,80	20		Bs.406.284,98	Bs.8.125.699,60
	Bs.210.500,00	Bs.13.829.713,80	21		Bs.406.284,98	Bs.8.531.984,58
	Bs.210.500,00	Bs.14.040.213,80	22		Bs.406.284,98	Bs.8.938.269,56
	Bs.210.500,00	Bs.14.250.713,80	23		Bs.406.284,98	Bs.9.344.554,54
	Bs.210.500,00	Bs.14.461.213,80	24		Bs.406.284,98	Bs.9.750.839,52
	Bs.210.500,00	Bs.14.671.713,80	25		Bs.406.284,98	Bs.10.157.124,50
	Bs.210.500,00	Bs.14.882.213,80	26		Bs.406.284,98	Bs.10.563.409,48
	Bs.210.500,00	Bs.15.092.713,80	27		Bs.406.284,98	Bs.10.969.694,46
	Bs.210.500,00	Bs.15.303.213,80	28		Bs.406.284,98	Bs.11.375.979,44
	Bs.210.500,00	Bs.15.513.713,80	29		Bs.406.284,98	Bs.11.782.264,42
	Bs.210.500,00	Bs.15.724.213,80	30		Bs.406.284,98	Bs.12.188.549,40
	Bs.210.500,00	Bs.15.934.713,80	31		Bs.406.284,98	Bs.12.594.834,38
	Bs.210.500,00	Bs.16.145.213,80	32		Bs.406.284,98	Bs.13.001.119,36
	Bs.210.500,00	Bs.16.355.713,80	33		Bs.406.284,98	Bs.13.407.404,34
	Bs.210.500,00	Bs.16.566.213,80	34		Bs.406.284,98	Bs.13.813.689,32
	Bs.210.500,00	Bs.16.776.713,80	35		Bs.406.284,98	Bs.14.219.974,30
	Bs.210.500,00	Bs.16.987.213,80	36		Bs.406.284,98	Bs.14.626.259,28
	Bs.210.500,00	Bs.17.197.713,80	37		Bs.406.284,98	Bs.15.032.544,26
	Bs.210.500,00	Bs.17.408.213,80	38		Bs.406.284,98	Bs.15.438.829,24
	Bs.210.500,00	Bs.17.618.713,80	39		Bs.406.284,98	Bs.15.845.114,22
	Bs.210.500,00	Bs.17.829.213,80	40		Bs.406.284,98	Bs.16.251.399,20

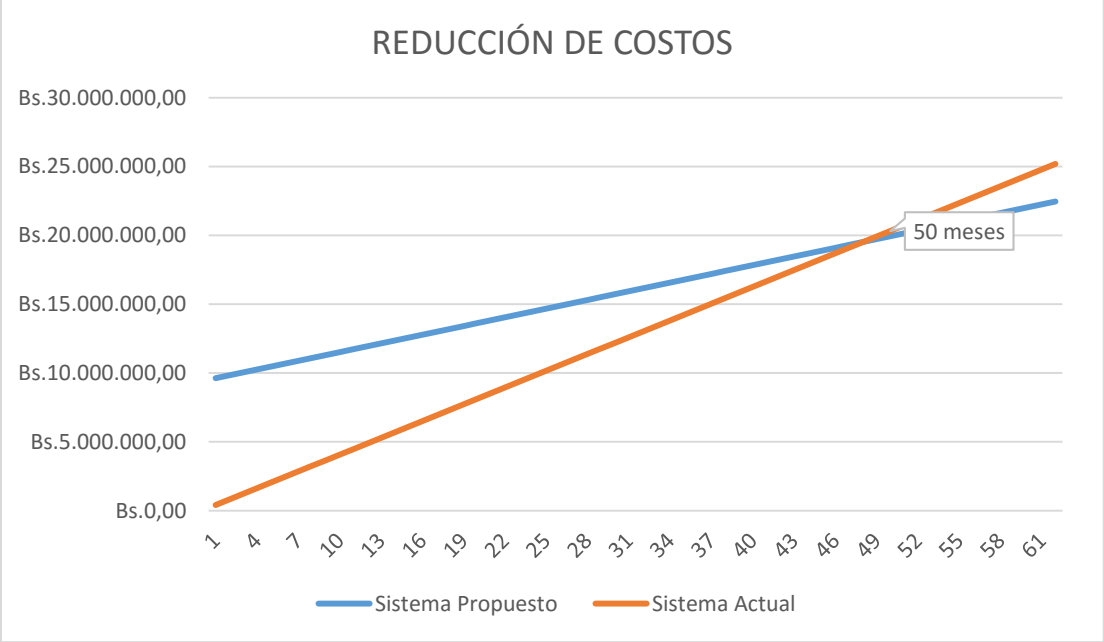
	Bs.210.500,00	Bs.18.039.713,80	41		Bs.406.284,98	Bs.16.657.684,18
	Bs.210.500,00	Bs.18.250.213,80	42		Bs.406.284,98	Bs.17.063.969,16
	Bs.210.500,00	Bs.18.460.713,80	43		Bs.406.284,98	Bs.17.470.254,14
	Bs.210.500,00	Bs.18.671.213,80	44		Bs.406.284,98	Bs.17.876.539,12
	Bs.210.500,00	Bs.18.881.713,80	45		Bs.406.284,98	Bs.18.282.824,10
	Bs.210.500,00	Bs.19.092.213,80	46		Bs.406.284,98	Bs.18.689.109,08
	Bs.210.500,00	Bs.19.302.713,80	47		Bs.406.284,98	Bs.19.095.394,06
	Bs.210.500,00	Bs.19.513.213,80	48		Bs.406.284,98	Bs.19.501.679,04
	Bs.210.500,00	Bs.19.723.713,80	49		Bs.406.284,98	Bs.19.907.964,02
	Bs.210.500,00	Bs.19.934.213,80	50		Bs.406.284,98	Bs.20.314.249,00
	Bs.210.500,00	Bs.20.144.713,80	51		Bs.406.284,98	Bs.20.720.533,98
	Bs.210.500,00	Bs.20.355.213,80	52		Bs.406.284,98	Bs.21.126.818,96
	Bs.210.500,00	Bs.20.565.713,80	53		Bs.406.284,98	Bs.21.533.103,94
	Bs.210.500,00	Bs.20.776.213,80	54		Bs.406.284,98	Bs.21.939.388,92
	Bs.210.500,00	Bs.20.986.713,80	55		Bs.406.284,98	Bs.22.345.673,90
	Bs.210.500,00	Bs.21.197.213,80	56		Bs.406.284,98	Bs.22.751.958,88
	Bs.210.500,00	Bs.21.407.713,80	57		Bs.406.284,98	Bs.23.158.243,86
	Bs.210.500,00	Bs.21.618.213,80	58		Bs.406.284,98	Bs.23.564.528,84
	Bs.210.500,00	Bs.21.828.713,80	59		Bs.406.284,98	Bs.23.970.813,82
	Bs.210.500,00	Bs.22.039.213,80	60		Bs.406.284,98	Bs.24.377.098,80
	Bs.210.500,00	Bs.22.249.713,80	61		Bs.406.284,98	Bs.24.783.383,78
	Bs.210.500,00	Bs.22.460.213,80	62		Bs.406.284,98	Bs.25.189.668,76

Tabla 19: Reducción de costos de la propuesta 1.

Fuente: Autor

Como se pueden observar en las tablas, el punto en que se amortiza la inversión del proyecto es a partir de los 50 meses, cabe acotar que el análisis no contempla ningún interés, inflación y aumento del salario de los empleados.

Como se pueden observar en las tablas, el punto en que se amortiza la inversión del proyecto es a partir de los 50 meses, cabe acotar que el análisis no contempla ningún interés, inflación y aumento del salario de los empleados.



Gráfica 5: Reducción de costos de la propuesta 1.

Fuente: Autor

Se expresa gráficamente la inversión necesaria para implementar el sistema propuesto mientras que para el sistema actual no se necesita inversión inicial alguna ya que este se encuentra implementado, sin embargo luego de 50 meses se retorna la inversión, es decir, es cuando se podrán apreciar la disminución de gastos luego de implementar el sistema propuesto.

- **PROPUESTA 2, EQUIPO BIOMÉTRICO SUPREMA BIOENTRY W**

REDUCCIÓN DE COSTOS			
Mes	Inversión Inicial	Beneficio Mensual	Acumulado
1	Bs.5.419.689,60	Bs.195.784,98	Bs.5.223.904,62
2	Bs.5.223.904,62	Bs.195.784,98	Bs.5.028.119,64
3	Bs.5.028.119,64	Bs.195.784,98	Bs.4.832.334,66
4	Bs.4.832.334,66	Bs.195.784,98	Bs.4.636.549,68
5	Bs.4.636.549,68	Bs.195.784,98	Bs.4.440.764,70
6	Bs.4.440.764,70	Bs.195.784,98	Bs.4.244.979,72
7	Bs.4.244.979,72	Bs.195.784,98	Bs.4.049.194,74
8	Bs.4.049.194,74	Bs.195.784,98	Bs.3.853.409,76
9	Bs.3.853.409,76	Bs.195.784,98	Bs.3.657.624,78
10	Bs.3.657.624,78	Bs.195.784,98	Bs.3.461.839,80
11	Bs.3.461.839,80	Bs.195.784,98	Bs.3.266.054,82
12	Bs.3.266.054,82	Bs.195.784,98	Bs.3.070.269,84
13	Bs.3.070.269,84	Bs.195.784,98	Bs.2.874.484,86
14	Bs.2.874.484,86	Bs.195.784,98	Bs.2.678.699,88
15	Bs.2.678.699,88	Bs.195.784,98	Bs.2.482.914,90
16	Bs.2.482.914,90	Bs.195.784,98	Bs.2.287.129,92
17	Bs.2.287.129,92	Bs.195.784,98	Bs.2.091.344,94
18	Bs.2.091.344,94	Bs.195.784,98	Bs.1.895.559,96
19	Bs.1.895.559,96	Bs.195.784,98	Bs.1.699.774,98
20	Bs.1.699.774,98	Bs.195.784,98	Bs.1.503.990,00
21	Bs.1.503.990,00	Bs.195.784,98	Bs.1.308.205,02
22	Bs.1.308.205,02	Bs.195.784,98	Bs.1.112.420,04
23	Bs.1.112.420,04	Bs.195.784,98	Bs.916.635,06
24	Bs.916.635,06	Bs.195.784,98	Bs.720.850,08
25	Bs.720.850,08	Bs.195.784,98	Bs.525.065,10
26	Bs.525.065,10	Bs.195.784,98	Bs.329.280,12
27	Bs.329.280,12	Bs.195.784,98	Bs.133.495,14
28	Bs.133.495,14	Bs.195.784,98	-Bs.62.289,84

Tabla 20: Reducción de costos de la propuesta 2.

