UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ECONÓMICAS Y SOCIALES
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE UNA EMPRESA DE DESARROLLO TECNOLÓGICO

Presentado por:

Rodrígues Fonseca, Gabriela de los Ángeles

Para optar al título de:
Especialista en Gerencia de Proyectos

Asesor:
López, Emmanuel

Caracas, julio de 2018

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ECONÓMICAS Y SOCIALES
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE UNA EMPRESA DE DESARROLLO TECNOLÓGICO.

Presentado por:

Rodrígues Fonseca, Gabriela de los Ángeles

Para optar al título de:
Especialista en Gerencia de Proyectos

Asesor:
López, Emmanuel

Caracas, julio de 2018

CARTA DE APROBACIÓN DEL ASESOR

Caracas, 05 de Julio de 2018

Directora del Programa Gerencia de Proyectos
Estudios de Postgrado
Universidad Católica Andrés Bello (UCAB)
Presente.-

Referencia: **Aprobación del Asesor**

Tengo a bien dirigirme a Usted a fin de informarle que he leído y revisado el borrador final del Trabajo Especial de Grado titulado "**Plan para la implementación de un sistema de control de acceso a las instalaciones de una empresa de desarrollo tecnológico**", presentado por la cursante Gabriela de los Ángeles Rodrígues F., titular de la cédula de identidad N° 18740532, como parte de los requisitos para optar al Título de **Especialista en Gerencia de Proyectos**.

A partir de dicha revisión, considero que el mencionado Trabajo Especial de Grado reúne los requisitos y méritos suficientes para ser sometido a evaluación por el distinguido Jurado que tenga(n) a bien designar.

Atentamente,

Ing. Emmanuel López C.

C. I. Nº 3.189.576

CARTA DE AUTORIZACIÓN DE LA EMPRESA

Soluciones Código 2L C.A.
Rif: J-29634540-6
Arquitectura Empresarial

Caracas, 27 de noviembre de 2017

CARTA DE AUTORIZACIÓN DE LA EMPRESA

Sres.
UNIVERSIDAD CATÓLICA ANDRÉS BELLO
Postgrado de Gerencia de Proyectos
Caracas.-

Tengo el agrado de dirigirme por medio de la presente, para hacer de su conocimiento que se ha **AUTORIZADO** al Ingeniero **Gabriela de los Ángeles Rodrígues Fonseca**; titular de la Cédula de Identidad V-18.740.532, hacer uso de la información de la empresa, esto en virtud de documentar y soportar los elementos de los distintos análisis estrictamente académicos que conlleva la realización del Trabajo Especial de Grado **"PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE LA EMPRESA SOLUCIONES CÓDIGO 2L"**, como requisito para optar al título de **Especialista en Gerencia de Proyectos**, exigidos por la Dirección General de los Estudios de Postgrado de la Universidad Católica Andrés Bello.

Sin otro particular al cual hacer referencia, quien suscribe.

Atentamente,

Soluciones
Codigo 2L C.A.
Ingeniería de Software
RIF: J-29634540-6

Ing. Luis Eduardo Ortuño
Presidente
Soluciones Código 2L, C.A
Tlfns de contacto: 0424.2571590 / 0412.2261086 / 0426.2261039

asesorias@codigo2L.com
www.codigo2L.com

LISTA DE ACRÓNIMOS Y SIGLAS

EDTEC: Empresa de desarrollo tecnológico.

FAR: Tasa de falsa aceptación (False Rejection Rate).

FRR: Tasa de falso rechazo (False Rejection Rate)

RFID: Identificación por radiofrecuencia (Radio Frequency Identification)

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ECONÓMICAS Y SOCIALES
POSTGRADO EN GERENCIA DE PROYECTOS

PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE UNA EMPRESA DE DESARROLLO TECNOLÓGICO.

Autor: Rodrígues, Gabriela
Asesor: López, Emmanuel
Año: 2018

RESUMEN

La empresa objeto de este estudio, la cual, con el fin de preservar su identidad se denominó Empresa de Desarrollo Tecnológico EDTEC, provee servicios de desarrollo de software, capacitación personal, asesorías y consultorías en el área tecnológica y afines. Posee 18 oficinas administrativas y de gestión a nivel nacional, por lo que requiere incrementar los requisitos de seguridad a sus instalaciones, equipos tecnológicos y personal que en ella labora. Para cumplimiento del objetivo general del estudio “diseñar un plan para la implementación de un sistema de control de acceso a las instalaciones de una empresa de desarrollo tecnológico”, se analizaron los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso, se determinó la factibilidad técnica, económica y financiera de cada uno de ellos dando como resultado que el dispositivo de reconocimiento por huella dactilar es el más viable y más usado por empresas a nivel mundial. El desarrollo de cada uno de los objetivos propuestos para este estudio contribuyó a la elaboración el documento "Plan para la implementación del Sistema de Control" como guía para garantizar el éxito en la implementación, así como la determinación de los riesgos asociados al plan para la implementación de un sistema de control de acceso. El plan para la implementación de un sistema de control de acceso tiene múltiples beneficios como la gestión de acceso al personal autorizado a las instalaciones y la seguridad de los equipos tecnológicos y del talento humano de la empresa para seguir brindando apoyo a los clientes en alcanzar sus objetivos empresariales.

Palabras Clave: Plan, Control de Acceso, Implementación de Sistema.
Línea de Trabajo: Definición y Desarrollo de Proyectos.

AGRADECIMIENTOS

Primeramente a Dios, por iluminar mi camino en todo momento y haberme dado la fuerza y la voluntad necesaria para seguir mis sueños y alcanzarlos.

A mi mama, por su apoyo inalcanzable, sus enseñanzas y valores que me han hecho crecer cada día como mejor ser humano, siendo mi modelo a seguir y permitiéndome culminar cada una de las etapas en mi carrera profesional.

A mi papá, por ser la luz que me guía desde el cielo seguidor de mis logros.

A mi bella familia por ofrecerme su apoyo incondicional en los momentos difíciles.

A mi esposo, por motivarme a ser mejor profesional y mejor persona cada día, por estar a mi lado en las buenas y en las malas, en cada paso que doy te veo tomándome de la mano y ayudándome a continuar.

A la UCAB, por brindarme los conocimientos académicos y las herramientas que me permiten destacar en el mundo laboral.

Al profesor Emmanuel López, por el aporte de sus conocimientos académicos, que han sido la base para mi desarrollo profesional.

A mis amigos por contar con su solidaridad y apoyo en todo momento.

A mis compañeras del postgrado Nomis y Betina, por enriquecer mis conocimientos cuando juntas asumimos el reto de ser Especialistas en Gerencia de Proyectos, por su ayuda y colaboración a lo largo del postgrado.

A todos que con un grano de arena contribuyeron en el desempeño de esta labor… Mil Gracias.

INDICE GENERAL

CARTA DE AUTORIZACIÓN DE LA EMPRESA iv

RESUMEN vi

AGRADECIMIENTOS vii

INDICE GENERAL viii

INDICE DE FIGURAS xi

INDICE DE TABLAS xii

INTRODUCCIÓN 1

CAPITULO I: EL PROBLEMA 3

1.1. Planteamiento del Problema 3

1.2. Objetivos del Estudio 6

1.2.1. Objetivo General 6

1.2.2. Objetivos Específicos 6

1.3. Justificación de la investigación 7

1.4. Alcance y Delimitaciones de la Investigación 8

CAPÍTULO II: MARCO TEORICO 9

2.1. Antecedentes 9

2.2. Fundamentos Teóricos 14

- Proyecto: 14
- Ciclo de vida de un proyecto: 15
- Gerencia de Proyecto: 16
- Áreas de conocimiento de la gerencia de proyectos: 17
- Dispositivos de reconocimiento: 22
- Identificación por radiofrecuencia (No biométrico): 24
- Software: 24

- Hardware: 24
- Bases de datos: 25
- Servidores: 25
- Estudio de Factibilidad: 25
- Factibilidad Técnico de un Proyecto: 25
- Factibilidad Económica y Financiera de un Proyecto: 26

2.3. Bases Legales 26

2.4. Definición de Términos 28

CAPITULO III: MARCO METODOLÓGICO 31

3.1. Tipo de Investigación 31

3.2. Diseño de la Investigación 32

3.3. Unidad de análisis 32

3.4. Técnicas e Instrumentos de recolección de datos 33

3.5. Fases de la Investigación 34

3.6. Procedimientos por Objetivos 35

3.7. Operacionalización de los Objetivos 37

3.8. Estructura Desagregada de Trabajo 40

3.9. Aspectos Éticos 41

3.10. Cronograma 41

3.11. Recursos 43

CAPITULO IV: MARCO ORGANIZACIONAL 45

4.1. Reseña Histórica 45

4.2. Misión 46

4.3. Visión 46

4.4. Objetivos 46

4.5. Estructura Organizativa 47

CAPITULO V: PRESENTACIÓN Y ANÁLISIS DE LOS DATOS 48

5.1. Analizar los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso. 48

5.2. Determinar la factibilidad técnica del proyecto para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC. 55

5.3. Realizar el estudio de factibilidad económica financiero que permita determinar la viabilidad de implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC..... 68

CAPITULO VI: LA PROPUESTA 77

6.1 Título..... 77

6.2 Propósito 77

6.3 Objetivo 77

6.4 Justificación 77

6.5 Alcance..... 77

6.6 Modo de uso..... 78

6.7 Estructura de la propuesta 78

6.8 Determinar los riesgos asociados al plan diseñado para la implementación del sistema de control de acceso. 80

6.9 Factibilidad de la propuesta 83

Factibilidad Técnica..... 83

Factibilidad Operativa 83

CONCLUSIONES Y RECOMENDACIONES..... 84

Conclusiones..... 84

Recomendaciones..... 85

REFERENCIAS BIBLIOGRÁFICAS 86

INDICE DE FIGURAS

Figura **Pág.**

FIGURA 1: ÍNDICE DE SEGURIDAD CIUDADANA 3

FIGURA 2: CICLO DE VIDA DE LOS PROYECTOS 15

FIGURA 3: ÁREAS DE CONOCIMIENTO EN LA GERENCIA DE PROYECTOS 21

FIGURA 4: ESTRUCTURA DESAGREGADA DE TRABAJO 40

FIGURA 5: CRONOGRAMA DE ACTIVIDADES 42

FIGURA 6: ESTRUCTURA ORGANIZATIVA DE EDTEC 47

FIGURA 7: SEGMENTACIÓN DEL USO DE LA BIOMETRÍA 55

FIGURA 8: ENCABEZADO DEL DOCUMENTO: PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO 79

FIGURA 9: SECCIÓN APROBACIÓN DEL PLAN 79

INDICE DE TABLAS

Tabla **Pág.**

TABLA 1: OPERACIONALIZACIÓN DE LOS OBJETIVOS 38

TABLA 2: PRESUPUESTO PARA LA INVESTIGACIÓN 43

TABLA 3: FACTORES QUE AFECTAN SOBRE LOS SISTEMAS BIOMÉTRICOS Y NO BIOMÉTRICOS 52

TABLA 4: CRITERIOS DE EVALUACIÓN DE LOS SISTEMAS BIOMÉTRICOS Y NO BIOMÉTRICOS 53

TABLA 5: ELEMENTOS COMUNES NECESARIOS PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESO 56

TABLA 6: ELEMENTOS NECESARIOS PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESO POR TIPO DE RECONOCIMIENTO 58

TABLA 7: PERSONAL REQUERIDO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO 60

TABLA 7: COMPARACIÓN ENTRE EL USO DE ELEMENTOS BIOMÉTRICOS Y NO BIOMÉTRICOS 63

TABLA 8: VULNERABILIDADES QUE AFECTAN A LOS SISTEMAS DE RECONOCIMIENTO BIOMÉTRICO 64

TABLA 9: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR TARJETAS DE PROXIMIDAD 68

TABLA 10: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE VOZ 69

TABLA 11: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE HUELLA DACTILAR 69

TABLA 12: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL 70

TABLA 13: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS 70

TABLA 14: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE PALMA DE LA MANO 71

TABLA 15: VALOR CUANTITATIVO Y CUALITATIVO DE LAS VARIABLES EMPLEADAS PARA LA EVALUACIÓN DE LAS ALTERNATIVAS 74

TABLA 16: EVALUACIÓN CUALITATIVA Y CUANTITATIVA DE LAS ALTERNATIVAS 74

TABLA 17: ESTIMACIÓN DE LA INVERSIÓN TOTAL PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE HUELLA DACTILAR 75

TABLA 18: DEPRECIACIÓN DE LOS ACTIVOS DE LA INVERSIÓN 76

TABLA 19: RIESGOS ASOCIADOS AL PLAN DISEÑADO 80

INTRODUCCIÓN

Actualmente, la tecnología brinda herramientas para establecer distintos niveles de seguridad en industrias, contra fenómenos naturales, seguridad informática e identificación y acceso de personal. Día a día, las empresas e instituciones buscan soluciones que ayuden a tener un control permanente en sus instalaciones, es por ello que han venido desarrollando sistemas de control que proporcionan acceso total o parcial al personal a áreas específicas dentro de las instalaciones.