Fuente: Autor

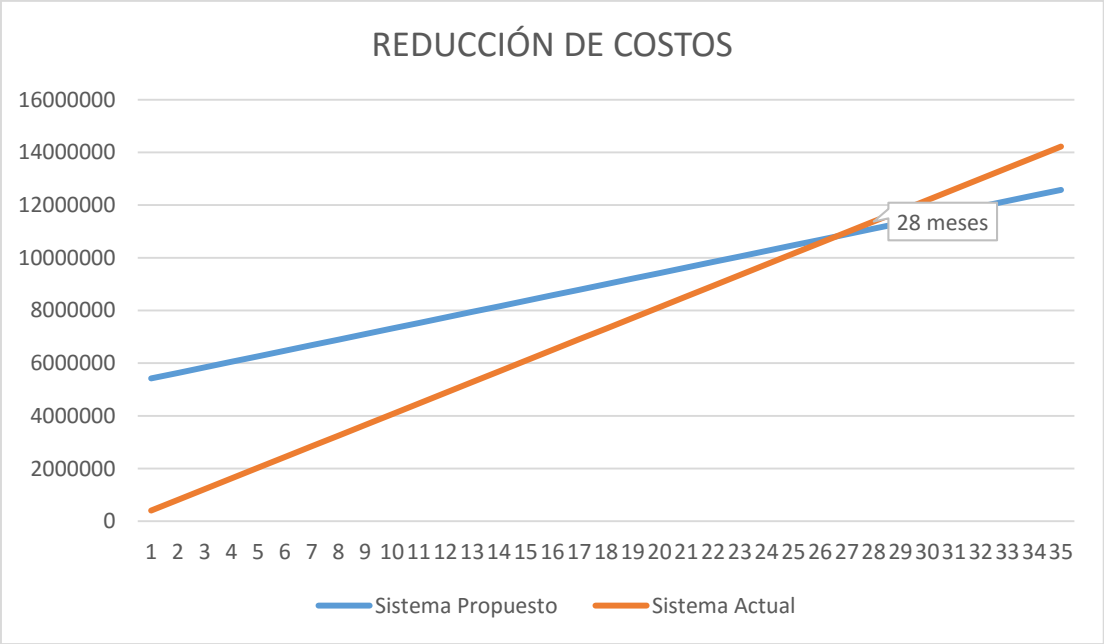
Al trabajar la propuesta 2, se verá reflejado la reducción de costos luego de 28 meses, es decir, se recupera la inversión realizada transcurrido este lapso de tiempo.

INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO	M	INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO
Bs.5.419.689,60		Bs.5.419.689,60	1		Bs.406.284,98	Bs.406.284,98
	Bs.210.500,00	Bs.5.630.189,60	2		Bs.406.284,98	Bs.812.569,96
	Bs.210.500,00	Bs.5.840.689,60	3		Bs.406.284,98	Bs.1.218.854,94
	Bs.210.500,00	Bs.6.051.189,60	4		Bs.406.284,98	Bs.1.625.139,92
	Bs.210.500,00	Bs.6.261.689,60	5		Bs.406.284,98	Bs.2.031.424,90
	Bs.210.500,00	Bs.6.472.189,60	6		Bs.406.284,98	Bs.2.437.709,88
	Bs.210.500,00	Bs.6.682.689,60	7		Bs.406.284,98	Bs.2.843.994,86
	Bs.210.500,00	Bs.6.893.189,60	8		Bs.406.284,98	Bs.3.250.279,84
	Bs.210.500,00	Bs.7.103.689,60	9		Bs.406.284,98	Bs.3.656.564,82
	Bs.210.500,00	Bs.7.314.189,60	10		Bs.406.284,98	Bs.4.062.849,80
	Bs.210.500,00	Bs.7.524.689,60	11		Bs.406.284,98	Bs.4.469.134,78
	Bs.210.500,00	Bs.7.735.189,60	12		Bs.406.284,98	Bs.4.875.419,76
	Bs.210.500,00	Bs.7.945.689,60	13		Bs.406.284,98	Bs.5.281.704,74
	Bs.210.500,00	Bs.8.156.189,60	14		Bs.406.284,98	Bs.5.687.989,72
	Bs.210.500,00	Bs.8.366.689,60	15		Bs.406.284,98	Bs.6.094.274,70
	Bs.210.500,00	Bs.8.577.189,60	16		Bs.406.284,98	Bs.6.500.559,68
	Bs.210.500,00	Bs.8.787.689,60	17		Bs.406.284,98	Bs.6.906.844,66
	Bs.210.500,00	Bs.8.998.189,60	18		Bs.406.284,98	Bs.7.313.129,64
	Bs.210.500,00	Bs.9.208.689,60	19		Bs.406.284,98	Bs.7.719.414,62
	Bs.210.500,00	Bs.9.419.189,60	20		Bs.406.284,98	Bs.8.125.699,60
	Bs.210.500,00	Bs.9.629.689,60	21		Bs.406.284,98	Bs.8.531.984,58
	Bs.210.500,00	Bs.9.840.189,60	22		Bs.406.284,98	Bs.8.938.269,56
	Bs.210.500,00	Bs.10.050.689,60	23		Bs.406.284,98	Bs.9.344.554,54
	Bs.210.500,00	Bs.10.261.189,60	24		Bs.406.284,98	Bs.9.750.839,52
	Bs.210.500,00	Bs.10.471.689,60	25		Bs.406.284,98	Bs.10.157.124,50
	Bs.210.500,00	Bs.10.682.189,60	26		Bs.406.284,98	Bs.10.563.409,48
	Bs.210.500,00	Bs.10.892.689,60	27		Bs.406.284,98	Bs.10.969.694,46
	Bs.210.500,00	Bs.11.103.189,60	28		Bs.406.284,98	Bs.11.375.979,44
	Bs.210.500,00	Bs.11.313.689,60	29		Bs.406.284,98	Bs.11.782.264,42
	Bs.210.500,00	Bs.11.524.189,60	30		Bs.406.284,98	Bs.12.188.549,40
	Bs.210.500,00	Bs.11.734.689,60	31		Bs.406.284,98	Bs.12.594.834,38

Tabla 21: Reducción de costos de la propuesta 2.

Fuente: Autor

Tomando en cuenta la propuesta 2, se debe realizar una inversión inicial de 5.419.689,60BsF y transcurridos 28 meses se obtendrá la reducción de costos.



Gráfica 6: Reducción de costos de la propuesta 2.

Fuente: Autor

Como se puede observar en las tablas y en la gráfica, el punto en que se amortiza el proyecto es a los 28 meses, cabe acotar que el análisis no contempla ningún interés, inflación o aumento del salario de los empleados.

- **PROPUESTA 3, EQUIPO BIOMÉTRICO SUPREMA BIOENTRY PLUS.**

REDUCCIÓN DE COSTOS			
MES	INVERSIÓN INICIAL	BENEFICIO MENSUAL	ACUMULADO
1	Bs.5.035.997,00	Bs.195.784,98	Bs.4.840.212,02
2	Bs.4.840.212,02	Bs.195.784,98	Bs.4.644.427,04
3	Bs.4.644.427,04	Bs.195.784,98	Bs.4.448.642,06
4	Bs.4.448.642,06	Bs.195.784,98	Bs.4.252.857,08
5	Bs.4.252.857,08	Bs.195.784,98	Bs.4.057.072,10
6	Bs.4.057.072,10	Bs.195.784,98	Bs.3.861.287,12
7	Bs.3.861.287,12	Bs.195.784,98	Bs.3.665.502,14
8	Bs.3.665.502,14	Bs.195.784,98	Bs.3.469.717,16
9	Bs.3.469.717,16	Bs.195.784,98	Bs.3.273.932,18
10	Bs.3.273.932,18	Bs.195.784,98	Bs.3.078.147,20
11	Bs.3.078.147,20	Bs.195.784,98	Bs.2.882.362,22
12	Bs.2.882.362,22	Bs.195.784,98	Bs.2.686.577,24
13	Bs.2.686.577,24	Bs.195.784,98	Bs.2.490.792,26
14	Bs.2.490.792,26	Bs.195.784,98	Bs.2.295.007,28
15	Bs.2.295.007,28	Bs.195.784,98	Bs.2.099.222,30
16	Bs.2.099.222,30	Bs.195.784,98	Bs.1.903.437,32
17	Bs.1.903.437,32	Bs.195.784,98	Bs.1.707.652,34
18	Bs.1.707.652,34	Bs.195.784,98	Bs.1.511.867,36
19	Bs.1.511.867,36	Bs.195.784,98	Bs.1.316.082,38
20	Bs.1.316.082,38	Bs.195.784,98	Bs.1.120.297,40
21	Bs.1.120.297,40	Bs.195.784,98	Bs.924.512,42
22	Bs.924.512,42	Bs.195.784,98	Bs.728.727,44
23	Bs.728.727,44	Bs.195.784,98	Bs.532.942,46
24	Bs.532.942,46	Bs.195.784,98	Bs.337.157,48
25	Bs.337.157,48	Bs.195.784,98	Bs.141.372,50
26	Bs.141.372,50	Bs.195.784,98	-Bs.54.412,48

Tabla 22: Reducción de costos de la propuesta 3.

Fuente: Autor

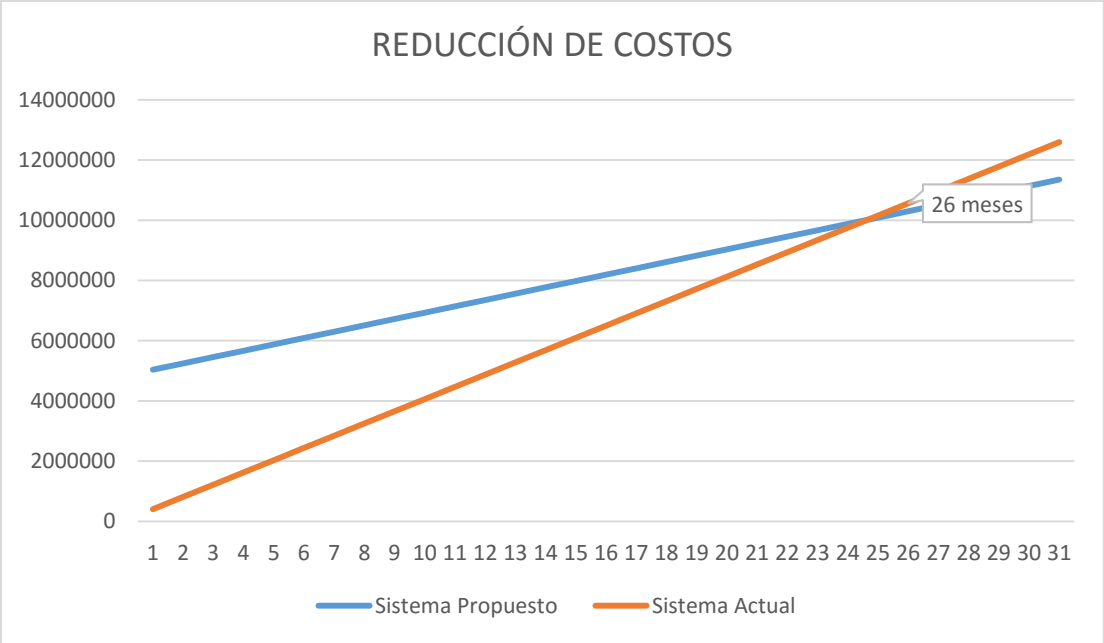
Empleando la propuesta 2, se obtendrá la reducción de costos transcurrido 26 meses.

INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO	M	INVERSIÓN	COSTOS DE OPERACIÓN	ACUMULADO
Bs.5.035.997,00		Bs.5.035.997,00	1		Bs.406.284,98	Bs.406.284,98
	Bs.210.500,00	Bs.5.246.497,00	2		Bs.406.284,98	Bs.812.569,96
	Bs.210.500,00	Bs.5.456.997,00	3		Bs.406.284,98	Bs.1.218.854,94
	Bs.210.500,00	Bs.5.667.497,00	4		Bs.406.284,98	Bs.1.625.139,92
	Bs.210.500,00	Bs.5.877.997,00	5		Bs.406.284,98	Bs.2.031.424,90
	Bs.210.500,00	Bs.6.088.497,00	6		Bs.406.284,98	Bs.2.437.709,88
	Bs.210.500,00	Bs.6.298.997,00	7		Bs.406.284,98	Bs.2.843.994,86
	Bs.210.500,00	Bs.6.509.497,00	8		Bs.406.284,98	Bs.3.250.279,84
	Bs.210.500,00	Bs.6.719.997,00	9		Bs.406.284,98	Bs.3.656.564,82
	Bs.210.500,00	Bs.6.930.497,00	10		Bs.406.284,98	Bs.4.062.849,80
	Bs.210.500,00	Bs.7.140.997,00	11		Bs.406.284,98	Bs.4.469.134,78
	Bs.210.500,00	Bs.7.351.497,00	12		Bs.406.284,98	Bs.4.875.419,76
	Bs.210.500,00	Bs.7.561.997,00	13		Bs.406.284,98	Bs.5.281.704,74
	Bs.210.500,00	Bs.7.772.497,00	14		Bs.406.284,98	Bs.5.687.989,72
	Bs.210.500,00	Bs.7.982.997,00	15		Bs.406.284,98	Bs.6.094.274,70
	Bs.210.500,00	Bs.8.193.497,00	16		Bs.406.284,98	Bs.6.500.559,68
	Bs.210.500,00	Bs.8.403.997,00	17		Bs.406.284,98	Bs.6.906.844,66
	Bs.210.500,00	Bs.8.614.497,00	18		Bs.406.284,98	Bs.7.313.129,64
	Bs.210.500,00	Bs.8.824.997,00	19		Bs.406.284,98	Bs.7.719.414,62
	Bs.210.500,00	Bs.9.035.497,00	20		Bs.406.284,98	Bs.8.125.699,60
	Bs.210.500,00	Bs.9.245.997,00	21		Bs.406.284,98	Bs.8.531.984,58
	Bs.210.500,00	Bs.9.456.497,00	22		Bs.406.284,98	Bs.8.938.269,56
	Bs.210.500,00	Bs.9.666.997,00	23		Bs.406.284,98	Bs.9.344.554,54
	Bs.210.500,00	Bs.9.877.497,00	24		Bs.406.284,98	Bs.9.750.839,52
	Bs.210.500,00	Bs.10.087.997,00	25		Bs.406.284,98	Bs.10.157.124,50
	Bs.210.500,00	Bs.10.298.497,00	26		Bs.406.284,98	Bs.10.563.409,48
	Bs.210.500,00	Bs.10.508.997,00	27		Bs.406.284,98	Bs.10.969.694,46
	Bs.210.500,00	Bs.10.719.497,00	28		Bs.406.284,98	Bs.11.375.979,44
	Bs.210.500,00	Bs.10.929.997,00	29		Bs.406.284,98	Bs.11.782.264,42
	Bs.210.500,00	Bs.11.140.497,00	30		Bs.406.284,98	Bs.12.188.549,40
	Bs.210.500,00	Bs.11.350.997,00	31		Bs.406.284,98	Bs.12.594.834,38

Tabla 23: Reducción de costos de la propuesta 3.

Fuente: Autor

Al ejecutar la propuesta 3, siendo esta la más económica la cual requiere una inversión inicial de 5.035.997BsF se podrá obtener la reducción de costos luego de 26 meses.



Gráfica 7: Reducción de costos de la propuesta 3.

Fuente: Autor

Basado en las tablas y en la gráfica, se demostró que el punto en que se amortiza el proyecto es a los 26 meses, demostrando que el sistema propuesto es rentable en comparación con el sistema actual; cabe acotar que el análisis no contempla ningún interés, inflación o aumento del salario de los empleados.

El estudio de Factibilidades permitió concluir que el desarrollo y la implementación del diseño del sistema planteado lograrán un incremento considerable en la eficiencia y eficacia en los procesos para el control de entrada y salida de personal y elaboración de planilla del área de producción en el beneficiado de café, de la zona occidental de El Salvador.

Basado en los estudios de factibilidad económica, se determinó que el uso de las tarjetas RFID es un sistema costoso, por lo que se propone el uso de sistema biométrico de huella dactilar. Se realizó un diagrama de proceso propuesto bajo la aplicación de dicho método. Se recomienda que la huella dactilar del personal contratista sea registrada y activada por el periodo que dure el contrato, evitando así demoras innecesarias en la reactivación diaria o semanal.

Diagrama: De proceso.

Proceso: Identificación y control de acceso al personal a la empresa CVG Bauxilum.

Inicio: Llega al portón 1.

Fin: Pasa a la empresa.

Fecha: 09/10/2015.

Método: Propuesto.

Seguimiento: Al personal fijo, contratado y contratista.

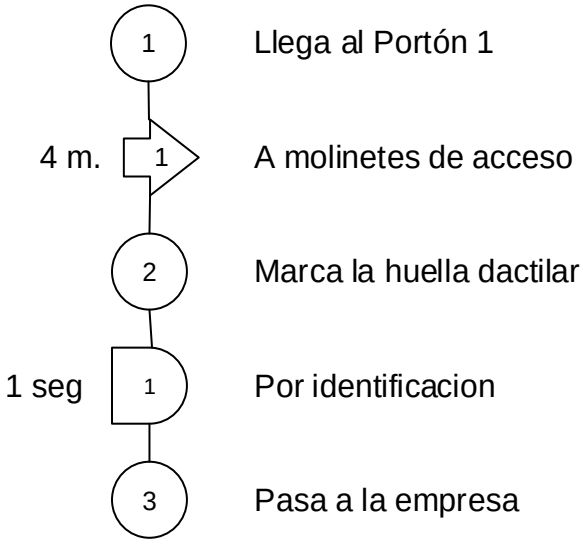
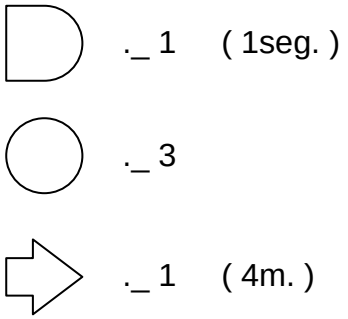


Figura 5.14: Diagrama de procesos propuesto para la identificación y acceso del personal fijo, contratado y contratista

Fuente: Autor

Resumen:



Total : 5

Figura 5.15: Resumen de diagrama de proceso propuesto para la identificación y acceso del personal fijo, contratado y contratista.

Fuente: Autor

MATRIZ FODA

Como se puede observar en la Tabla 24, La Matriz FODA está compuesta por cuatro componentes claves: fortalezas, oportunidades, debilidades, y amenazas. Las fortalezas y debilidades son los factores internos sobre los cuales la industria del envase tiene control y puede influir, mientras que las oportunidades y amenazas son los factores externos que la industria del envase no puede controlar. Estos luego se unen para crear cuatro grupos adicionales los cuales: (a) los FO, se tienen que explotar; (b) los DO, se tienen que buscar; (c) los FA, se deben confrontar; y (d) los DA, se deben evitar.

Esta matriz es fundamental para poder desarrollar todas las estrategias posibles que se desprenden de los factores externos e internos, y que finalmente permitirán alcanzar los objetivos a largo plazo trazados.

- **FORTALEZAS.**
    - Disponibilidad para instalar un sistema de control de acceso biométrico.
    - Base de datos centralizadas
    - Software y Hardware con tecnología de punta
    - Conexión cifrada desde el lector hasta el servidor.
    - Alta seguridad en el acceso de personal.
    - Reducción de costos frente a otras tecnologías.
    - Información oportuna y veraz.
    - Adecuada infraestructura tecnológica.

- **OPORTUNIDADES.**
  - Poder adquisitivo.
  - Disponibilidad de las tecnologías en el país.
  - Posibilidad de actualizar complementar el software por el SDK y el API del hardware.
  - Viabilidad de instalar equipos lectores adicionales en modo red y en modo autónomos.
- **DEBILIDADES.**
  - Mal uso por parte de los usuarios, sin embargo se puede contrarrestar este efecto mediante información y capacitación.
  - Tasa de falsos positivo y falsos negativo, por captura ineficiente en el registro
- **AMENAZAS.**
  - Capacitación del personal para el manejo del software
  - Posibles incidentes y eventuales fallas en el suministro eléctrico.

Diseño de sistema automatizado biométrico mediante el uso de huella dactilar para el control de acceso	Fortalezas: • Disponibilidad para instalar un sistema de control de acceso biométrico. • Base de datos centralizadas • Software y Hardware con tecnología de punta • Conexión cifrada desde el lector hasta el servidor. • Alta seguridad en el acceso de personal. • Reducción de costos frente a otras tecnologías. • Información oportuna y veraz. • Adecuada infraestructura tecnológica.	Debilidades: • Mal uso por parte de los usuarios, sin embargo se puede contrarrestar este efecto mediante información y capacitación. • Tasa de falsos positivo y falsos negativo, por captura ineficiente en el registro
Oportunidades: • Poder adquisitivo. • Disponibilidad de las tecnologías en el país. • Posibilidad de actualizar complementar el software por el SDK y el API del hardware. • Viabilidad de instalar equipos lectores adicionales en modo red y en modo autónomos.	FO: • Solicitar recursos financieros para la modernización del sistema de control de acceso. • Integración de aplicaciones desarrolladas por la empresa con el sistema biométrico mediante el SDK y la base de datos. • Mediante la disponibilidad en el mercado nacional, la implantación es rápida y eficiente, además de tener garantía inmediata.	DO: • Fortalecer el registro de datos del personal. • Establecer aplicaciones desarrolladas por la empresa y optimizar el algoritmo de los equipos.
Amenazas: • Capacitación del personal para el manejo del software • Posibles incidentes y eventuales fallas en el suministro eléctrico.	FA: • Impulsar mediante intranet, los beneficios del sistema biométrico y la seguridad de acceso a la planta • Aprovechar la implantación del sistema, para instalar un sistema redundante de energía eléctrica (UPS).	DA: • Capacitar al personal para evitar un mal uso de los dispositivos. • Instalar equipos UPS para evitar posibles pérdidas. • Capacitar al personal que laborara con el sistema para evitar falsos positivos y negativos.