Un sistema de control de acceso permite, de forma automática, aprobar o negar el paso de una persona a sitios restringidos en función a ciertos parámetros establecidos por una organización.

Enfocado con respecto a la identificación y acceso de personal, las compañías están implementando sistemas que facilitan el acceso con información propia de cada usuario; dentro de este campo existen varias alternativas que brindan soluciones para cada una de las necesidades, tales como escaneo de la huella digital, escaneo del iris, reconocimiento de voz y reconocimiento a través de tarjetas magnéticas, entre otros métodos.

Naturalmente, los dispositivos que se utilizan para controlar el ingreso de personas a un edificio o algunas de sus áreas dependen del nivel de seguridad que se requiera y de la cuantificación del impacto de una amenaza sobre sus activos, tanto en lo relativo a pérdidas económicas como a daños de personas o a la imagen social de la organización

La empresa objeto de este estudio, la cual, con el fin de preservar su identidad se denominará en lo sucesivo Empresa de Desarrollo Tecnológico EDTEC, provee servicios de desarrollo de software, capacitación personal, asesorías y consultorías en el área tecnológica y afines. Posee 18 oficinas administrativas y de gestión a nivel nacional, por lo que requiere incrementar los requisitos de seguridad a sus instalaciones, equipos tecnológicos y personal que en ella labora.

El presente estudio surge de la necesidad de implementar un sistema de identificación y control de acceso a las instalaciones de la empresa EDTEC para incrementar la seguridad de sus activos más importantes.

El presente documento, que presenta el estudio a realizar, está estructurado en cuatro capítulos, que se describen a continuación:

Capítulo I El problema: Se presenta el planteamiento del problema, se formulan los objetivos de la investigación así como la justificación y el alcance de la misma.

Capítulo II Marco teórico: Se presentan los estudios previos que fundamentan esta investigación, las bases teóricas que sustentan el estudio y el contexto legal necesario para desarrollar la presente investigación.

Capítulo III Marco metodológico: Se describe el tipo y diseño de investigación, seleccionados para el desarrollo, se detallan las técnicas e instrumentos de recolección y análisis de datos. Se indican las consideraciones éticas seguidas durante el desarrollo de la investigación.

Capítulo IV Marco organizacional: Se describen algunos elementos de la Empresa de Desarrollo Tecnológico (EDTEC) tales como su misión, visión, objetivos.

Capítulo V Desarrollo de los objetivos: Se describen el detalle de los objetivos específicos analizando los diferentes dispositivos de reconocimiento existentes en el mercado, se determina la factibilidad técnica y económica financiera de implementar un sistema de control de acceso.

Capítulo VI La propuesta: Se enfatiza la importancia, el propósito, el objetivo el alcance y la utilidad de la propuesta del presente Trabajo Especial de Grado.

Finalmente se presentan las conclusiones y recomendaciones en función del desarrollo de los objetivos de la investigación, así como las referencias bibliográficas consultadas para elaborar este documento.

CAPITULO I: EL PROBLEMA

En este capítulo se presenta el planteamiento del problema, el alcance y delimitaciones de la investigación, los objetivos generales y específicos, así como las razones que justifican el desarrollo del mismo.

1.1. Planteamiento del Problema

"Venezuela se encuentra en el primer lugar como el país más inseguro del mundo", de acuerdo a un estudio realizado por la firma Gallup mediante un sondeo de opinión usado frecuentemente en los medios de comunicación de masas para representar la opinión pública.

El índice de seguridad ciudadana de Gallup toma en cuenta la confianza en la policía local, la percepción de seguridad entre la población e incidentes registrados de robos. El estudio de Gallup se realizó a partir de encuestas telefónicas y presenciales entre 2009 y 2013 dirigidas a cerca de 1.000 adultos mayores de 15 años de cada país, con un margen de error de entre 2,1 y 5,6 puntos porcentuales, y un nivel de confianza del 95%.

Entre los encuestados para el caso de Venezuela, solo el 19% afirmó sentirse seguro, el 22% afirma haber sido víctima de un hurto en los últimos doce meses y 74% reconoce que desconfía de las autoridades locales.

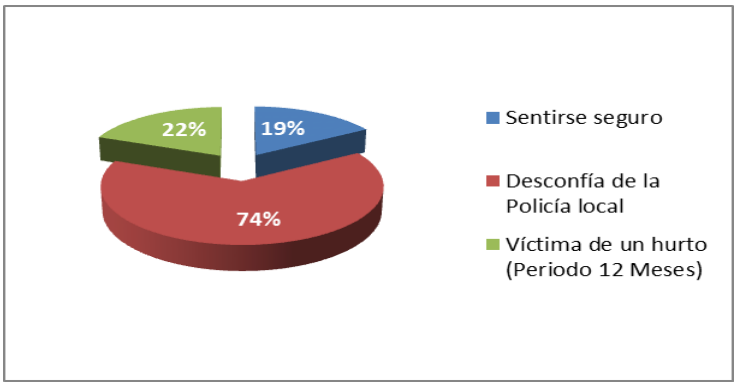


Figura 1: Índice de seguridad ciudadana

Fuente: La Investigadora con datos de Empresa Gallup (2014)

Teniendo como premisa que Venezuela cuenta con un alto índice de inseguridad en el mundo y que está creciendo progresiva e indeteniblemente, aunado a una afectación económica continua producto de la inflación y los altos niveles de desabastecimiento, en algunos casos con ausencia casi total de algunos rubros de alimentos, medicinas y equipos de tecnología, entre otras deficiencias, se puede deducir que, los indicadores de seguridad no mejoran en corto plazo, lo que exige a las organizaciones tomar medidas para resguardar sus instalaciones y activos que en ella se encuentren, incrementando su necesidad de elevar los niveles de seguridad de acceso a fin de brindar tranquilidad a quienes forman parte de cada una de las áreas que en ella se encuentran.

Es por ello que resulta relevante y prioritario, en las organizaciones, contar con un sistema de control de acceso que garantice la protección frente a situaciones que puedan poner en riesgo la seguridad de las instalaciones de la organización y al personal que en ella labora, a un costo acorde a la realidad económica del país.

Un sistema de control de acceso es aquel que permite, de forma automática y efectiva, aprobar o negar el paso a una persona en sitios restringidos en función a ciertos parámetros establecidos. De igual manera, los sistemas de control de acceso permiten llevar un registro de los movimientos de los usuarios en un espacio determinado.

Estos sistemas de control de acceso ofrecen un método seguro de control mediante mecanismos de identificación y puntos de acceso. Entre los mecanismos se pueden mencionar tarjetas con banda magnética, tarjetas de identificación por radiofrecuencia, tarjetas de identificación mediante código de barra o componente biométrico mediante huella dactilar, reconocimiento facial, reconocimiento de iris, entre otros.

EDTEC es una empresa que provee servicios de desarrollo de software, capacitación personal, asesorías y consultorías en el área tecnológica y afines, situándose como una de las empresas de más rápido crecimiento a nivel nacional.

En ella labora personal altamente calificado y con mucha experiencia en las áreas de consultoría y asesoría integral y tecnológica.

Por ser una empresa con más de 10 años en el mercado, posee 18 oficinas administrativas y de gestión con un sostenido crecimiento y expansión a nivel nacional e internacional, por lo que también es necesario incrementar sus niveles de seguridad implementando un sistema de control de acceso a sus instalaciones que garantice la integridad y protección de sus activos tecnológicos y talento humano.

Actualmente el acceso del personal a las instalaciones de la empresa EDTEC, es realizado manualmente, teniendo en la entrada de cada una de las instalaciones, una persona autorizada para controlar el mismo, siendo el reconocimiento visual la principal forma de acceso de los empleados. Este proceso de verificar visualmente es lento e inseguro porque el personal encargado de restringir o aprobar el acceso a las instalaciones carece de información actualizada sobre el personal que labora en cada una de las instalaciones.

Aunado a la difícil tarea de controlar el acceso del personal a las instalaciones, hay que agregar el factor de la gran inseguridad que se vive actualmente en el país, situación que ha generado gran preocupación para la empresa, la cual pensando resguardar sus instalaciones y activos que en ella se encuentren, desea incrementar sus niveles de seguridad realizando un plan (proyecto) para implementar un sistema de control de acceso.

1.1.1 Formulación del Problema

¿Cuáles son los elementos que se deben tomar en cuenta para diseñar un plan para la implementación de un sistema de control de acceso a la empresa EDTEC?

1.1.2 Sistematización del Problema

¿Qué elementos tecnológicos deben ser considerados y evaluados para la implementación de un sistema de control de acceso a las instalaciones?

¿Cuál es el resultado de la factibilidad técnica asociada a la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC?

¿Cuál es la factibilidad económica financiera asociada a la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC?

¿Cuál son los elementos que debe tener un diseño de plan para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC?

¿Por qué puede fallar el plan diseñado?

1.2. Objetivos del Estudio

1.2.1. Objetivo General

Diseñar un plan para la implementación de un sistema de control de acceso a las instalaciones de una empresa de desarrollo tecnológico.

1.2.2. Objetivos Específicos

- ✓ Analizar los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso.
- ✓ Determinar la factibilidad técnica del proyecto para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC.
- ✓ Realizar el estudio de factibilidad económica financiero que permita determinar la viabilidad de implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC.
- ✓ Formular el plan para la implementación de un sistema de control de acceso a las instalaciones de la empresa objeto de estudio.
- ✓ Determinar los riesgos asociados al plan diseñado para la implementación del sistema de control de acceso.

1.3. Justificación de la investigación

En la actualidad la empresa EDTEC ha crecido tanto en infraestructura tecnológica como en el número de personal calificado en prestar los servicios de desarrollo de software, capacitación personal, asesorías y consultorías en el área tecnológica y afines, por lo que la implementación de un sistema de control de acceso tiene múltiples beneficios como la gestión de acceso al personal autorizado a las instalaciones y la seguridad de los equipos tecnológicos y del talento humano de la empresa para seguir brindando apoyo a los clientes en alcanzar sus objetivos empresariales.

Para garantizar la eficiencia y la puesta en marcha de cualquier proyecto, las organizaciones requieren aplicar metodologías que integren un conjunto de conocimientos mediante la planificación, control de costo y tiempo y el desempeño final del trabajo. En tal sentido, la realización de este trabajo de investigación permite obtener una visión clara, precisa y objetiva en base a datos e indicadores que reflejen si el plan diseñado, a proponer, para la implementación de un sistema de control de acceso es viable o no y en base a los resultados obtenidos en este estudio, se podrán tomar decisiones en cuanto a la ejecución o no del proyecto.

Es de resaltar, que el diseño de un plan de proyecto, aunado al beneficio de tener una visión clara de los objetivos del proyecto, permite:

- ✓ Mejorar los niveles de comunicación de las personas responsables del proyecto mediante flujos de trabajo y el conocimiento del rol que cada uno tiene dentro del mismo.
- ✓ Establecer metas y elegir los medios necesarios para alcanzarlas, proporcionando una herramienta de gran apoyo para el seguimiento y la toma de decisión.
- ✓ El ahorro de tiempo y costos mediante la asignación optimizada de los recursos al proyecto.

Adicionalmente, con el desarrollo de esta investigación, el autor logra profundizar los conocimientos previamente adquiridos durante los estudios de

la Especialización en Gerencia de Proyectos, con énfasis en el área de Definición y Desarrollo de Proyectos puesto que este estudio representa una implementación práctica de la teoría estudiada.

1.4. Alcance y Delimitaciones de la Investigación

El alcance de esta investigación comprende todo lo necesario para presentar el diseño de un plan para la implementación de un sistema de control de acceso, con todos los pasos necesarios para aplicarlo de una manera eficaz y trasparente causando el menor impacto posible.

Según Tamayo & Tamayo, (2004):

> "…toda investigación debe delimitarse en función del espacio y el tiempo, indicando la materia específica en la que se circunscribe, la población y muestra a la que es aplicable y el punto en el tiempo asociado al fenómeno de estudio. Estos límites contribuyen a fijar la duración de la investigación y evita trabajos inconclusos debido a temas muy extensos…", (p.120).

Para desarrollar la propuesta de este estudio, se consideraron las siguientes premisas:

No revelar la identidad de la empresa sobre la cual se desarrolló la investigación, para lo cual se utilizó la denominación genérica Empresa de Desarrollo Tecnológico EDTEC.

El presente estudio tuvo como finalidad diseñar un plan para implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC. Este plan se realizará de acuerdo a los requerimientos específicos de la empresa EDTEC en base a las mejores prácticas, de modo que satisfaga las necesidades por las cuales se emprende.

Este estudio incluye las fases de definición y planificación del proyecto, sin llegar a las fases de implementación ni evaluación, por lo que estas fases quedaron fuera del alcance del mismo.

CAPÍTULO II: MARCO TEORICO

Gómez (2006) indica que una vez planteado el problema de estudio, el siguiente paso consiste en sustentar teóricamente el estudio; ello implica analizar y exponer las teorías, los enfoques teóricos, las investigaciones y los antecedentes que se consideren pertinentes para el estudio. Es decir, en esta etapa se debe describir en qué estado está el conocimiento respecto al problema de la investigación, para luego fundamentar lo que se va a hacer.

Por su parte Rodríguez (2005), conceptualiza el marco teórico y conceptual como "La exposición resumida, concisa y pertinente del conocimiento científico y he hechos empíricamente acumulados acerca de nuestro objeto de estudio", añadiendo que "su preparación en cuanto al proceso de análisis y síntesis permite precisar, metodológicamente nuestro problema y la hipótesis correspondiente" (p.57)

2.1. Antecedentes

De acuerdo a lo expresado por Tamayo y Tamayo (2004) los antecedentes de un estudio "constituyen una síntesis conceptual de las investigaciones o trabajos realizados sobre el problema formulado con el fin de determinar el enfoque metodológico de la misma investigación" (p.149).

Para construir una síntesis conceptual de trabajos realizados que se encuentran estrechamente relacionados con el propósito de esta investigación, se tomaron en consideración los siguientes antecedentes:

Gutiérrez (2007) en su Trabajo Especial de Grado: **Estudio de Factibilidad para el Control de Acceso Biométrico, en una Empresa empleando lectores de huella digital**, para optar por el título Especialista en Gerencia de Proyectos en Ingeniería, realizó un estudio de factibilidad para comercializar el control de acceso biométrico, teniendo en cuenta costos, instalación y mantenimiento de este tipo de acceso. Este estudio aportó a la presente investigación, información sobre

elementos tecnológicos (software y hardware) que vienen siendo empleados desde hace varios años para el control de acceso y el reconocimiento e identificación de personas, como lo es la biometría. La biometría se ha convertido en un concepto popular en nuestros días por ser una técnica o herramienta confiable y segura que permite la identificación de personas mediante el análisis de aquellas características que tienen los individuos y que lo hacen único en comparación con los demás. Entre estas características podemos encontrar: huellas digitales, rasgos de la cara, el iris y la retina en los ojos, morfología de las manos, la voz y los olores corporales.

Palabras clave: Estudio de Factibilidad, Biometría, Reconocimiento de Huella Dactilar, Control de Acceso.

En este mismo orden de ideas, los autores Cortés, Medina y Muriel (2010). En su artículo **Sistemas de seguridad basados en biometría**, publicado en la revista "Scientia et Technica" indican que "los sistemas de seguridad basados en biometría son un medio eficaz y eficiente para el reconocimiento de ser humano" (p. 98), y que entre estos componentes destacan el reconocimiento facial o de rostro, el reconocimiento de la voz, el análisis del patrón de iris, el reconocimiento de las huellas dactilares, el análisis del mapa de la retina del ojo, el olor corporal, el análisis de la forma del oído, el análisis de la forma de la mano, la geometría de los dedos, la forma de la cabeza, el análisis del mapa de venas de la mano, etc., haciendo énfasis en el reconocimiento de la huella dactilar como una de las más usadas en el mundo.

Este artículo ayudó a ofrecer los elementos primordiales que deben tener los dispositivos biométricos:

> "El primer elemento hace referencia a la adquisición análoga o digital de algún indicador biométrico de una persona (por ejemplo la adquisición de una huella dactilar utilizando un escáner).
>
> El segundo elemento establece: La comprensión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados.

> Por último, se establece una interfaz con aplicaciones ubicadas dentro del mismo u otro sistema.” (p. 100)

Palabras clave: Biometría, Control, Huella Dactilar, Reconocimiento, Tratamiento Digital. Visual Studio Punto Net.

Por su parte, Bernal (2012) en su Trabajo Especial de Grado: **Estudio de Factibilidad para la Instalación de una Franquicia de Lavado Ecológico de Automóviles en la Ciudad de Puerto Ordaz, Estado Bolívar**, para optar por el título de Especialista en Gerencia de Proyectos, determinó la factibilidad para la instalación de una franquicia de lavado ecológico de automóviles en la ciudad de Puerto Ordaz, Estado Bolívar. En esta investigación se especifica que, de acuerdo a la técnica de evaluación de proyectos propuesta por Blanco (2010), un estudio de factibilidad debe tener tres fases principales:

a. Estudio de mercado
b. Estudio técnico
c. Estudio económico - financiero.

Este estudio de factibilidad realizado por Bernal (2012), apoyó la presente investigación en la identificación de la estructura que debe tener un estudio técnico (análisis de la tecnología e infraestructura requerida para la implementación, control de calidad, etc.) y un estudio económico financiero (materias primas o suministros, componentes de la inversión, gastos de fabricación o implementación, etc.).

A su vez, mediante este estudio, se pudo constatar que, aunque las técnicas de análisis empleadas para la evaluación de proyectos sirven para hacer una serie de determinaciones como mercado insatisfecho, costos totales, rendimiento de la inversión, etc., no elimina la necesidad de tomar una decisión, pues el estudio no decide por sí mismo.

Palabras clave: Factibilidad, Lavado Ecológico, Automóviles, Carros de Lavado Autónomo, Franquicia.

Aunado a lo anterior, Alves, Benedetto, Etchart, Luna, Leal, Fernández, Berón, y Loggio (2014), en su artículo **Identificación de Personas Mediante Sistemas Biométricos. Estudio de Factibilidad y su Implementación en Organismos Estatales**, analizaron las dificultades en los procedimientos de autentificación de personas en organismos públicos e implementaron posibles soluciones a través de la utilización de sistemas biométricos. Este estudio aporta información relevante de los sistemas biométricos utilizados en la actualidad, los cuales se encuentran clasificados en dos grandes grupos: estáticos y dinámicos. Dentro del primer grupo, se ubican las características que se enfocan en aspectos estructurales y por lo tanto se encuentran vinculadas a determinados órganos y sistemas, como la cara, la mano, el iris, la piel, las venas, las huellas dactilares y el olor químico corporal, mientras que en el segundo grupo se encuentran las características de tipo funcional, tales como el habla, la voz, la escritura manuscrita y el reconocimiento de la firma escrita. A su vez, indican que es deseable que un sistema biométrico contemple las siguientes propiedades:

a. “Unicidad: Significa que no deben existir dos individuos que posean la misma característica. La unicidad debe ser distinguible, aunque sea única.

b. Fiabilidad: Se la suele denominar también como rendimiento (performance) o nivel de exactitud. La fiabilidad de un sistema es la probabilidad de que ese sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período de tiempo determinado. Esta característica, hace referencia a la precisión del reconocimiento, los recursos requeridos y el entorno operativo.

c. Facilidad de uso: Tiempo en el que los nuevos usuarios desarrollan una interacción efectiva con el sistema o producto. Está relacionada con la predictibilidad, la familiaridad, la generalización de los conocimientos previos y la consistencia.

d. Resistencia a ataques: Se la suele denominar también como resistencia del sistema biométrico a ser burlado. El término se refiere a la preparación y disposición que se hace anticipadamente para evitar un riesgo ante posibles intentos de violación al sistema.

e. Aceptabilidad: Significa el grado de aceptación de las personas en base a su cultura, al hecho de que no perjudique a las personas y que además sea higiénica.

f. Costo aceptable: Los componentes del costo en cualquier sistema biométrico incluyen hardware y software asociado para capturar la biometría, instalación, incluyendo los sueldos del equipo encargado de la implementación, montaje, conexión e integración del sistema de usuarios, capacitación de los mismos, alternativas para usuarios que no pueden registrarse, mantenimiento del sistema, administración de bases de datos centralizadas de imágenes/plantillas biométricas y poder de procesamiento del programa de respaldo.” (p. 52)

Palabras clave: Sistemas Biométricos, Identificación de Personas, Organismos Estatales, Seguridad y Control.

Por otra parte, Poveda y Merchán (2015), en su artículo **Implementación de un Sistema de Control de Acceso basado en Reconocimiento Facial**, presentan aspectos de la implementación de un sistema de control de acceso basado en reconocimiento facial. El mismo verifica en tiempo real si las personas que entran a las instalaciones de la Universidad Tecnológica de Panamá (UTP) forman parte de la base de datos del personal que labora en las mismas. Este artículo aporta a la presente investigación, elementos de innovación en materia de biometría para el control de acceso y seguridad de las instalaciones donde se implemente, aplicando un corrector de falsos positivos y disminución de los tiempos de búsqueda mediante el método de Viola & Jones, aunque este método se usa exclusivamente para el reconocimiento facial.

Palabras clave: Reconocimiento Facial, Extracción de Características, Sistema Biométrico, Fisherfaces, Control de Acceso.

2.2. Fundamentos Teóricos

Según Balestrini (2002) el marco teórico es:

> "El resultado de la selección de aquellos aspectos más relacionados del cuerpo teórico epistemológico que se asume, referidos al tema específico elegido para su estudio". (p.91)

De allí pues, que su racionalidad, estructura lógica y consistencia interna, va a permitir el análisis de los hechos conocidos, así como, orientar la búsqueda de otros datos relevantes.

Con el objeto de brindar el apoyo conceptual a la presente investigación, se consideran los siguientes aspectos teóricos.

- **Proyecto:** Según el PMI (2013) “un proyecto es un esfuerzo temporal realizado para crear un producto, servicio o resultado único” (p.4). Todos los proyectos tiene la característica de ser temporal lo que implica que tiene un principio y un final definido. El final se alcanza cuando se logran los objetivos del proyecto, cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto.

  De igual manera, los autores Sapag y Sapag (2007, p.1) definen un proyecto como “la búsqueda de una solución inteligente al planteamiento de un problema tendiente a resolver, entre tantas, una necesidad humana.”

  Por su parte, Palacios (2009) indica que un proyecto es un trabajo que se realiza en una organización con el objetivo de dirigirse a una situación deseada, definiéndolo como “un conjunto de actividades orientadas a un fin común, que tienen un comienzo y una terminación. Son respuestas inteligentes para atender a los requerimientos o necesidades del mercado” (p.27).

A su vez, Gray y Larson (2009) definen un proyecto como un esfuerzo complejo, no rutinario, limitado por el tiempo, el presupuesto, los recursos y las especificaciones de desempeño para cumplir las necesidades del cliente.

Todos los autores coinciden en el concepto de temporalidad, esto debido a que los proyectos tienen un comienzo y final definido, dejando claro que temporal no necesariamente ha de ser corta duración, pero siempre un proyecto va a tener una duración limitada.

- **Ciclo de vida de un proyecto:** Un ciclo de vida de un objeto o sistema es el conjunto de etapas o fases en las cuales evoluciona este objeto o sistema, desde que nace hasta que finaliza. Para el PMI (2013) el ciclo de vida de los proyectos se define como “la serie de fases por las que atraviesa un proyecto desde su inicio hasta su cierre. Las fases son generalmente secuenciales y sus nombres y números son determinados por las necesidades de gestión y control de la organización u organizaciones que participan en el proyecto” (p.38).