Tabla 24: Matriz FODA.

Fuente: Autor

ESTRATEGIAS DERIVADAS DEL ANÁLISIS FODA

Las estrategias derivadas del análisis FODA van enfocada a explotar las fortalezas y aprovechar las oportunidades, así como superar las debilidades y afrontar las amenazas.

- Estrategias de Fortalezas – Oportunidades.
  - Solicitar recursos financieros para la modernización del sistema de control de acceso.
  - Integración de aplicaciones desarrolladas por la empresa con el sistema biométrico mediante el SDK y la base de datos.
  - Mediante la disponibilidad en el mercado nacional, la implantación es rápida y eficiente, además de tener garantía inmediata
- Estrategia Debilidad – Oportunidad
  - Fortalecer el registro de datos del personal.
  - Establecer aplicaciones desarrolladas por la empresa y optimizar el algoritmo de los equipos.
- Estrategia Fortaleza – Amenaza
  - Impulsar mediante intranet, los beneficios del sistema biométrico y la seguridad de acceso a la planta
  - Aprovechar la implantación del sistema, para instalar un sistema redundante de energía eléctrica (UPS)
- Estrategia Debilidad – Amenaza
  - Capacitar al personal para evitar un mal uso de los dispositivos.
  - Instalar equipos UPS para evitar posibles pérdidas.
  - Capacitar al personal que laborara con el sistema para evitar falsos positivos y negativos.

CONCLUSIONES

Los resultados obtenidos permiten concluir con los siguientes aspectos:

1. Se diagnosticó con éxito las fallas que presentan el actual sistema, las consecuencias que genera de dar pases manuales que van desde los gastos excesivos de papelería, falsificaciones, ingresar a áreas no autorizadas.
2. Se determinó que en la actualidad existen once sistemas de identificación disponibles en el mercado nacional, optando como mejor alternativa los sistemas biométricos que gozan un lugar importante en una variedad de aplicaciones que resuelven distintos tipos de problemas como el control de acceso.
3. Se pudo conocer que debido al avance tecnológico y el empuje del mercado, el desarrollo de nuevos componentes y sensores capaces de detectar nuevas características fisiológicas así como el desarrollo de nuevos modelos de identificación y clasificación de rasgos del comportamiento, hacen que el uso de la biometría se presente como una de las mejores opciones para reconocer y autenticar usuarios gracias a que la validación la realiza utilizando características inherentes al mismo.
4. Mediante la recopilación de información, se pudo observar que el personal que labora en la División Identificación y Control de Acceso, se encuentra motivado por el diseño del nuevo sistema de identificación, demostrando interés por el mismo.
5. El estudio de Factibilidades permitió concluir que el desarrollo y la implementación del diseño del sistema planteado lograrán un

incremento considerable en la eficiencia y eficacia en los procesos para el control de entrada y salida de personal.

6. Se pudo evidenciar que a partir de 26 meses la empresa obtendrá un beneficio mensual de 195.784,98BsF al implementar la propuesta 3 del sistema diseñado, demostrando así que se reducirán considerablemente los costos en la división.

RECOMENDACIONES

A continuación se ha recogido un conjunto de consejos y recomendaciones para la investigación, implantación y uso de las tecnologías biométricas así como para su regulación:

1. Desarrollar e implementar el diseño del sistema automatizado de control de acceso biométrico en CVG Bauxilum.
2. Realizar la migración del sistema RFID al sistema biométrico por fases: 1) Contratistas, 2) Visitantes, 3) Pasantes y por ultimo Personal fijo.
3. Registrar y activar la huella dactilar del personal contratista una única vez durante el periodo que dure el contrato, evitando así demoras innecesarias en la reactivación diaria o semanal.
4. Capacitar al personal encargado de utilizar el software, sobre el uso correcto del sistema, para aprovechar al máximo todas sus virtudes.
5. Enviar información haciendo uso del correo interno y de la página web, que indiquen la migración al sistema biométrico dactilar, sus ventajas y beneficios así como el procedimiento para hacer uso del mismo.
6. Realizar mantenimiento preventivo al sistema según sea lo indicado por el fabricante para evitar los daños del mismo y prolongar la vida útil de los equipos.
7. Recomendar al responsable de cada cuadrilla llevar un control estricto sobre el cumplimiento del horario de cada personal a cargo, tomando en cuenta las horas de entrada y salida generadas por el sistema biométrico de identidad.

BIBLIOGRAFÍA

- Arias, F (2006). El proyecto de la investigación. Caracas, Venezuela: Editorial Episternal. Quinta Edición.

- Castellano, B. Hercilio y Vadell, Hermano (1990). El Oficio del Planificador. Caracas, Venezuela.

- Deborah Russell & G.T. Gangemi (1991). Computer Security Basics. Clif. O'Reilly & Associates, Sebastopol, Russia.

- Kerlinger, Fred N. (1997), Investigación del Comportamiento, edito Mc Graw Hill 3ra ed., México.

- Narváez, R (1997). Orientaciones Prácticas para la elaboración de informe de investigación. U.N.E.X.P.O Puerto Ordaz, Venezuela.

- Ruiz Olabuenaga, J.I. e Ispizua (1989). La descodificación de la vida cotidiana: Publicaciones de la Universidad de Deusto. , M.A. (Ed.). Bilbao

- Sabino, C (1992). El proceso de la investigación. Editorial Panapo. Caracas, Venezuela.

- Santa Palella y Feliberto Martins (2010), “Metodología de la Investigación Cuantitativa”, edit. Fedupel. 2da edición. Caracas, Venezuela.

- Tamayo y Tamayo, M (2003). “El proceso de la investigación científica". Editorial Limusa. Cuarta Edición. México

- Venegas, Pedro (2006). Planificación educativa: bases metodológicas para su desarrollo en el siglo XXI. San José, Costa Rica.

- Weiss (1980), La Investigación Evaluativa. México: Trillas.

INFOGRAFÍA

- Kimaldi. Biometría e identificación de personas. 2008. Consultado el (14/09/2015) de: http://www.kimaldi.com.

- Silvestre, Katz. “How to cite a Internet source”. Ehow.com. 2011. Consultado el (14/09/2015) de: www.ehow.com/how_4481180_cite-internet-source.html.

- Silvestre, Katz. “How to cite a Internet source”. Ehow.com. 8/2010. 25 de febrero de 2011. Consultado el (14/09/2015) de: www.ehow.com/how_4481180_cite-internet-source.html.

- TEC Electrónica, S.A. Lectores de huella digital. de C.V. Consultado el (15/09/2015) de: http://www.tecmex.com.mx/promos/bit/bit0903-bio.html

- Reconocimiento de voz. Universidad de las Américas Puebla, México. Consultado el (15/09/2015) de: http://ict.udlap.mx/people/ingrid/Clases/IS412/index.html

- Reconocimiento facial: enfoques predominantes. Ministerio Interior de Argentina. Consultado el (16/09/2015) de: http://www.biometria.gov.ar/referencia/ref_rf_approaches.php

- OLGUÍN S, Patricio. Sensores Biométricos. Revista de la escuela de Electrónica. Consultado el (16/09/2015) de: http://neutron.ing.ucv.ve/revista-e/No6/default.htm

- Reconocimiento de voz. Universidad de las Américas Puebla, México. Consultado el (16/09/2015) de: http://ict.udlap.mx/people/ingrid/Clases/IS412/index.html

- Reconocimiento facial: enfoques predominantes. Ministerio Interior de Argentina. Consultado el (16/09/2015) de: http://www.biometria.gov.ar/referencia/ref_rf_approaches.php

- Sistemas biométricos: Matching de huellas dactilares mediante transformada de Hough generalizada. Consultado el (16/09/2015) de: http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

ANEXOS

ANEXO 1

Manual de Normas y Procedimientos

Identificación y Acceso a las Instalaciones de

C.V.G. BAUXILUM, C.A.

Código 03.01.01

Título	Código
Identificación y Acceso a las Instalaciones de CVG BAUXILUM, C.A.	03.01.01

Contenido

I. Objetivo

Establecer las normas y procedimientos para la identificación y acceso de trabajadores, contratistas, visitantes y vehículos a las instalaciones de CVG BAUXILUM, C.A.

II. Funciones

- Identificación en la Empresa
- Acceso a las instalaciones de la Empresa

III. Unidades Responsables

- Gerencia Seguridad Patrimonial
  - División Protección de Planta Alúmina
  - División Protección de Planta Bauxita

IV. Formularios Utilizados

- SG-074 "Solicitud Carnet de Identificación"
- SG-055 "Solicitud Pase para Vehículo"
- SG-123 "Solicitud Acceso Vehículo de Contratista"
- SG-118 "Solicitud de Acceso a Personal Contratista"
- SG-023 "Registro Individual de Personal Contratista"
- RH-062 "Autorización para Asignación y/o Deducción"

V. Normas

A. Generales

1. La identificación y acceso de trabajadores, contratistas y visitantes a las instalaciones de CVG BAUXILUM, C.A., debe ser controlado a través del Sistema Integrado de Seguridad Patrimonial (SISP).

2. La División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, debe entregar el carnet de identificación a trabajadores, contratistas y visitantes, así como la calcomanía o pase de vehículo, previa presentación de los documentos soportes respectivos.

3. El acceso y tránsito de trabajadores, contratistas, visitantes por las dependencias de la Empresa, está regulado por el uso y porte del carnet de identificación en sitio

visible (a nivel de tórax) y pase o calcomanía en el vehículo, si fuere el caso, y deben transitar sólo por el área autorizada.

B. De la Identificación del Trabajador

4. La División Empleo y Compensación o Coordinación Recursos Humanos, según corresponda, debe:

   4.1. Solicitar a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, la emisión del carnet de identificación, en caso de ingreso o variación en los datos del trabajador (tipo de nómina, unidad de adscripción, cargo, entre otros), tal como lo establecen las normas y procedimientos "Ingreso de Personal" y "Movimiento de Personal".