Por su parte, Lledó y Rivarola (2007), definen el ciclo de vida como un conjunto de fases que permiten hacer más eficiente la administración del proyecto, produciéndose distintos entregables en cada una de ellas.

Chamoun (2002) indica que las fases de la vida de un proyecto son las siguientes:

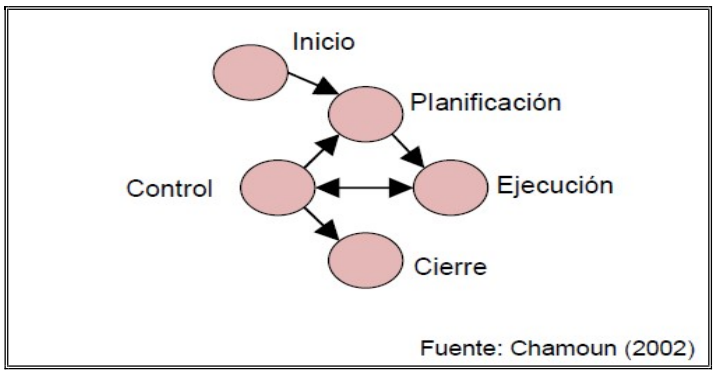


Figura 2: Ciclo de vida de los proyectos

a. Inicio: en esta fase se establece la visión del proyecto y los objetivos a alcanzar.
b. Planificación: es la fase en la cual se desarrolla el plan que permitirá alcanzar los objetivos del proyecto.
c. Ejecución: en esta fase se llevan a cabo las tareas que permitirán desarrollar el proyecto, se incluyen actividades como contratación, compras, distribución de información, etc.
d. Control: en esta fase se evalúa el avance del proyecto comparando lo planificado con lo ejecutado, realizando los cambios que sean necesarios para corregir cualquier desviación.
e. Cierre: el cierre es la fase en la cual se realizan las actividades de conclusión del proyecto, tales como cierre de contratos y elaboración de memoria.

- **Gerencia de Proyecto:** Para el PMI (2013) la gerencia o dirección de proyectos se define como "la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo" (p.5). Por su parte, Llorens Fábregas (2005) conceptualiza la gerencia de proyectos como "un arte que requiere imaginación, flexibilidad, creatividad y capacidad de anticipación para ser exitosa" (p.10).

Por otra parte, Torres Hernández y Torres Martínez (2014) establecen que dirigir un proyecto por lo general implica:

a. Identificar requisitos.
b. Abordar las diversas necesidades, inquietudes y expectativas de los interesados según se planifica y efectúa el proyecto.
c. Equilibrar las restricciones contrapuestas del proyecto que se relacionan entre otros aspectos con el alcance, la calidad, el cronograma, el presupuesto, los recursos y el riesgo.

Todos estos autores coinciden al indicar que los objetivos de la gerencia de proyecto están ligados a lograr que el proyecto alcance los

resultados esperados, en el plazo y con los costos de ejecución que oportunamente acordaron.

La administración o gestión de proyectos basada en el modelo expuesto en el PMI (2013), se lleva a cabo mediante la realización de procesos que cubren diez áreas de conocimientos a través del ciclo de vida del proyecto, permitiendo de esta forma la ejecución eficaz del mismo y el logro de los objetivos planteados.

- **Áreas de conocimiento de la gerencia de proyectos:**

a. Gestión de la integración del proyecto: de acuerdo a lo expresado en la guía de fundamentos para la dirección de proyectos en el PMI (2013) , esta área incluye los procesos y actividades necesarios para identificar, definir, combinar, unificar y coordinar los diversos procesos y actividades de la dirección de proyectos dentro de los grupos de procesos de dirección de proyectos.

   Los procesos de la gestión de integración del proyecto incluyen:

   - Desarrollar el acta de constitución del proyecto.
   - Desarrollar el plan para la dirección del proyecto.
   - Dirigir y gestionar el trabajo del proyecto.
   - Monitorear y controlar el trabajo del proyecto.
   - Realizar el control integrado de cambios.
   - Cerrar el proyecto o fase.

b. Gestión del alcance del proyecto: el PMI (2013) establece que ésta área de conocimiento se enfoca primordialmente en definir y controlar qué se incluye y qué no se incluye en el proyecto.

   Los procesos de la gestión del alcance del proyecto incluyen:

   - Planificar la gestión del alcance.
   - Recopilar requisitos.
   - Definir el alcance.

- Crear la EDT/WBS.
- Validar el alcance.
- Controlar el alcance.

c. Gestión del tiempo del proyecto: “incluye los procesos requeridos para gestionar la terminación en plazo del proyecto” (PMI, 2013, p.140).

   Los procesos de la gestión del tiempo del proyecto incluyen:

   - Planificar la gestión del cronograma.
   - Definir las actividades.
   - Secuenciar las actividades.
   - Estimar los recursos de las actividades.
   - Estimar la duración de las actividades.
   - Desarrollar el cronograma.
   - Controlar el cronograma.

d. Gestión de los costos del proyecto: según PMI (2013), esta área de conocimiento incluye los procesos relacionados con planificar, estimar, presupuestar, financiar, obtener financiamiento, gestionar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado.

   Los procesos de la gestión de los costos del proyecto incluyen:

   - Planificar la gestión de los costos.
   - Estimar los costos.
   - Determinar el presupuesto.
   - Controlar los costos.

e. Gestión de la calidad del proyecto: la Gestión de la Calidad del Proyecto, de acuerdo a lo expresado en el PMI (2013), utiliza políticas y procedimientos para implementar el sistema de gestión de la calidad de la organización en el contexto del proyecto, y, en la

forma que resulte adecuada, apoya las actividades de mejora continua del proceso, tal y como las lleva a cabo la organización ejecutora.

Los procesos de la gestión de la calidad del proyecto incluyen:

- Planificar la gestión de la calidad.
- Realizar el aseguramiento de calidad.
- Controlar la calidad.

f. Gestión de los recursos humanos del proyecto: la gestión de los recursos humanos “incluye los procesos que organizan, gestionan y conducen al equipo del proyecto” (PMI, 2013, p.254).

   Los procesos de la gestión de los recursos humanos del proyecto incluyen:

   - Planificar la gestión de los recursos humanos.
   - Adquirir el equipo del proyecto.
   - Desarrollar el equipo del proyecto.
   - Dirigir el equipo del proyecto.

g. Gestión de las comunicaciones del proyecto: esta área de conocimiento “incluye los procesos requeridos para asegurar que la planificación, recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados.” (PMI, 2013, p.286).

   Los procesos de la gestión de las comunicaciones del proyecto incluyen:

   - Planificar la gestión de las comunicaciones.
   - Gestionar las comunicaciones.
   - Controlar las comunicaciones.

h. Gestión de los riesgos del proyecto: de acuerdo a lo establecido en el PMI (2013) esta área de conocimiento “incluye los procesos para llevar a cabo la planificación de la gestión de riesgos, así como la identificación, análisis, planificación de respuesta y control de los riesgos de un proyecto” (p.308).

   Los procesos de la gestión de los riesgos del proyecto incluyen:

   - Planificar la gestión de los riesgos.
   - Identificar los riesgos.
   - Realizar el análisis cualitativo de los riesgos.
   - Realizar el análisis cuantitativo de los riesgos.
   - Planificar las respuestas a los riesgos.
   - Controlar los riesgos.

i. Gestión de las adquisiciones del proyecto: la gestión de las adquisiciones “incluye los procesos necesarios para comprar o adquirir productos, servicios o resultados que es preciso obtener fuera del equipo del proyecto” (PMI, 2013, p.354).

   Los procesos de la gestión de las adquisiciones del proyecto incluyen:

   - Planificar la gestión de las adquisiciones.
   - Efectuar las adquisiciones.
   - Controlar las adquisiciones.
   - Cerrar las adquisiciones.

j. Gestión de los interesados del proyecto: La Gestión de los Interesados del Proyecto “incluye los procesos necesarios para identificar a las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto, para analizar las expectativas de los interesados y su impacto en el proyecto, y para desarrollar estrategias de gestión adecuadas a fin de lograr la participación

eficaz de los interesados en las decisiones y en la ejecución del proyecto" (PMI, 2013, p.390).

Los procesos de la gestión de los interesados del proyecto incluyen:

- Identificar a los interesados.
- Planificar la gestión de los interesados.
- Gestionar la participación de los interesados.
- Controlar la participación de los interesados.

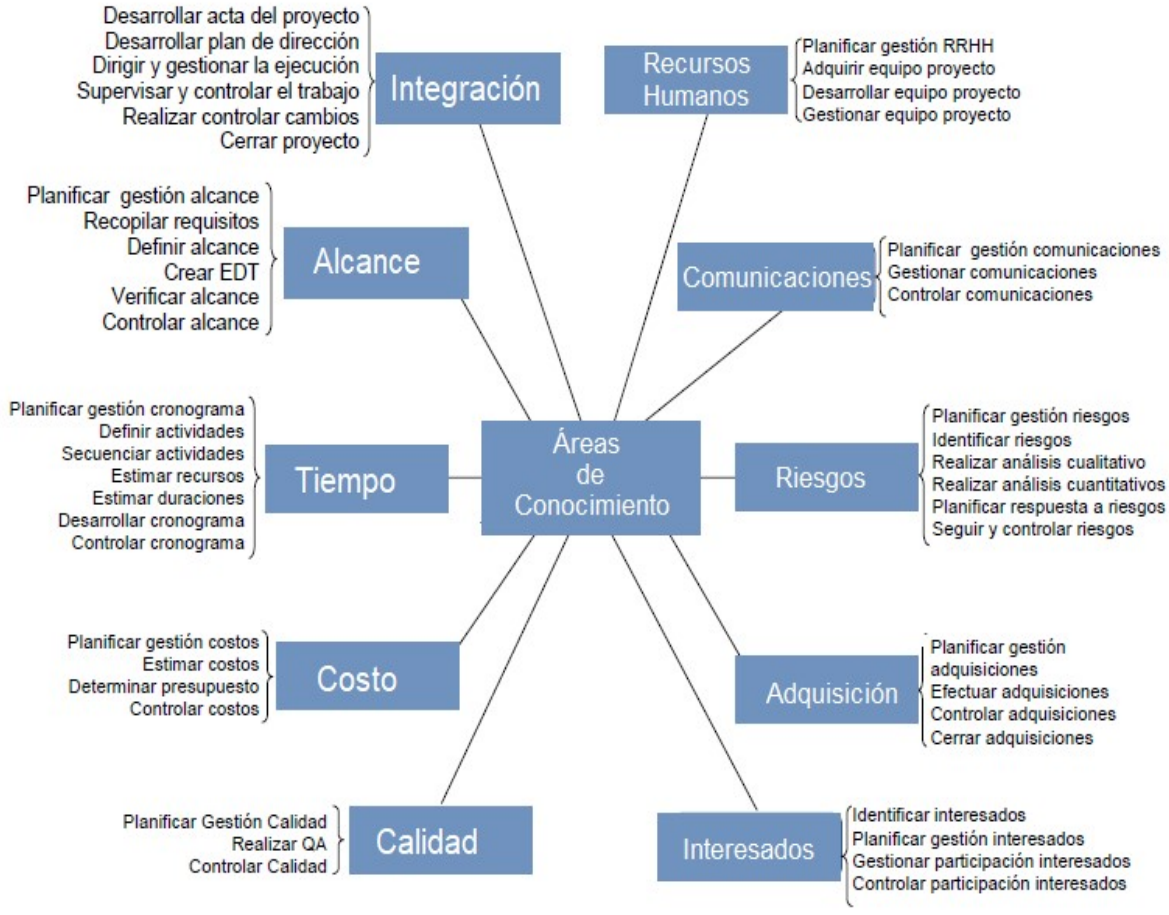


Figura 3: Áreas de conocimiento en la gerencia de proyectos

Fuente: La investigadora con datos del PMI (2013)

- **Dispositivos de reconocimiento:** Son herramientas que se utilizan para identificar de manera inequívoca a personas, comparando características extraídas con los patrones de los usuarios registrados en un sistema. Estos dispositivos podemos clasificarlos en Biométricos y no biométricos.

    - Biométricos: Los dispositivos biométricos son usados en sistemas computarizados de seguridad, principalmente para identificar atributos físicos. Estos han sido diseñados para máximos estándares de seguridad y múltiples aplicaciones. Coronel (2017) expresó que un sistema biométrico es un sistema de identificación de personas que se sirve de la biometría informática para condicionar el acceso a un bien o servicio. Los mecanismos de control automáticos de acceso a bienes o servicios incluyen, además, bases de datos y sistemas físicos como puertas de acceso controladas electrónicamente".

        - Etapas en un sistema de identificación biométrica:

            - Captura: Se toman los datos biofísicos, evidentemente depende de la técnica biométrica seleccionada. Esta fase es muy importante ya que en ella está contenida la interfaz hombre máquina y el sensor para la captura de información biométrica.

            - Procesamiento: los datos biofísicos capturados se procesan, para posteriormente extraer un patrón, el cual se almacenara y será el conjunto de datos que caracterizara a ese usuario.

            - Utilización: Una vez que se tiene almacenado el patrón del usuarios, este puede utilizar el sistema con normalidad, y sus características son comparadas con el patrón almacenado.

- Comparación: Una vez extraídas las características, almacenadas y utilizadas se procede a realizar la comparación tomando una nueva captura para ser comparada con las almacenadas dando como resultado un puntaje o probabilidad de semejanza.

- Autenticación: Si la comparación supera un determinado umbral de similitud, se considera que el usuario es el indicado, rechazando la comparación en caso contrario.

- Técnicas de Identificación biométricas:
  - Geometría de mano.
  - Reconocimiento de huella dactilar.
  - Reconocimiento de voz.
  - Reconocimiento facial o de rostro.
  - Reconocimiento mediante el escaneo del iris.
  - Reconocimiento mediante firma.

- Tasas de errores de los sistemas biométricos: Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas de un sistema de control de acceso por biometría:
  - Una persona autorizada es aceptada
  - Una persona autorizada es rechazada
  - Un impostor es rechazado
  - Un impostor es aceptado

  Estas estadísticas anteriores se utilizan para establecer dos tasas de errores:
  - Tasa de falsa aceptación (FAR: False Acceptance Rate) que se define como la frecuencia relativa con

que un impostor es aceptado como un individuo autorizado.

- Tasa de falso rechazo (FRR: False Rejection Rate) definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.

- **Identificación por radiofrecuencia (No biométrico):** El sistema de identificación por radiofrecuencia o RFID (Radio Frequency Identification) es un sistema inalámbrico de almacenamiento y recuperación de datos que usa ondas de radio para determinar la identificación de pequeños dispositivos denominados etiquetas o tags RFID.

  De acuerdo con lo expresado por Vargas (2013) existen 3 componentes básicos en un sistema de RFID:

  - El tag, etiqueta o transponder: consiste en un pequeño circuito, integrado con una pequeña antena, capaz de transmitir un número de serie único hacia un dispositivo de lectura, como respuesta a una petición.

  - El lector: está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control.

  - Un controlador o equipo anfitrión: comúnmente una PC en la cual corre una base de datos y algún software de control.

- **Software:** De acuerdo a lo expresado por la Real Academia Española (2001), el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.

- **Hardware:** La Real Academia Española (2001) también define al hardware, como el conjunto de los componentes que conforman la parte material (física) de una computadora, a diferencia del software que

refiere a los componentes lógicos (intangibles). Sin embargo, el concepto suele ser entendido de manera más amplia y se utiliza para denominar a todos los componentes físicos de una tecnología.

- **Bases de datos:** Se conoce como base de datos al conjunto de informaciones que está organizado y estructurado de un modo específico para que su contenido pueda ser tratado y analizado de manera rápida y sencilla.

- **Servidores:** Cobo, Gómez, Pérez y Rocha (2005) conceptualizan los servidores como ordenadores que ofrecen sus servicios al resto de equipos conectados. En ellos es donde se encuentran alojadas páginas web, base de datos y aplicaciones entre otras.

- **Estudio de Factibilidad:** un estudio de factibilidad se formula con base en información que tiene la menor incertidumbre posible para medir las posibilidades de éxito o fracaso de un proyecto de inversión, apoyándose en el estudio de factibilidad se tomará la decisión de proceder o no con su implementación. De acuerdo a lo expresado por Baca (2010), en un estudio de factibilidad se plantean dos (2) objetivos fundamentales, que son:

    - Analizar y presentar todas las variables que condicionan la realización de la futura inversión, destacando las más complejas e importantes para el proyecto.

    - Demostrar la rentabilidad económica para el capital invertido y para los recursos económicos comprometidos en el proyecto (p.2).

- **Factibilidad Técnico de un Proyecto:** la factibilidad técnica se determina con el estudio técnico del proyecto. Sapag y Sapag (2007) indican que: “El estudio técnico tiene por objetivo proveer información para cuantificar el monto de las inversiones y de los costos de operación

pertinentes a esta área" (p.19). El estudio técnico pretende resolver las preguntas referentes a dónde, cuándo, cuanto, cómo y con que producir lo que se desea.

- **Factibilidad Económica y Financiera de un Proyecto:** el objetivo del estudio financiero pretende determinar el monto de los recursos económicos necesarios para la realización del proyecto, la duración del periodo de inversión, las fuentes de financiamiento y el costo total de la implementación de la solución a un problema, (Baca, 2010, p.160) mientras que el estudio económico tiene como propósito determinar si la inversión propuesta será económicamente rentable (Baca, 2010, p.160).

2.3. Bases Legales

Según Villafranca (2002) "Las bases legales no son más que se leyes que sustentan de forma legal el desarrollo del proyecto". A su vez, indica que las bases legales "son leyes, reglamentos y normas necesarias en algunas investigaciones cuyo tema así lo amerite" (p.51).

A continuación se presentan las bases legales que sustentan el presente estudio:

La Ley Especial contra los Delitos Informáticos publicada en Gaceta Oficial de la República Bolivariana de Venezuela número 37.313 del 30 de octubre de 2001, que regula el comportamiento de los ciudadanos en materia informática, estipula que:

Artículo 11: "Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones

afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado".

El artículo anterior estipula la sanción por obtener, revelar y difundir información de los sistemas que sean implementados. Resulta relevante para la investigación contar con una norma que permita limitar a cualquier persona natural o jurídica en cuanto al mal uso o espionaje de las bases de datos que se destinen para el resguardo o digitalización de información perteneciente al personal de una institución

Artículo 21: "Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos, señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa".(p. 6).

Lo anterior, se refiere a la interferencia en la información, es decir, que capture información legal y la modifique o la utilice para su beneficio o para terceros será penado por dos años de prisión. Este Artículo de la Ley Especial Contra Los Delitos Informáticos tiene una muy preponderante relevancia a la problemática planteada, ya que es la norma más próxima a combatir el fraude tecnológico y la extorsión informática.

En esta misma línea de basamento legal, se encuentra el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas publicada en Gaceta Oficial de la República Bolivariana de Venezuela número 37.148 del 28 de febrero de 2001, mediante el decreto número 1.181, que tiene por objeto otorgar y reconocer eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y los certificados electrónicos.

Este Decreto-Ley será aplicable a los mensajes de datos y firmas electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, esta norma se puede concatenar al objeto de estudio de la investigación debido a que los sistemas de control de acceso manejan una forma de reconocimiento electrónico.

2.4. Definición de Términos

Biometría: de acuerdo a los autores Cortés, Medina, y Muriel (2010), la biometría o biométrica proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo sistema y dispositivo biométrico se encarga de medir e identificar alguna característica propia de los seres vivos.

Geometría de mano: es un método de identificación o reconocimiento mediante características geométricas de las manos. Cortés, Medina y Muriel (2010) indican que este método de reconocimiento es mucho más eficiente que el de huellas dactilares, ya que al leer la mano de forma completa, permite capturar muchas más variables como imágenes individuales de algunos dedos y extraer datos como longitudes, anchuras, alturas, posiciones relativas y articulaciones entre otras.

Identificación: acción de identificar o identificarse. De acuerdo a lo expresado por los autores Alves, Benedetto, Etchart, Luna, Leal, Fernández, Berón y Loggio (2014), la identificación en la biometría es una tarea donde el sistema intenta determinar la identidad de alguien comparándola con todas los registros existentes en una base de datos.

Identificación a través de tarjetas magnéticas: es un método de identificación eficiente pero su nivel de seguridad es mucho menor, pues se presta a suplantaciones por pérdida o avería. Este método de reconocimiento permite el acceso mediante el uso de la tecnología RFID (Radio Frequency Identification o Identificación por Radiofrecuencia) permite la lectura y escritura de datos a distancia de las tarjetas usando la transmisión por radiofrecuencia.

Reconocimiento de huella dactilar: Cortés, Medina, y Muriel (2010), indican que el reconocimiento de huellas dactilares es otra de las técnicas más usadas y fiables a nivel mundial y, además, se utiliza en numerosas aplicaciones por ser rápido y de bajo costo. Consta de un dispositivo capaz de leer, guardar e identificar las huellas dactilares. La identificación con huellas dactilares está basada principalmente en la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, y valles.

Reconocimiento de voz: consiste en conocer la identidad de una persona a partir de las características únicas de su voz. Este proceso se basa en la medida de parámetros fisiológicos, por lo que también se conoce como biometría de voz. Alves, Benedetto, Etchart, Luna, Leal, Fernández, Berón y Loggio (2014) indican que:

> "Esta modalidad biométrica presenta algunos desafíos únicos que no se encuentran en otras formas de reconocimiento humano y es que tienen que lidiar con los distintos acentos dentro de un idioma y las diferentes formas de hablar de cada persona. Para esto lo primero es obtener la huella vocal, que se puede sacar haciendo una captura dinámica mientras la persona habla. Esta huella registra las características de la voz, como pueden ser el timbre, el agudo, la edad o si es masculina o femenina. Pero también determina cuál es el canal por el que se está hablando, de manera que establece el posible grado de distorsión para ser capaz de reconocer al usuario a través de otro canal." (p.56).

Reconocimiento facial o de rostro: El reconocimiento de rostro, actualmente, es menos exacto que el análisis de huellas dactilares. Cortés, Medina y Muriel (2010) establecen que los sistemas basados en reconocimiento facial clasifican la apariencia de la persona e intenta medir algunos puntos nodales del rostro como la distancia entre los ojos, el ancho de la nariz, la distancia del ojo a la boca, o la longitud de la línea de la mandíbula.

Reconocimiento mediante el escaneo del iris: El reconocimiento de iris es un método de autenticación biométrica que utiliza técnicas de reconocimiento de patrones (los cuales, han sido almacenados anteriormente en una base de datos) en imágenes de alta resolución del iris del ojo de un individuo. De acuerdo a lo

expresado por Alves, Benedetto, Etchart, Luna, Leal, Fernández, Berón y Loggio (2014), la ventaja de este método es que los patrones de iris son invariables en el tiempo y su falsificación es muy difícil. Cabe destacar además, que no se tiene la necesidad de contacto directo con el dispositivo de captura, lo que lo hace menos intrusivo, y extiende la vida útil del dispositivo. El reconocimiento del iris utiliza la tecnología de las cámaras: con una fina iluminación infrarroja se reduce el reflejo que se haya podido producir en la convexa córnea y poder crear detalladas imágenes de las complejas estructuras del iris. Una vez convertidas en plantillas digitales, estas imágenes proporcionan una representación matemática del iris, las cuales coinciden con una identificación positiva e inequívoca de un individuo.

Reconocimiento mediante firma: De acuerdo a lo expresado por Cortés, Medina y Muriel (2010), es la técnica biométrica que consiste en el reconocimiento a través de una firma, entre las ventajas que tiene es que es muy económica si se requiere implementar. Un sistema de este tipo solo necesita una tableta de escritura conectada al computador. El escaneo de la firma se analiza desde dos puntos de vista, siendo estos la firma en sí y el modo en que se efectúa. Los datos almacenados incluyen la velocidad, la presión, la dirección, el largo del trazado y las áreas donde el lápiz se levanta. El gran inconveniente de este método es que una persona nunca firma de manera idéntica dos veces.

Sistema de control de acceso: es aquel que permite, de forma automática, aprobar o negar el paso de una persona a sitios restringidos en función a ciertos parámetros establecidos.