   4.2. Informar al trabajador la actualización del carnet de identificación cuando exista variación de información.

5. La División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, debe emitir el carnet de identificación para los trabajadores el cual contiene información relacionada a la Gerencia de adscripción, cargo actual, apellidos y nombres, número de personal, tipo de sangre, número de la cédula de identidad, foto actual, tipo de nómina y áreas permitidas, de acuerdo a:

   a) Fondo

Fondo	*Tipo de Nómina*
Blanco	Gerencial
Rojo	Ejecutiva
Amarillo	Mensual Mayor
Verde	Diaria y Mensual Menor

   b) Barras de Acceso

Barras de Acceso	*Áreas Permitidas en la Empresa*
Amarillo	Todas
Azul	Muelle, Industrial, Administrativa y Campamento
Rojo	Industrial, Administrativa y Campamento
Verde	Administrativa y Campamento

6. Las barras de acceso deben ser asignadas de acuerdo a las siguientes condiciones:

   - La nómina mensual y diaria tienen acceso al área donde se desempeñan; a excepción de aquellos cargos que por naturaleza de las funciones y por facultad de la gerencia de adscripción, deben tener acceso a otras áreas.
   - La nómina gerencial y ejecutiva tienen acceso a todas las áreas de la Empresa.

7. El acceso al muelle debe ser autorizado por la División Empleo y Compensación en los casos de ingreso del trabajador, previa notificación del Supervisor y en función a la asignación permanente o temporal por la unidad de adscripción o del Supervisor inmediato del trabajador.

8. El trabajador en caso de pérdida del carnet de identificación, debe solicitar la reposición mediante una comunicación por escrito a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, cuyo costo se establece de acuerdo a los materiales utilizados y descontado según tipo de nómina:

   - Nómina gerencial, ejecutiva y mensual mayor, en una (1) cuota.
   - Nómina diaria y mensual menor, en dos (2) cuotas.

9. En caso de renovación del carnet de identificación, el trabajador debe notificar a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, la emisión de un nuevo carnet de identificación y devolver el carnet deteriorado.

10. El trabajador al finalizar su relación laboral con la Empresa, debe devolver el Carnet de Identificación a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, y solicitar el formulario "Solvencia" donde indique la devolución del mismo, tal como está previsto en la norma y procedimiento "Terminación de Servicios del Trabajador".

C. De la Identificación del Contratista

11. El acceso a la Empresa del personal de contratistas debe ser tramitado ante la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, a solicitud del representante del contratista, a través del formulario "Solicitud de Acceso Personal Contratista", acompañado de copia del Documento Contractual y los siguientes anexos por cada trabajador:

- RH-023 "Registro Individual de Personal Contratista".
- Dos (2) fotografías tipo carnet.
- Copia de la Planilla 14-02 del Instituto Venezolano de los Seguros Sociales (IVSS) o última tarjeta de servicio del trabajador.
- Copia de la cédula de identidad, en caso de portar comprobante, anexar fotocopia de la partida de nacimiento.
- Planilla de Postulación del Sindicato, para aquellos trabajos conexos o inherentes al proceso productivo.
- Examen Médico Laboral (externo), cuando el contrato sea mayor o igual a un (1) mes.

12. El carnet de identificación para el personal contratista tiene un costo establecido por la Empresa en función a los materiales utilizados y debe ser cancelado por el representante de la empresa contratista ante la División Tesorería o División Finanzas Bauxita, tal como se establece en la norma y procedimiento "Ingreso a Caja – Depósitos Bancarios".

13. La renovación del carnet de identificación, en caso de prórroga en la ejecución del trabajo, debe ser solicitado por la unidad responsable del servicio contratado ante la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, con tres (3) días de antelación a la fecha de vencimiento, cumpliendo con los requisitos exigidos en la norma nro. 11 de la presente norma y procedimiento.

14. En caso de culminación de los trabajos contratados o cuando ocurran despidos o desincorporación de trabajadores contratistas antes de la fecha de vencimiento del contrato, el representante de la empresa contratista debe devolver el carnet de identificación a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, a fin de actualizar los registros en el Sistema Integrado de Seguridad Patrimonial (SISP).

15. La unidad responsable de los trabajos contratados, debe informar a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, la culminación de trabajos, despidos o desincorporación de trabajadores contratistas a fin de ser invalidados y mantener actualizado el listado de personal autorizado.

D. De la Identificación del Visitante

16. La División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, debe:

    16.1. Establecer mecanismos que permitan informar y orientar al visitante sobre las normas de circulación, comportamiento y seguridad básica que debe cumplir dentro de las instalaciones de la Empresa.

    16.2. Permitir el acceso a los visitantes solamente por el Portón Principal en Matanzas o Portón "A" en Los Pijiguaos y en caso de visitantes con vehículo, debe solicitar el pase respectivo.

    16.3. Suspender el acceso o permanencia de visitantes en sus instalaciones cuando se presente algún hecho que afecte directa o indirectamente los intereses de la Empresa.

17. Toda visita institucional debe ser notificada a la Gerencia Asuntos Públicos, por lo menos con cuarenta y ocho (48) horas de anticipación, a fin de preparar la logística que pueda implicar dicha visita (traslado, aeropuerto, equipos, pases de acceso a la Empresa, entre otros).

18. El visitante, una vez finalizada la visita, debe colocar el carnet de identificación en el buzón ubicado en la manga de acceso.

19. Todo residente que planifique traer visitantes al Campamento de Los Pijiguaos debe tramitar la solicitud de pases, de acuerdo a lo establecido en las Normas Internas del Campamento de Los Pijiguaos.

E. De la Identificación de los Vehículos

20. Los trabajadores y contratistas deben solicitar pase de vehículo a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, mediante el formulario "Solicitud Pase de Vehículo" o "Solicitud Acceso Vehículos de Contratista" y anexar los siguientes documentos:

    - Copia del título de propiedad o carnet de circulación.
    - Copia de la licencia de conducir vigente.
    - Copia de la póliza de seguro del vehículo (todo riesgo y vigente).

- Certificado médico vigente.
- Inspección del vehículo.

21. La identificación de los Vehículos debe efectuarse a través de:

    21.1. Calcomanías para los vehículos de los trabajadores contratados por tiempo indeterminado y los contratados por tiempo determinado y contratistas cuya prestación de servicios sea mayor a seis (6) meses.

    21.2. Pases para los trabajadores o contratistas cuyo tiempo de contratación o servicio a prestar sea menor o igual a seis (6) meses.

22. Las calcomanías para los vehículos, se otorgan de acuerdo al área y están identificadas con los siguientes colores:

    - Verde: Áreas Administrativa y Residencial
    - Amarillo: Todas las Áreas de la Empresa
    - Rojo: Áreas Industriales

23. La Empresa sólo permite el acceso de un (1) vehículo por trabajador y al contratista, de acuerdo a lo establecido en el documento contractual.

24. El pase o calcomanía del vehículo debe ser colocado en el lado izquierdo del parabrisa y tendrá validez durante el año que fue otorgado y el período de renovación debe ser notificado por la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda.

25. El pase o calcomanía de vehículos propiedad de los trabajadores tiene carácter personal e intransferible. El mismo no autoriza la conducción del vehículo por las instalaciones de la Empresa a otra persona diferente a la que se le otorgó el acceso.

26. El trabajador que venda o transfiera el vehículo de su propiedad y posea acceso (calcomanía) a las instalaciones de la Empresa, debe desprender la calcomanía adherida al vehículo y entregarla a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda.

27. Los conductores de los vehículos durante su permanencia en la Empresa deben cumplir con las disposiciones establecidas en la Ley de Tránsito Terrestre y su Reglamento vigente.

F. Del Acceso a las Instalaciones de la Empresa

28. Los trabajadores, contratistas y visitantes a los efectos de accesar las instalaciones de la Empresa deben colocar el carnet de identificación en el lector óptico en el punto de control correspondiente.

29. Los puntos de control que regularán el acceso a las instalaciones de la Empresa, son los siguientes:

    - Portón principal en Matanzas, se registra la hora de entrada y salida del trabajador, contratista o visitante. A los efectos de controlar la entrada y salida de la jornada laboral de los trabajadores, se tomará en cuenta el registro en este portón.
    - Portón principal en Los Pijiguaos, se registra la hora de entrada y salida de visitantes y contratistas.
    - Área de trabajo en Los Pijiguaos, se registra la hora de entrada y salida del trabajador, contratista o visitante. A los efectos de controlar la entrada y salida de la jornada laboral de los trabajadores, se tomará en cuenta el registro en este portón.
    - Áreas restringidas, se registra la hora de entrada y salida del trabajador, contratista o visitante.

30. El trabajador o contratista que accese a las instalaciones de la Empresa debe permitir la revisión del vehículo (maletero, motor, guantera u otra parte del vehículo que se requiera) por la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda.

31. La División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, debe:

    31.1. Autorizar al trabajador y contratista el acceso de vehículo a la Empresa y controlar la renovación o anulación del mismo cuando el caso lo requiera.

    31.2. Detener los vehículos con carga de pasajeros en la parte posterior o cuando su conductor presente estado de ebriedad y proceder de acuerdo al caso.

32. Cuando el acceso a las instalaciones a la Empresa no sea permitido, la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según

corresponda, debe verificar con el afectado el motivo de rechazo y las averiguaciones pertinentes.

33. El horario de visita a las áreas industriales y administrativas está sujeto al horario de trabajo administrativo establecido en la Empresa.

34. Las visitas a las áreas industriales deben realizarse en vehículo de la Empresa o particular autorizado por el Gerente del área responsable y conformado por la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, previa inspección técnica y operativa por parte de éste, a fin de garantizar su seguridad y de los bienes de la Empresa.

35. Las visitas a las áreas industriales, que por circunstancias especiales deben efectuarse fuera del horario establecido, deben estar autorizadas por el Gerente de área a visitar o por el responsable operativo.

36. Las visitas al área comercial u hospital en Los Pijiguaos, deben efectuarse de acuerdo a las Normas Internas del Campamento de Los Pijiguaos.

Pasos a Seguir

A. De la Identificación del Trabajador

División Protección de Planta Alúmina o División Protección de Planta Bauxita

1. De acuerdo a las normas y procedimientos "Ingreso de Personal" y "Movimiento de Personal", recibe de la División Empleo y Compensación o Coordinación Recursos Humanos, según corresponda, el formulario "Solicitud Carnet de Identificación", en original, solicita cédula de identidad al trabajador y revisa. Continúa paso 3.

2. Recibe información del trabajador sobre emisión de un nuevo carnet de identificación, por pérdida o deterioro.

3. Consulta en el Sistema de Información del Sector Aluminio (SISA), módulo de recursos humanos, información del trabajador:

   3.1. Si es nuevo ingreso, registra información en el SISP, módulo de identificación y genera carnet de identificación, según tipo de nómina y acceso a las áreas y entrega al trabajador junto con la cédula de identidad. Continúa paso 6.

   3.2. Si es por cambio de estatus, actualiza información del trabajador en el SISP, módulo de identificación, genera carnet de identificación y entrega al trabajador. Continúa paso 6.

   3.3. Si es por deterioro, consulta en el SISP, módulo identificación, información del trabajador, genera carnet de identificación, entrega al trabajador y destruye el carnet deteriorado. Continúa paso 6.

   3.4. Si es por pérdida, genera carnet de identificación, solicita firma del trabajador en formulario "Autorización para Asignación y/o Deducción" y entrega carnet de identificación al trabajador. Continúa paso 4.

4. Entrega a la División Administración de Beneficios o División Relaciones Industriales, según corresponda, el formulario "Autorización para Asignación y/o Deducción" y archiva original del formulario "Solicitud Carnet de Identificación" y comunicación del trabajador.

División Administración de Beneficios o División Relaciones Industriales

5. Recibe de la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda, el original del formulario "Autorización para Asignación

y/o Deducción", registra en el SISA, módulo recursos humanos, monto a descontar por concepto de pérdida de carnet de identificación y archiva formulario en el expediente del trabajador.

Trabajador

6. Recibe carnet de identificación y cédula de identidad e ingresa a las instalaciones de la Empresa, tal como lo establece en el aparte F de las normas "Acceso a las Instalaciones de la Empresa" de la presente norma y procedimiento.

B. De la Identificación del Contratista

División Protección de Planta Alúmina o División Protección de Planta Bauxita

1. Recibe formulario "Solicitud de Acceso a Personal Contratista", previamente conformado por la unidad usuaria, y copia de los documentos de los trabajadores.
2. Consulta en el Sistema de Información del Sector Aluminio (SISA), módulo de proveedores, pedido asignado al contratista.
3. De acuerdo al número de carnets de identificación solicitados, elabora formulario "Recibo de Ingreso a Caja", firma y entrega al contratista para que efectúe el pago respectivo.
4. Efectuado el pago, recibe del contratista copia del formulario "Recibo de Ingreso a Caja", revisa y registra en el SISP, módulo de identificación, información del contratista, emite y entrega carnet de identificación por cada trabajador al contratista. Archiva documentos.

C. De la Identificación del Vehículo a Trabajador y Contratista

Trabajador

1. Elabora el formulario "Solicitud Pase de Vehículo", en original, en caso de vehículo nuevo ingreso, anexa copias de documentos personales (cédula de identidad, certificado médico y licencia de conducir), documentos del vehículo y póliza de seguro, firma y entrega a la División Protección de Planta Alúmina o División Protección de Planta Bauxita, según corresponda. Continúa paso 3.

División Protección de Planta Alúmina o División Protección de Planta Bauxita

2. Recibe del trabajador o contratista el formulario "Solicitud Pase para Vehículo" o "Solicitud Acceso Vehículo de Contratista", revisa documentos anexos y procede:

   2.1. Si es trabajador de la Empresa, consulta en el SISA datos del trabajador e información de la Póliza de Seguro de Vehículo y consulta o registra en el SISP, de acuerdo al caso, datos del vehículo. Registra información del vehículo y número de la calcomanía en el SISP, módulo identificación. Continúa paso 4.

   2.2. Si es contratista, revisa documentos, consulta en el SISA, módulo de materiales, información del contratista referente a pedido asignado, registra en el SISP, módulo identificación, información del conductor y del vehículo autorizado y número de calcomanía o pase asignado.

3. Genera "Pase de Vehículo", firma y solicita firma del trabajador o contratista, coloca calcomanía o pase en el lado izquierdo del parabrisa del vehículo del trabajador o contratista. Archiva copias de los documentos del vehículo, del conductor y el formulario "Pase de Vehículo".

4. Informa al trabajador o contratista que puede ingresar a las instalaciones de la Empresa, tal como lo establece la parte B de las normas "Acceso a las Instalaciones de la Empresa" de la presente norma y procedimiento.

D. Identificación y Pase del Vehículo de Visitante

División Protección de Planta Alúmina o División Protección de Planta Bauxita

1. Recibe solicitud verbal del visitante, documento de identidad e información sobre persona a visitar. Contacta persona y solicita autorización de acceso del visitante:

   1.1. Si el acceso es autorizado y tiene vehículo, solicita al visitante documentos del vehículo y del seguro. Registra en el SISP, módulo de identificación, información del visitante, del vehículo y número de carnet de identificación, entrega al visitante el carnet y pase de vehículo, junto con los documentos respectivos. Continúa paso 3.

   1.2. Si el acceso es autorizado y no tiene vehículo registra en el SISP, módulo de identificación, información del visitante y número del carnet de identificación y entrega al visitante junto con el documento de identidad.

   1.3. Si el acceso es denegado, devuelve documento de identidad y del vehículo del visitante.

VI. Anexos

(No aplica)

ANEXO 2

Grupo Monve - Catalogo de Equipos de Control de Asistencia y Acceso.

GRUPO MONVE C.A.
J-40185924-0

GRUPO MONVE C.A.
J-40185924-0

En GRUPO MONVE contamos con los más innovadores productos biométricos los cuales poseen la más alta tecnología de identificación de huellas dactilares o rostros con los más altos estándares de calidad que han demostrado liderazgo con reconocimientos internacionales en el ámbito de biometría, seguridad y calidad.

Nuestra misión es proveer servicios de calidad en tecnologías avanzadas, basándonos como principal objetivo en satisfacer de manera eficiente las necesidades y problemas que se les presenten a nuestros clientes.

Con una fuerte política de cálida suministraremos a nuestros clientes productos y servicios que cumplan con sus necesidades, incluyendo los requisitos legales y reglamentarios que apliquen.

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Certificación Internacional

Supremacía en confiabilidad biométrica con los mejores resultados en evaluaciones NIST MINEX

Sobresaliendo entre los mejores 20 fabricantes biométricos más grandes e importantes del mundo, obteniendo los mejores resultados en la evaluación *Minutiae Interoperability Exchange (MINEX)* realizada por el *National Institute of Standars & Technology (NIST)* de EE.UU. en el año 2008.

NIST MINEX es una evaluación rigurosa de algoritmos biométricos dactilares cuyo propósito es:

° Proveer medidas sobre el rendimiento e interoperabilidad en la extracción y comparación de información dactilar a través de algoritmos biométricos automáticos.

° Establecer estándares de codificación y comparación en el marco del programa de control biométrico gubernamental *United States Government´s Personal Identity Verification (PIV).*

°Comprobar que la tecnología biométrica sea realmente confiable para la verificación de identidad de personas.

Supremacía en control de acceso:

Los productos que manejamos en GRUPO MONVE han ganado numerosos premios mundiales, incluyendo el reconocimiento "Mejor Producto de control de acceso" otorgado en el prestigioso evento *Detektor Internacinal Award* en los años 2009 y 2010, premio a los más avanzados productos lanzados al mercado en tres categorías: Control de Acceso, Alarma & Detección y CCTV.

Supremacía en la industria biométrica:

Un prestigioso grupo Frost & Sullivan otorgo un reconocimiento de "Compañía Biométrica del 2009", basando el análisis en criterios de calidad, crecimiento industrial, seguridad, presencia en el mercado global y durabilidad de los productos. **Considerando los productos biométricos los mejores del mundo.**

Supremacía en precisión biométrica: obteniendo los mejores resultados en evaluación FVC

En la competencia de precisión biométrica *Fingerprint Verification Competition* (FCV 2006), científicos de la más prestigiosa universidades emitieron la mayor cantidad de medallas de oro a favor de los algoritmos biométricos de identificación, determinando que es la más precisa del mundo.

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Ventajas y Beneficios de los Equipos Biométricos

En Control de Acceso

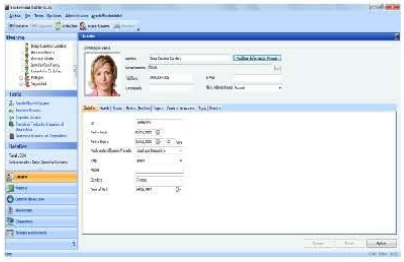
- Mayor seguridad al ofrecer tecnología biométrica más precisa del mercado.
- Restricciones de acceso precisas en función de áreas físicas, días, rango de horas o jerarquía del usuario

- Monitoreo en tiempo real del estado de las puertas.
- Dedo de emergencia para situaciones especiales.
- Posee bajo costo de implementación ya que no requiere paneles de control y emplea cableado estándar Ethernet.

- Compatibilidad con sistemas existentes basados en tarjetas de proximidad
- Interface de comunicación wiegand hacia lectores de proximidad esclavos o paneles de control para fácilmente modernizar y reutilizar sistemas de control de acceso existentes.

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0
En Control de Asistencia



- Alta precisión y velocidad de control al tener la capacidad de controlar grandes flujos de empleados.
- Reportes de asistencia listos para usar:

Consolidación de las marcaciones en tiempo real

Calculo automático de horas de trabajo, sobretiempos, ausencias, tardanzas, salidas tempranas.

- La información de asistencia puede ser exportada hacia sistemas ERP y de nómina.

- Genera reportes exportables en varios formatos: XLS, PDF, CSV, RTF, HTML, ODBC.

- Diversos puntos de control de asistencia distribuidos pueden consolidar la información en un servidor central.
- Las marcaciones se almacenan en base de datos estándar (MySQL, MS, SQL, Oracle)

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Equipos de Control de Acceso y Asistencia






E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0
Equipos de Control Biométrico

Face Station

Algoritmo de reconocimiento facial de última generación
- Tecnología basada en algoritmos biométricos innovadores y optimizados

Alta capacidad y rápido reconocimiento biométrico de rostros
- Capacidad de 10.000 rostros y 1'000.000 registros internamente
- Identifica 1.000 rostros en 1 segundo

Reconocimiento biométrico facial
- Dos cámara faciales (infrarroja y visible)
- Reconocimiento de rostro y registro de fotografía

Flexibilidad en modos de validación
- Varios modos de autenticación: Rostro, PIN, Tarjeta de Proximidad, Tarjeta de Proximidad + Rostro, Tarjeta de Proximidad + PIN

Múltiples opciones de lector de tarjetas RF integrado
- Mifare 13.56MHz.

Fácil Instalación e interconexión
- Comunicación directa a red TCP/IP Ethernet o WiFi (opcional) con encriptación.
- Interface de comunicación complementaria RS485, RS232 y USB.
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relays internos para control directo de cerradura y alarma.
- Soporta alimentación Power over Ethernet (PoE)

Poderosa interface de usuario
- Pantalla táctil LCD de 4.3" a colores WGVA.
- Muestra mensajes e imágenes generales y personales.
- Administración local mediante pantalla táctil
- Sonido de alta calidad configurable.

Características avanzadas de control de acceso
- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Características avanzadas de control de asistencia
- Permite definir hasta 16 eventos de asistencia.

Dimensiones 132mm x 165mm x 60mm

E-mail: info@grupomonve.com
Web: www.grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124

GRUPO MONVE C.A.
J-40185924-0

BioStation T2

Algoritmo de huella dactilar preciso y rápido
- Ganador de las evaluaciones internacionales biométricas NIST MINEX y FVC 2006

Alta capacidad y rápido reconocimiento de huellas dactilares
- Capacidad de 200.000 dedos y 1'000.000 registros internamente
- Identifica 3.000 huellas en 1 segundo

Flexibilidad en modos de validación
- Varios modos de autenticación: Huella Dactilar, PIN, Tarjeta de Proximidad, Tarjeta de Proximidad + Huella Dactilar, Tarjeta de Proximidad + PIN

Cámara integrada
- Cámara con detección de presencia de rostro y registro de fotografía.