Sistemas de reconocimiento biométricos: De acuerdo a Alves, Benedetto, Etchart, Luna, Leal, Fernández, Berón y Loggio (2014), estos sistemas, reconocen a una persona en base a características físicas (huellas dactilares, rasgos de la mano o de la cara, patrones del iris) o características conductuales aprendidas o adquiridas (patrones de voz, patrones de firma ológrafa, patrones de tipeo).

CAPITULO III: MARCO METODOLÓGICO

De acuerdo a Balestrini (2002), el marco metodológico "está referido al momento que alude al conjunto de procedimientos lógicos, tecno-operacionales implícito en todo proceso de investigación, con el objeto de ponerlos de manifiesto y sistematizarlos" (p.125)

A continuación se presenta el marco metodológico de la presente investigación.

3.1. Tipo de Investigación

El objetivo de la presente investigación está orientado a diseñar un plan para la implementación de un sistema de control de acceso para las instalaciones de una empresa de desarrollo tecnológico EDTEC. En tal sentido, el estudio se enmarcó como una investigación proyectiva o investigación – desarrollo.

De acuerdo a lo expresado por Hurtado (2000) las investigaciones proyectivas son "todas aquellas investigaciones que conducen a inventos, programas, diseños o a creaciones dirigidas a cubrir una determinada necesidad, y basadas en conocimientos anteriores" (p. 323). La investigación proyectiva consiste en encontrar la solución a los problemas prácticos, se ocupa de cómo deberían ser las cosas para alcanzar los fines y funcionar adecuadamente.

De lo expuesto anterior, se puede deducir que el presente estudio corresponde al tipo de Investigación Proyectiva.

Por otra parte, según los tipos de investigación propuestos por Valarino, Yáber y Cemborain (2010), la presente investigación es de tipo "Investigación - Desarrollo", ya que la misma tiene como objetivo ofrecer una propuesta para satisfacer una necesidad real, pero no lleva consigo la acción de implantarla.

3.2. Diseño de la Investigación

Con relación al diseño de la investigación, Arias (2006) lo define como “La estrategia general que adopta el investigador para responder al problema planteado” (p.26).

El diseño de la investigación es de tipo documental, no experimental, transeccional. La investigación documental es conceptualizada como “el estudio de problema con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en fuentes bibliográficas y documentales” (UPEL, 1990, p.6).

Por su parte, el diseño de investigación no experimental es aquel que se realiza sin manipular deliberadamente variables, basándose fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para después analizarlos.

Los diseños transeccionales recolectan datos en un solo momento, en un tiempo único, siendo su principal propósito el describir variables, y analizar su incidencia e interrelación en un momento dado (Tecnicas-de-estudio.org, 2017).

3.3. Unidad de análisis

De acuerdo a lo expresado por Rada (2007), “La unidad de análisis corresponde a la entidad mayor o representativa de lo que va a ser objeto específico de estudio en una medición y se refiere al qué o quién es objeto de interés en una investigación” (p. 1).

Por otra parte, tomando como referencia lo expresado por Hernández, Fernández y Baptista (2003), donde conceptualizan la unidad de análisis como “personas, contextos, eventos, sucesos, comunidades de análisis sobre el cuál se habrán de recolectar los datos” (p. 302), se puede decir que la unidad de análisis para este estudio estuvo conformada por las áreas consideradas vulnerables de la empresa de desarrollo tecnológico EDTEC, en las cuales se requiera de la implementación de un sistema de control de acceso.

3.4. Técnicas e Instrumentos de recolección de datos

De acuerdo a los expresado por Hurtado (2010) las técnicas de recolección "tienen que ver con los procedimientos utilizados para la recolección de datos, es decir, el cómo. Estas pueden ser de revisión documental, observación, encuesta y técnicas sociométricas, entre otras" (p. 153). Conjuntamente con las técnicas de recolección deben identificarse los instrumentos mediante los cueles se recabarán y registrarán los datos que se desprenderán del estudio. Valarino et al (2010) indican los siguientes: "cuestionario o inventario, las pruebas (test) y el sociograma, las escalas objetivas, los grupos focales o focus group, el panel y el Delphi, los documentos, registros, materiales,…" (p.128).

Arias (2004) identifica dos tipos de instrumentos para la investigación documental: revisión o análisis documental y análisis de contenido.

De lo antes expuesto y con base al diseño adoptado en esta investigación, para la realización de la misma se emplearán las técnicas siguientes: revisión documental mediante observación directa y entrevista no estructurada, utilizando los instrumentos de ficha resume de datos, blog de anotaciones y guía de entrevista no estructurada.

De acuerdo a lo expresado por Veliz (2007):

> "la observación es una técnica que se debe emplear para relacionar el sujeto de estudio con el objeto, dotando al investigador de una teoría y un método adecuado para que la investigación tenga una orientación correcta y el trabajo de campo arroje datos exactos y confiables" (p. 79).

En cuanto a los instrumentos de esta técnica de observación, la utilización de una ficha resume de datos, pretende dejar un registro manual de todas las características, procesos y aspectos importantes que se observen en la revisión documental.

Por otra parte, Arias (2006) en cuanto a la entrevista no estructurada afirma que: "más que un simple interrogatorio, es una técnica basada en un diálogo o conversación entre el entrevistador y el entrevistado acerca de un tema

previamente determinado, de tal manera que el entrevistador pueda obtener la información requerida" (p. 73)

El análisis de los datos recabados, contribuirá a la determinación de los requerimientos y plataforma necesaria para el sistema de control de acceso, así como las políticas existentes en la empresa con respecto al control de acceso a las instalaciones por parte de sus empleados.

3.5. Fases de la Investigación

Todo estudio o investigación debe recorrer una serie de etapas o fases sucesivas, esta estructura permitirá facilitar la planificación del presente estudio. Valarino et al (2010) indican que "una fase está compuesta por una serie ordenada o jerarquizada de actividades y tareas relacionadas para lograr un objetivo" (p. 206). Mediante la estructuración en fases se podrá saber quién está involucrado en cada etapa, que tipo de trabajo será necesario en cada etapa y cuál es el resultado que cada etapa deberá producir. El presente trabajo se planteó bajo la siguiente estructura de fases:

- ✓ Fase I: descripción y definición del proyecto. Se desarrolla el capítulo I de la presente investigación realizando el planteamiento del problema, la formulación de los objetivos, la justificación de la investigación el alcance y la delimitación de la investigación, analizando las causas, los efectos y el impacto de la situación planteada que orientarán el logro de los resultados.

- ✓ Fase II: definición de las bases teóricas, los antecedentes de la investigación y las bases legales. Los antecedentes son estudios previos que constituyen una síntesis conceptual de las investigaciones o trabajos realizados sobre el diseño de un plan para la implementación de un sistema de control de acceso con el fin de determinar el enfoque metodológico de la misma investigación y los fundamentos teóricos son los elementos de la teoría más relacionados con el estudio, el cual sustenta el análisis de los datos requeridos para el elaborar un plan para la implementación de un

sistema de control de acceso. En esta fase también se define las bases que sustentan de forma legal el desarrollo del proyecto.

- ✓ Fase III operacionalización de los objetivos, definir la unidad de análisis, determinar los instrumentos y técnicas de recolección de datos, especificar el cronograma de la investigación, los aspecto éticos a considerar y los recursos necesarios para llevarla a la cabo, así como realizar la estructura desagregada de trabajo la cual consiste en la descomposición jerárquica, orientada al entregable, del trabajo a ser realizado en el proyecto.
- ✓ Fase IV: recopilar la información de la empresa de desarrollo tecnológico EDTEC, como su misión, visión, reseña histórica y organigrama general.
- ✓ Fase V: recabar los datos requeridos en la investigación, analizar el mercado referente a los distintos dispositivos que son utilizados en los sistemas de control de acceso, realizar el estudio de factibilidad técnica, económica y financiera.
- ✓ Fase VI: realizar el diseño del plan para la implementación de un sistema de control de acceso a las instalaciones de la empresa de desarrollo tecnológico EDTEC y analizar los riesgos asociados al mismo.

3.6. Procedimientos por Objetivos

Analizar los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso.

- ➢ Recolección de datos.
- ➢ Realizar la revisión documental como técnica de recolección de datos para validar las características del producto, precio y oferta.

Determinar la factibilidad técnica del proyecto para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC.

- Recolección de datos.
- Realizar la revisión documental mediante la observación directa así como entrevistas no estructuradas a fuentes directas y expertos en la empresa de desarrollo EDTEC para validar la factibilidad técnica en cada uno de los elementos empleados para el reconocimiento de personas que son comúnmente incluidos en un sistema de control de acceso. Esta factibilidad técnica tiene como objetivo identificar el tipo de maquinaria o equipo que puede ser usado, la capacidad instalada y utilizada en la empresa y los elementos de infraestructura requeridos para la implementación de un sistema de control acceso.

Realizar el estudio de factibilidad económica financiero que permita determinar la viabilidad de implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC.

- Recolección de datos.
- Realizar la revisión documental y consulta a expertos para conocer la factibilidad económica y financiera del uso en cada uno de los dispositivos de reconocimiento que pueden ser incluidos en un sistema de control de acceso para así poder determinar la inversión inicial que requeriría la implantación del sistema de control de acceso a las instalaciones de la empresa EDTEC.

Formular el plan para la implementación de un sistema de control de acceso a las instalaciones de la empresa objeto de estudio.

- Recolección de datos.

- Realizar la revisión documental como técnica de recolección de datos para validar los elementos que debe tener un plan para la implementación de un sistema de control de acceso a las instalaciones de EDTEC.

Determinar los riesgos asociados al plan diseñado para la implementación del sistema de control de acceso.

- Recopilar información en materia de riesgos asociados a la implementación de un sistema de control de acceso y los diferentes dispositivos utilizados para el reconocimiento de personas mediante revisión documental y entrevistas no estructuradas a expertos en el área.

3.7. Operacionalización de los Objetivos

De acuerdo a Hurtado (2010): “La operacionalización se realiza cuando el investigador desea hacer un abordaje focalizado en la investigación, cuando ya tiene un concepto específico del evento y su intención es construir un instrumento estructurado.” (p. 131).

A continuación se definen las variables que son desarrolladas en la investigación para dar respuesta a los objetivos anteriormente planteados:

Tabla 1: Operacionalización de los objetivos

Objetivo especifico	Variables	Técnicas	Fuentes de Información	Indicadores
Analizar los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso.	Análisis de Mercado	Revisión Documental	Documentos	Característica del producto. Precio del producto. Oferta.
Determinar la factibilidad técnica del proyecto para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC.	Factibilidad Técnica	Revisión Documental. Entrevista no estructurada. Observación Directa	Documentos. Fuentes Directas en la Empresa. Juicio de Expertos.	Maquinaria y Equipos. Capacidad Instalada y Utilizada. Elementos de Infraestructura.
Realizar el estudio de factibilidad económica financiero que permita determinar la viabilidad de implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC.	Estudio Económico y Financiero	Revisión Documental	Documentos	Inversión Inicial
		Consulta a Expertos	Documentos	
Formular el plan para implementar un sistema de control de acceso a las instalaciones de la empresa objeto de estudio.	Diseño de plan	Revisión Documental	Documentos.	Elementos del plan.
Determinar los riesgos asociados al plan diseñado para la implementación del sistema de control de acceso.	Análisis de Riesgos	Revisión Documental. Entrevista no estructurada.	Documentos. Juicio de Expertos.	Tratamiento de los riesgos.

- ✓ Análisis de mercado: Con esta variable se busca conocer los diferentes dispositivos de reconocimiento existentes en el mercado, midiendo los riesgos y posibilidades de éxito de cada uno de ellos, esto con el fin de facilitar la toma de decisión sobre el dispositivo a usar para la implementación del sistema de control de acceso para la empresa de desarrollo tecnológico EDTEC.

- ✓ Factibilidad técnica: este análisis servirá para determinar la infraestructura necesaria para la implementación del sistema de control de acceso. De este estudio también se obtendrán los costos de inversión y de operación en los procesos de producción.

- ✓ Factibilidad económica y financiera: este análisis se construirá con la información resultante del estudio técnico y la transforma en valores, es por ello que el objetivo principal de este estudio es organizar y procesar la información que se tiene para la obtención de resultados que sirvan de base para su evaluación.

- ✓ Formular el plan: Con esta variable se busca conocer los elementos que debe tener un plan para la implementación de un sistema de control de acceso.

- ✓ Determinar los riesgos: con esta variable se busca conocer los riesgos asociados al diseño del plan para implementación de un sistema de control de acceso que pudieran afectar el tiempo, costo y alcance del proyecto.

3.8. Estructura Desagregada de Trabajo

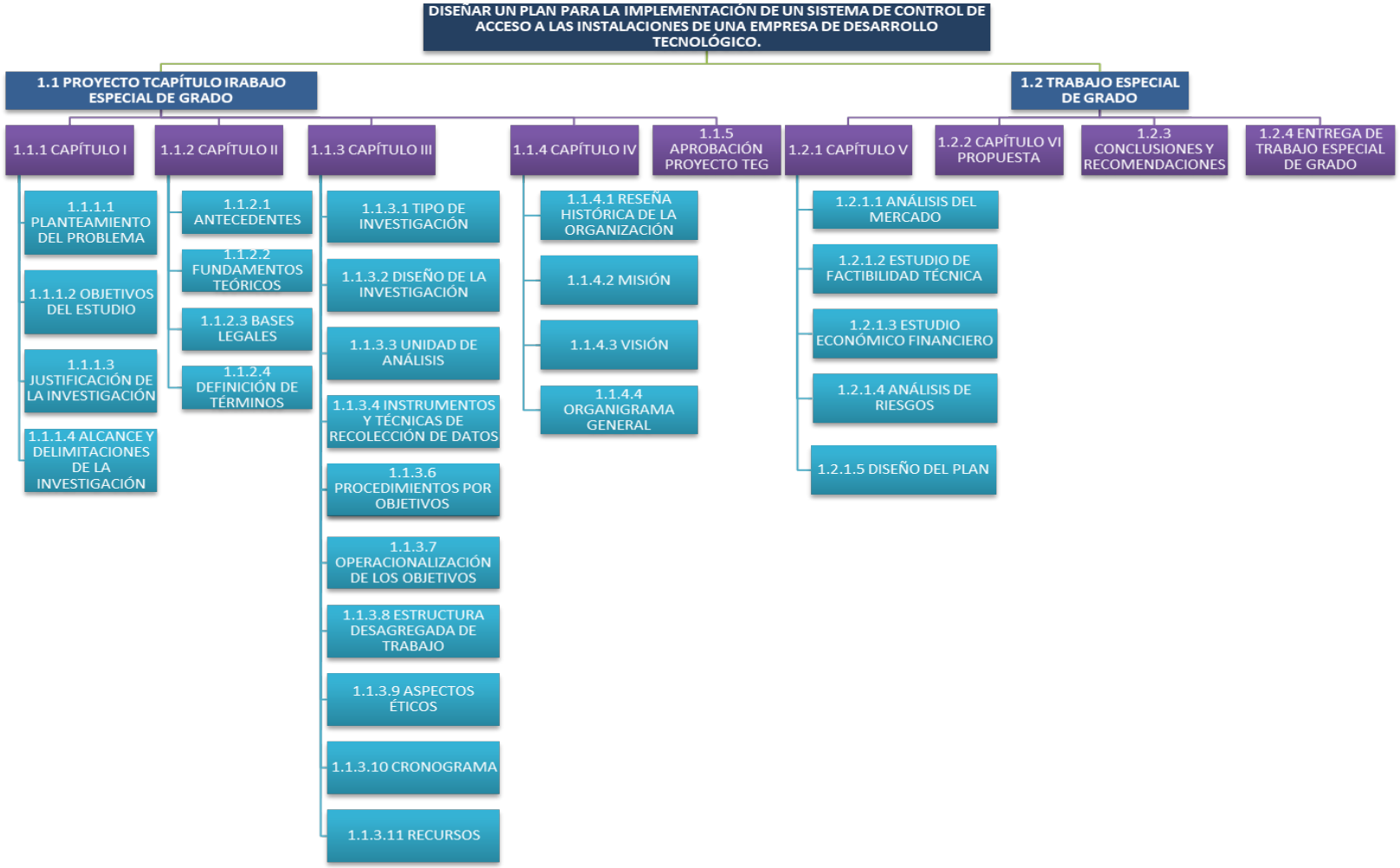


Figura 4: Estructura desagregada de trabajo

3.9. Aspectos Éticos

La investigación no debe ser sólo un acto técnico, es ante todo el ejercicio de un acto responsable y desde esta perspectiva, la ética de la investigación es planteada como un subconjunto de los valores en general.

Los aspectos éticos comprueban a los individuos que deben elegir un curso de acción, en ocasiones en una situación en la que dos o más principios de ética entran en conflicto. Valarino et al (2010) agregan que el investigador debe "ser fiel a los resultados obtenidos y decir la verdad, sin falsear los mismos a su conveniencia, además de no apropiarse de las ideas ajenas, ya sea de los escritos o de las investigaciones previas" (p. 210).

Por su parte, el código de ética y conducta profesional del PMI (2006) se estructura en base a un conjunto de cuatro valores fundamentales: respeto, equidad, responsabilidad y honestidad. Estos cuatro valores fundamentan el correcto comportamiento de los integrantes del PMI, lo cual también se hace extensible a quienes fundamentan su quehacer profesional sobre las mejores prácticas promovidas por el PMI (2013).

Por otra parte, el código de ética del Colegio de Ingenieros de Venezuela (1996) para profesionales en la ingeniería, arquitectura y carreras afinas, se fundamenta en un conjunto de valores que norman el comportamiento profesional de un agremiado, dentro de este conjunto destacan los valores siguientes: virtud, conocimiento, legalidad, seriedad, reputación, justicia, protección del medio ambiente, respeto a las leyes (CIV, 1996).

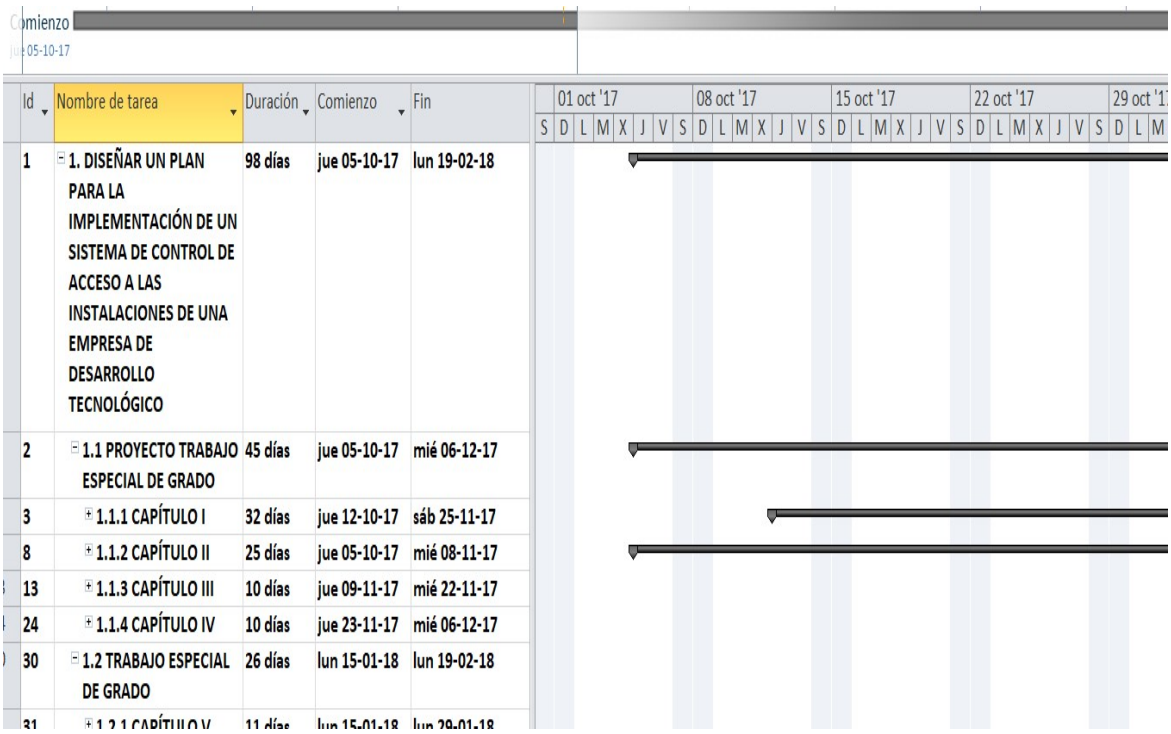
3.10. Cronograma

Desarrollar el cronograma del proyecto, consiste en definir y secuenciar actividades y estimar los recursos de las mismas; es un proceso iterativo, determina las fechas de inicio y finalización planificadas para las actividades del proyecto.

Portillo (2014) indica que el cronograma de la investigación es una herramienta gráfica que muestra las actividades realizadas en la investigación y el lapso de tiempo que cada una de ellas requirió para ser completada.

El desarrollo del cronograma exige que se revisen y se corrijan las estimaciones de duración y las estimaciones de los recursos para crear un cronograma del proyecto aprobado que pueda servir como línea base con respecto a la cual poder medir el avance.

Hurtado (2010) considera el cronograma como una parte importante del proceso de planificación, el cual debe contener las actividades así como la duración en tiempo de estas. El desarrollo del cronograma continúa a lo largo del proyecto, a medida que el trabajo avanza, el plan de gestión del proyecto cambia, y los eventos de riesgo anticipados ocurren o desaparecen al tiempo que se identifican nuevos riesgos.



Id	Nombre de tarea	Duración	Comienzo	Fin
1	1. DISEÑAR UN PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE UNA EMPRESA DE DESARROLLO TECNOLÓGICO	98 días	jue 05-10-17	lun 19-02-18
2	1.1 PROYECTO TRABAJO ESPECIAL DE GRADO	45 días	jue 05-10-17	mié 06-12-17
3	1.1.1 CAPÍTULO I	32 días	jue 12-10-17	sáb 25-11-17
8	1.1.2 CAPÍTULO II	25 días	jue 05-10-17	mié 08-11-17
13	1.1.3 CAPÍTULO III	10 días	jue 09-11-17	mié 22-11-17
24	1.1.4 CAPÍTULO IV	10 días	jue 23-11-17	mié 06-12-17
30	1.2 TRABAJO ESPECIAL DE GRADO	26 días	lun 15-01-18	lun 19-02-18
31	1.2.1 CAPÍTULO V	11 días	lun 15-01-18	lun 29-01-18

Figura 5: Cronograma de actividades

3.11. Recursos

El objetivo de este apartado es determinar la magnitud de la inversión necesaria para la realización de este estudio. El financiamiento del mismo fue realizado directamente por el investigador.

La realización de la presente investigación demandó recursos de tipo humano, materiales y tecnológicos. Los recursos humanos están representados en el profesor asesor y el investigador. Los recursos materiales necesarios para el desarrollo de la presente investigación fueron copias, papel, tóner, impresiones, traslados a la Universidad e inscripción de la cátedra Seminario de TEG y Trabajo Especial de Grado. Los recursos tecnológicos necesarios fueron internet, teléfono móvil y un computador con las aplicaciones necesarias para su utilización como Word, Excel y software de proyectos Project, entre otros.

Los costos de la Inscripción de la cátedra Seminario de TEG y Trabajo Especial de Grado fueron calculados en base a la matrícula del trimestre Septiembre - Diciembre 2017 de la Universidad Católica Andrés Bello en su sede de Montalbán. Por otra parte, se incluyen los honorarios profesionales del asesor aunque no implique que los mismos representen un gasto para el investigador por estos servicios.