Múltiples opciones de lector de tarjetas RF integrado
- EM 125Khz, Mifare 13.56MHz.

Fácil Instalación e interconexión
- Comunicación directa a red TCP/IP Ethernet o WiFi (opcional) con encriptación.
- Interface de comunicación complementaria RS485, RS232 y USB.
- Gestión a través de pendrive USB para localidades sin red.
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relays internos para control directo de cerradura y alarma.
- Soporta alimentación Power over Ethernet (PoE)

Poderosa interface de usuario
- Pantalla TouchScreen de 5" a colores.
- Muestra mensajes e imágenes generales y personales.
- Teclas de acceso rápido.
- Sonido de alta calidad configurable.
- Servidor web embebido.

Características avanzadas de control de acceso
- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Características avanzadas de control de asistencia
- Permite definir hasta 16 eventos de asistencia.

Dimensiones 155mm x 155mm x 40mm

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioStation

Algoritmo de huella dactilar preciso y rápido

- Ganador de las evaluaciones internacionales biométricas NIST MINEX y FVC 2006

Alta capacidad y rápido reconocimiento de huellas dactilares

- Capacidad de 200.000 dedos y 1'000.000 registros internamente
- Identifica 3.000 huellas en 1 segundo

Flexibilidad en modos de validación

- Varios modos de autenticación: Huella Dactilar, PIN, Tarjeta de Proximidad, Tarjeta de Proximidad + Huella Dactilar, Tarjeta de Proximidad + PIN

Múltiples opciones de lector de tarjetas RF integrado

- EM 125Khz, HID Prox 125kHz, Mifare 13.56MHz.

Fácil Instalación e interconexión

- Comunicación directa a red TCP/IP Ethernet o WiFi (opcional) con encriptación.
- Interface de comunicación complementaria RS485, RS232 y USB.
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relay interno para control directo de cerradura.

Poderosa interface de usuario

- Pantalla LCD de 2.5" a colores de 320x240 pixeles.
- Muestra mensajes e imágenes generales y personales.
- Teclas para administración local.
- Sonido de alta calidad configurable.

Características avanzadas de control de acceso

- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Características avanzadas de control de asistencia

- Permite definir hasta 16 eventos de asistencia.

Dimensiones 135mm x 128mm x 50mm.

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioLite Net

Algoritmo de huella dactilar preciso y rápido
- Ganador de las evaluaciones internacionales biométricas NIST MINEX y FVC 2006

Alta capacidad y rápido reconocimiento de huellas dactilares
- Capacidad de 5000 dedos y 50.000 eventos internamente
- Identifica 2.000 huellas en 1 segundo

Flexibilidad en modos de validación
- Varios modos de autenticación: Huella Dactilar, PIN, Tarjeta de Proximidad, Tarjeta de Proximidad + Huella Dactilar, Tarjeta de Proximidad + PIN

Múltiples opciones de lector de tarjetas RF integrado
- EM 125Khz, Mifare 13.56MHz.

Estructura protegida para instalación en exteriores
- Certificación de protección a intemperie IP65
- Resistente al agua y climas externos desde -20°C hasta +50°C

Fácil Instalación e interconexión
- Comunicación directa a red Ethernet TCP/IP con encriptación.
- Interface de comunicación complementaria RS485
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relay interno para control directo de cerradura.

Fácil administración y operación
- Pantalla LCD gráfica, LED multicolor y sonido multitono para uso intuitivo.
- Teclado para administración local.

Diseño delgado y elegante
- Adecuado para ser instalado en el marco de la puerta o espacios pequeños.

Características avanzadas de control de acceso
- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Características avanzadas de control de asistencia
- Permite definir hasta 16 eventos de asistencia.

Dimensiones 60mm x 185mm x 40mm

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioEntry W

Algoritmo de huella dactilar preciso y rápido

- Ganador de las evaluaciones internacionales biométricas NIST MINEX y FVC 2006

Alta capacidad y rápido reconocimiento de huellas dactilares

- Capacidad de 5000 dedos y 50.000 eventos internamente
- Identifica 2.000 huellas en 1 segundo

Flexibilidad en modos de validación

- Varios modos de autenticación: Huella Dactilar, Tarjeta de Proximidad, Tarjeta de Proximidad + Huella Dactilar

Múltiples opciones de lector de tarjetas RF integrado

- EM 125Khz, Mifare 13.56MHz.

Estructura protegida para instalación en exteriores

- Certificación de protección a intemperie IP65
- Resistente al agua y climas externos desde -20°C hasta +50°C

Fácil Instalación e interconexión

- Comunicación directa a red Ethernet TCP/IP con encriptación.
- Interface de comunicación complementaria RS485
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relay interno para control directo de cerradura.

Fácil administración y operación

- LED multicolor y sonido multitono para uso intuitivo.
- Permite el uso de tarjetas maestras para administración local.

Diseño delgado y elegante

- Adecuado para ser instalado en el marco de la puerta o espacios pequeños.

Características avanzadas de control de acceso

- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Dimensiones 50mm x 172mm x 41mm

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioEntry Plus

Algoritmo de huella dactilar preciso y rápido
Alta capacidad y rápido reconocimiento de huellas dactilares

- Capacidad de 5000 dedos y 50.000 eventos internamente
- Identifica 2.000 huellas en 1 segundo

Flexibilidad en modos de validación

- Varios modos de autenticación: Huella Dactilar, Tarjeta de Proximidad, Tarjeta de Proximidad + Huella Dactilar

Múltiples opciones de lector de tarjetas RF integrado

- EM 125Khz, HID Prox 125kHz, Mifare 13.56MHz, iCLASS 13.56MHz

Fácil Instalación e interconexión

- Comunicación directa a red Ethernet TCP/IP con encriptación.
- Interface de comunicación complementaria RS485
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relay interno para control directo de cerradura.

Fácil administración y operación

- LED multicolor y sonido multitono para uso intuitivo.
- Permite el uso de tarjetas maestras para administración local.

Diseño delgado y elegante

- Adecuado para ser instalado en el marco de la puerta o espacios pequeños.

Características avanzadas de control de acceso

- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje y dedo de emergencia para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Dimensiones 50mm x 160mm x 37mm

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0
Equipos de Control de Proximidad

XPass

Alta capacidad.
- Capacidad de 40.000 tarjetas y 50.000 eventos internamente

Múltiples opciones de lector de tarjetas RF integrado
- EM 125Khz, HID Prox 125kHz, Mifare 13.56MHz.

Estructura Protegida para instalación en exteriores.
- Certificación de Protección a intemperie IP65.
- Resistente al agua y climas extremos desde -20˚C hasta +50˚C

Fácil Instalación e interconexión
- Comunicación directa a red Ethernet TCP/IP con encriptación.
- Interface de comunicación complementaria RS485.
- Entrada /salida Wiegand configurable hasta 64 bits. Puede controlar un lector externo.
- Relay interno para control directo de cerradura.
- Soporta alimentación Power over Ethernet (PoE)

Fácil administración y operación.
- LED multicolor y sonido multitono para uso intuitivo.
- Permite el uso de tarjetas maestras para administración local.

Diseño delgado y elegante.
- Adecuado para ser instalado en el marco de la puerta o espacios pequeños.

Características avanzadas de control de acceso
- Permisos de accesos configurables de manera detallada.
- Gestión de alarmas, sensor de desmontaje para eventualidades.
- Opción a unidad de expansión Secure I/O para configuraciones extendidas

Dimensiones 148mm x 204mm x 48mm

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Otros Equipos

Módulo de Expansión Secure I/O

El módulo de expansión brinda puertos de entrada (sensores, botones) y salida (relés para alarmas, cerraduras) adicionales para aplicaciones de control de acceso. Provisto de comunicación cifrada, proporciona una forma segura y cómoda de escalar las funciones de control de acceso de los terminales.
Hasta cuatro unidades Secure I/O pueden agregarse a un terminal, lo que equivale a adicionar ocho (8) relés y dieciséis (16) sensores adicionales.

BioMini Lector Dactilar de Enrolamiento

El BioMini es un Sensor óptico resistente a ralladuras que permite realizar el enrolamiento de las huellas de los nuevos usuarios directamente desde la PC donde se encuentre el software BioStar. Lo cual brinda mayor comodidad para el registro del nuevo personal.
Usa interface USB 2.0 con unas dimensiones de 66mm x 90mm x 58mm, con una resolución de 500dpi con 256 niveles de gris.

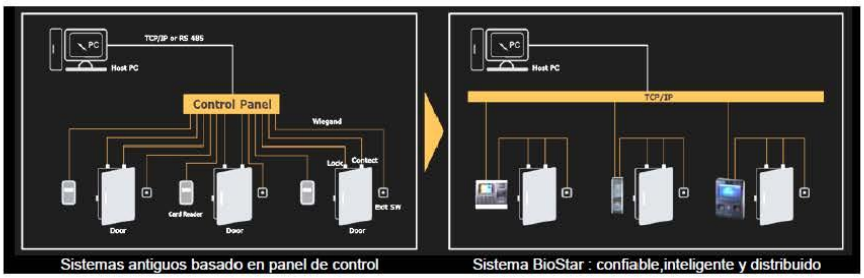
E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

SOFTWARE BIOSTAR

El software de control de acceso y asistencia **BioStar** es de última generación basado en conectividad IP y seguridad biométrica de alto desempeño. La combinación de la más alta seguridad biométrica de los terminales con su conectividad TCP/IP nativa permite sacar el máximo provecho a ambas tecnologías, ya que cada terminal instalado en cada puerta trabaja como lector y controlador inteligente, que puede trabajar de manera autónoma y continua.

El costo total de esta solución es muy atractivo puesto que no se requieren complejos paneles de control y el cableado se hace mucho más sencillo. La gestión de usuarios, plantillas biométricas, tarjetas, reglas de control de acceso, informes de auditoría y reportes de control de asistencia se pueden hacer en forma cómoda y consolidada desde el **BioStar**. La comunicación está protegida mediante mecanismos de cifrado de alta seguridad.



Sistemas antiguos basado en panel de control | Sistema BioStar : confiable,inteligente y distribuido

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Versiones del BioStar

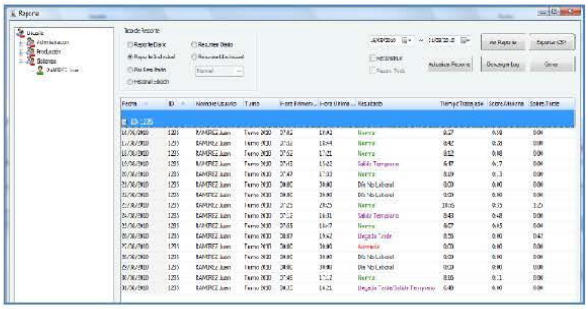
Características		BioStar F	BioStar SE
Sistema	Licenciamiento	Gratuito	Licencia para servidor
	Base de Datos	MSSQL, MySQL Oracle	MSSQL, MySQL Oracle
	Dispositivos Max	20	512
	Clientes Recurrentes	2	32
	Server Matching	-	Si
Control de Acceso	Calendarios de Tiempo	128	128
	Grupos de acceso	128	128
	Anti-passback	-	Si
	Zonas Inteligentes	-	Anti-passback, límite de entrada, alarma de acceso, alarma de incendio
	Notificación por email	-	Si
	Monitoreo	Si	Si
	Mapa visual	-	Si
	Integración con CCTV	-	Si
	Impresión de Carnets	-	Si
Control de Asistencia	Calculo de horas de trabajo	Si	Si
	Manejo de Turnos	Semanal	Semanal, rotativos (N-días)
	Días Libres y Feriados	Si	Si
	Reportes Exportables	Si	Si
	Tabla de Entrada y Salida	-	Si

Reportes del BioStar

El software permite generar de manera rápida y comoda varios tipos de reportes de asistencia completos, entre ellos tenemos el reporte diario, resumen diario, reporte individual, resumen individual y reporte de resultado. En todos ellos se puede elegir qué información mostrar como por ejemplo:

Reporte Individual

Este reporte muestra la actividad laboral de los trabajadores, ordenada por día, en este reporte se aprecia información detallada como la hora de entrada, hora de salida, el tiempo trabajado en horario normal, horas extra, ausencias, tardanzas, salidas antes.

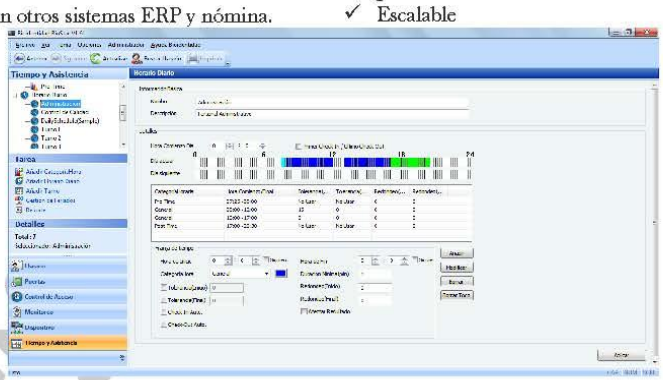


E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Beneficios

- ✓ Control de Acceso y Asistencia integrado.
- ✓ Comunicación TCP/IP distribuida.
- ✓ Soporta Grandes cantidades de empleados.
- ✓ Interfaz gráfica amigable.
- ✓ Multiusuario.
- ✓ Integración con otros sistemas ERP y nómina.
- ✓ Identificación real de las personas
- ✓ Alta Seguridad
- ✓ Óptima relación calidad-precio
- ✓ Fácil integración con lectores de tarjetas de proximidad existentes
- ✓ Escalable



Ahorro en las Tareas de Recursos Humanos al transcribir datos para el cálculo de las nominas

Número de Personas	10	25	50	100	500	1000
Tiempo requerido por RRHH por personas a la semana en minutos	5	5	5	5	5	5
Ahorro de trabajo a la semana expresado en horas	0:20	0:50	1:40	3:20	16:40	33:20
Ahorro de trabajo al mes expresado en horas	1:20	3:20	6:40	13:20	66:40	133:20
Ahorro de Trabajo al año por parte del personal de RRHH	**16**	**40**	**80**	**160**	**800**	**1600**

Genera un ahorro para la empresa al eliminar errores y fraudes por ausencias, tardanzas, salidas antes o pago de sobre tiempo

Número de Personas	10	25	50	100	500	1000
Horas de trabajo semanales por persona	40	40	40	40	40	40
Trabajo semanal	400	1,000	2,000	4,000	20,000	40,000
Porcentaje de Error estimado por ausencias, tardanzas o salidas antes	1.00%	1.00%	1.00%	1.00%	1.00%	1.00%
Ahorro de pagos semanales expresado en horas	4	10	20	40	200	400
Ahorro de pagos mensual expresado en horas	16	40	80	160	800	1,600
Ahorro en horas de pagos al año	**192**	**480**	**960**	**1,920**	**9,600**	**19,200**

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Lista de Clientes.

- Taller Giroto C.A.
- Farmacia Génesis Centro C.A.
- Industrias Alimenticias Viena C.A.
- Laboratorios Leti S.A.V. www.leti.com.ve
- Cultural Print C.A. www.culturalprint.com
- MAX CENTER (Grupo Dartysy C.A.). www.maxcenter.com.ve
- Industrial Saxolutions C.A.
- CINEX (Suramericana de Espectáculos S.A.) www.cinex.com.ve
- Estacionamientos Marcos Fuertes S.R.L
- Estacionamientos Mar-Fuer C. A.
- Estacionamientos Cediaz C.A.
- Clínica Cem-Anex S.C
- Instituto Universitario de Maracaibo. IUTM www.iutm.edu.ve
- Estacionamiento MLPG C.A.
- Estacionamiento Aventura Plaza C.A.
- TOYOTA INDUSTRIAL DE VENEZUELA C.A. www.toyotaindustrial.com.ve
- Alimentos Súper-S C.A.
- Taxand Consultores C.A. www.taxand.com.ve
- Inversiones SIMBI C.A. www.simbi.com.ve
- Clínica CEMO C.A. www.clinicacemo.com
- CMQ Mediprot C.A.
- La Lucha C.A.
- Instituto Aeropuerto Internacional de Maiquetía IAIM www.aeropuerto-maiquetia.com.ve
- CONVIASA www.conviasa.aero
- Grupo Único C.A. www.grupounico.com.ve
- Zona Franca Industrial, Comercio y de Servicio de Paraguaná C.A. (ZONFIPCA)
- Industrias Metalúrgicas Nacionales C.A. www.inmet.com.ve
- LINIO (R-SC Interne Services C.A.) www.linio.com.ve
- CAMERON VENEZOLANA S.A. www.c-a-m.com
- Topac Business Solutions de Venezuela S.A.
- MOHECA C.A.
- Informática y Telecomunicaciones Integradas INTELIGEN SA www.inteligensa.com

E-mail: info@grupomonve.com
Teléfonos: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

ANEXO 3

Lista de precios Equipos Biométricos

julio 2015.

GRUPO MONVE C.A.
J-40185924-0

Equipos Biométricos para Control de Acceso y Asistencia






Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124

Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Confidencialidad:

Este documento contiene información confidencial de uso exclusivo de sus destinatarios. Está prohibida la modificación, retransmisión, difusión, copia u otro uso de esta información, por personas distintas al destinatario o para fines que contravengan a Grupo MONVE, C.A. si usted ha recibido este documento por error, por favor bórrelo y notifique al remitente.

Asistencia Técnica:

Brindamos asesoría en la Pre-implementación del Sistema. Capacitamos al personal clave de la institución en la operación del sistema respondiendo todas sus dudas al momento de la instalación del producto.

Precio en Bolívares:

Los precios indicados son en moneda nacional (Bs.). Dichos precios no incluyen el Impuesto al Valor Agregado (IVA).
Los precios pueden cambiar sin previo aviso.

Nota importante: los equipos se traen bajo pedido de acuerdo a la disponibilidad internacional.

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Lista de Precio Julio 2015

Equipos por Biométrico por control de Huella Dactilar

BioEntry Plus

	BioEntry Plus EM	Equipo Biométrico y Tarjeta EM 125 kHz	428.792,00
	BioEntry Plus Mifare	Equipo Biométrico Con Tarjeta Mifare 13.56MHz	492.882,00
	BioEntry Plus HID	Equipo Biométrico Con Tarjeta HID 125kHz	514.672,60

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioEntry W

	BioEntry W Mifare	Equipo Biométrico Con Tarjeta Mifare 13.56MHz	613.371,20
	BioEntry W HID	Equipo Biométrico Con Tarjeta HID 125kHz	677.461,20

BioLite Net

	BioLite Net EM	Equipo Biométrico y Tarjeta EM 125 kHz	619.780,20

BioStation T2

	BioStation T2 EM	Equipo Biométrico, Tarjeta EM 125 kHz y Pin. Toma Fotografía	1.177.363,20

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

BioStation

	BioStation EM	Equipo Biométrico, Tarjeta EM 125 kHz y Pin	1.003.038,40
	BioStation HID Prox	Equipo Biométrico, Tarjeta HID 125kHz	1.087.637,20

Equipos por Control de Proximidad

Xpass

	Xpass EM	Control de Tarjeta EM 125kHz	292.921,20
	Xpass Mifare	Control de Tarjeta Mifare 13.56MHz	305.739,20
	Xpass HID	Control de Tarjeta HID 125kHz	369.829,20

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Otros Equipos

Secure I/O

Secure I /O	Módulo de expansión de puertos de terminal de control. Agrega 2 relés y 4 entradas de sensores	108.342,00

BioMini

BioMini	Lector Biométrico USB Permite el enrolamiento de huellas desde el PC con el BioStar	114.751,00

BioStar SE

BioStar SE	Software BioStar -Permite Horarios Rotativos	580.533,20

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Accesorios de Proximidad

Tarjetas Imprimibles EM

Grupo de 10 Tarjeta de proximidad EM 125kHz	3.296,00

Accesorios de Control de Acceso

Cerraduras Electromagnéticas

- Cerradura Electromagnética.
- Fuerza de Retención: 600 Libras.
- Alimentación Soportada: DC 12V / DC 24V.
- Sensor de Supervisión: NO & NC.
- Peso: 2 Kg.
- Led indicador

27.540,24

Base ZL para Cerraduras Electromagnéticas

- Base tipo ZL para cerradura 600 lbs
- (3 piezas).

14.539,20

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com

GRUPO MONVE C.A.
J-40185924-0

Botón pulsador Liberador de Puertas

01

- Botón pulsador liberador de puerta.
- Normalmente NA/NC/COM.
- Dimensiones 115*40*24 mm.
- Material: Aluminio.
- Alimentación Soportada: DC 12V

7.449,65

02

- Botón liberador de puerta Touch Screen
- Normalmente NA/NC/COM.
- Dimensiones: 86*50*25 mm
- Alimentación Soportada: DC 12V

12.000,04

Botón Liberador de Puertas sin contacto

01

- Botón liberador de puerta sin contacto.
- Normalmente NA/NC/COM.
- Dimensiones: 115* 70*29mm
- Material: Aluminio.
- Alimentación Soportada: DC 12V

12.000,04

Email: info@grupomonve.com
Teléfono: 0212-314.9760 / 0424-159.6168 / 0414-240.1124
Web: www.grupomonve.com