A continuación se presenta el presupuesto necesario para llevar a cabo este trabajo de investigación:

Tabla 2: Presupuesto para la investigación

Presupuesto para la Investigación		
Tipo de Recurso	**Unidades**	**Costo Bs.**
Humanos		
Investigador	550 hrs	2.860.000
Asesor	60 hrs	312.000
Materiales		
Inscripción cátedra Seminario de Trabajo Especial de Grado	3 uc	174.000
Inscripción Trabajo Especial de Grado	4.8 uc	278.400
Traslados a la Universidad	5 viajes	15.000
Libros digitales	1 und	0
Copias, impresiones, tóner y papel	Varias	100.000

Presupuesto para la Investigación		
Tipo de Recurso	**Unidades**	**Costo Bs.**
Tecnológicos		
Computador	1 und	0
Internet móvil	6 meses	200.000
Teléfono móvil	6 meses	200.000
Licencia sistema operativo Windows	1 licencia	0
Licencia office de Windows	1 licencia	0
Software de proyectos Project	1 licencia	0
	Total Bs.	**4.205.000**

CAPITULO IV: MARCO ORGANIZACIONAL

El marco organizacional de una empresa se desarrolla para conocer cómo opera la misma para lograr el cumplimiento de sus metas y objetivos. El presente capítulo de la investigación dará a conocer los aspectos más relevantes de la empresa de desarrollo tecnológico EDTEC, entre los que se puede mencionar: reseña histórica, misión, visión, objetivos y estructura organizativa.

4.1. Reseña Histórica

Aun cuando la empresa de desarrollo tecnológico EDTEC ha comenzado con el desarrollo de sus actividades comerciales en el mercado de la innovación y las tecnologías de información en el año 2008, antes de su origen legal han contado con un grupo de profesionales con gran experiencia en las áreas de desarrollo tecnológico, permitiéndole brindar a su cartera de clientes, servicios de alto valor agregado.

La experiencia adquirida a lo largo de los años ha permitido avanzar fuertemente en la implementación de sistemas orientados a la gestión informática y automatización de procesos empresariales. Desde el comienzo, el desarrollo de Software ha sido dedicado a requerimientos para clientes especializados en ofrecer servicios de entrenamiento físico, a partir de allí, se han ido desarrollando en forma creciente tanto el área de desarrollo de software como la de consultoría tecnológica, ofreciendo una óptima asistencia técnica a sus clientes a una excelente relación costo-beneficio, con la convicción que el liderazgo en la calidad del servicio de atención al cliente es una competencia necesaria y determinante en un mundo altamente cambiante y competitivo.

4.2. Misión

Cubrir las necesidades globales para el desarrollo de soluciones de sus clientes y crear valor para sus accionistas y otros grupos de interés al convertirse en la compañía de desarrollo más eficiente y rentable del mundo.

Para lograr su misión, consideran fundamental contar con un equipo de profesionales altamente capacitados, y con el compromiso y la motivación necesaria para satisfacer a sus clientes, buscando ser reconocidos y aceptados tanto por sus productos y servicios como por su cultura empresarial, priorizando la mejora continua que asegure la evolución económica de largo plazo, en un clima de trabajo cordial que fomente la creatividad, el respeto y la ética comercial.

EDTEC posee la fuerte convicción que tanto el conocimiento y capacidad técnica como la calidad del servicio de atención a sus clientes son las que diferencian a las empresas líderes, colocando todo su esfuerzo en mejorarlos sostenidamente.

4.3. Visión

Consolidar el liderazgo de la empresa de desarrollo de tecnología EDTEC en el mercado nacional, expandiendo sus servicios de desarrollo de software en todos los mercados posibles, para situarse como una de las de las empresas de más rápido y mejor crecimiento a nivel mundial.

4.4. Objetivos

- Proveer soluciones de software apoyados en tecnologías innovadoras en todas las áreas demandantes de desarrollo informático inteligente aplicado a la gestión de procesos productivos, buscando permanentemente la diferenciación por la calidad del servicio y la satisfacción del cliente.
- Ser una Empresa reconocida y elegida como “innovadora” entre sus clientes por la calidad de las propuestas y el estricto cumplimiento de los compromisos asumidos.

- Desarrollar cuidadamente los recursos humanos para asegurar una cultura institucional basada en la ética, la innovación y la búsqueda permanente de la excelencia, para que estas sean las bases para un crecimiento sustentable que aseguren el futuro de la compañía.

4.5. Estructura Organizativa

En el organigrama se observan las presidencias operativas y administrativas de la empresa EDTEC donde se encuentran los servicios ofrecidos por la misma.

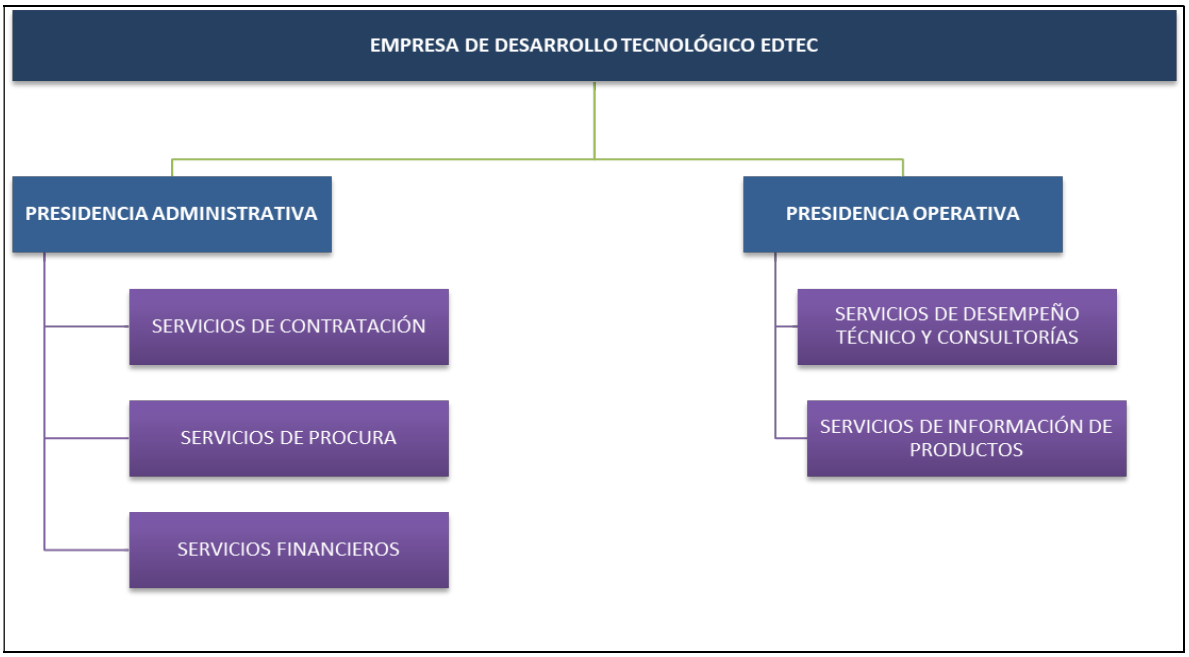


Figura 6: Estructura Organizativa de EDTEC

CAPITULO V: PRESENTACIÓN Y ANÁLISIS DE LOS DATOS

Este capítulo contiene el análisis de los resultados mediante el desarrollo de cada uno de los objetivos planteados en el proyecto.

5.1. Analizar los diferentes dispositivos de reconocimiento existentes en el mercado para implementar un sistema de control de acceso.

Todos los sistemas de control de acceso y las tecnologías que los mismos emplean, poseen al momento de su implementación, beneficios y desventajas. Comparar sistemas de control de acceso de manera descontextualizada, ya sea sobre el funcionamiento, usabilidad o cualquier otro criterio, es erróneo, ya que no refleja correctamente, que la identificación es sólo parte de un sistema mayor. Sin embargo, al tener una visión de las potencialidades o limitaciones probables de cada sistema, se puede determinar qué aplicaciones son factibles, o cuales funcionarán mejor en una situación en particular.

Entre los distintos tipos de reconocimiento implementados en los sistemas de control de acceso podemos mencionar:

- ✓ Reconocimiento de huella dactilar: Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca, ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, sin necesidad de una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos.

Figura 7: Sistema biométrico - control de acceso y asistencia por huellas dactilares
Fuente: Tecniplanet (2016)

- ✓ Reconocimiento de voz: Esta modalidad biométrica presenta algunos desafíos únicos que no se encuentran en otras formas de reconocimiento humano y es que tienen que lidiar con los distintos acentos dentro de un idioma y las diferentes formas de hablar de cada persona, ya que la voz varía dependiendo de la situación, puede verse influenciado por una congestión nasal, por ejemplo. Es susceptible al engaño si se producen grabaciones. Su fiabilidad se encuentra por debajo de otros sistemas biométricos.

Figura 8: Sistema digital de reconocimiento vocal
Fuente: Grundig Business System

- ✓ Reconocimiento facial o de rostro: Los rasgos de la cara pueden verse afectados con el paso del tiempo, así como un cambio en el crecimiento de

los bellos faciales puede influir a la hora de realizar la identificación. Sin embargo en algunos casos al contar con patrones faciales puede llevarse a cabo la autenticación de una identidad.

Figura 9: Control de acceso y presencia por reconocimiento facial
Fuente: Izux Ingeniería y Seguridad (2014)

- ✓ Reconocimiento mediante el escaneo del iris: Es uno de los sistemas de identificación más usados ya que los patrones oculares cuentan con una probabilidad de coincidencia muy cercana a cero y a la hora de la muerte estos se degeneran rápidamente evitando así un fraude del patrón. A pesar de esto, posee desventajas ya que al realizar la lectura con un láser es incómodo para el usuario y además si la persona usa lentes se verá afectado su patrón de reconocimiento por lo que no podrá realizarse la identificación.

Figura 10: Reconocimiento biométrico por iris
Fuente: Biométricos.net (2014)

- ✓ Reconocimiento por radiofrecuencia mediante tarjetas de identificación: Las tarjetas de identificación por radiofrecuencia combinan rapidez y comodidad en su uso dado que el usuario solo debe acercar la tarjeta al lector, o incluso, sin sacarla de bolsillo o cartera puede acceder al área requerida, siempre y cuando esté autorizado para ello. A su vez, este mecanismo de identificación es menos costoso que otros mecanismos que utilizan biometría para la identificación y control de acceso a personas. Por otra parte, las tarjetas de identificación no son del todo fiable, dado que las mismas pueden ser robadas o falsificadas permitiendo suplantar la identidad de la persona.

Figura 11: Lector biométrico y de proximidad para control de accesos

Fuente: Accesor (2018)

- ✓ Reconocimiento palmar: Es el sistema de reconocimiento más rápido aunque cuenta con un índice de error demasiado alto, ya que se basa en medidas de longitud, ancho y área. Puede existir la posibilidad de que dos personas tengan una geometría demasiado parecida y que se genere una identificación errónea.

Figura 12: Lector de palma de la mano

Fuente: Electronic development sales (Edsales) (2018)

El funcionamiento de los distintos tipos de reconocimiento implementados en los sistemas de control de acceso, se ve influenciado por diversos factores que pueden afectar su rendimiento. En cuanto a los factores que afectan directa o indirectamente sobre estos sistemas, se pueden establecer dos grandes grupos:

a) Aquellos inherentes al propio dispositivo o tecnología empleada, denominados también ambientales: Se incluyen en este grupo la luz, ruidos, temperatura, ruido electromagnético, humedad, suciedad y contaminantes, variaciones de voltaje, golpes y vibraciones.

Tabla 3: Factores que afectan sobre los sistemas biométricos y no biométricos

Sistema de Reconocimiento / **Factor Ambiental**	Huella Dactilar	Palmar	Iris	Facial	Voz	Radiofrecuencia (Tarjeta)
Luz	x	x	x	x		x
Ruido					x	
Temperatura	x	x				x
Humedad	x	x				x
Suciedad y Contaminantes	x	x	x	x		x
Variaciones de Voltaje	x	x	x	x	x	x

Sistema de Reconocimiento / Factor Ambiental	Huella Dactilar	Palmar	Iris	Facial	Voz	Radiofrecuencia (Tarjeta)
Golpes y Vibraciones	x	x	x	x	x	x

b) Aquellos correspondientes a los factores ajenos a los dispositivos, que de una u otra manera afectan a todos los sistemas, denominados requisitos, características o criterios de evaluación: En este grupo se destacan las siguientes características: universalidad, fiabilidad, facilidad de uso, prevención de ataques, aceptabilidad, permanencia, costo, unicidad, capacidad de almacenamiento y tamaño del lector.

Tabla 4: Criterios de evaluación de los sistemas biométricos y no biométricos

Sistema de Reconocimiento / Características	Huella Dactilar	Palmar	Iris	Facial	Voz	Radiofrecuencia (Tarjeta)
Unicidad	Alta	Alta	Alta	Media	Baja	Baja
Fiabilidad	Alta	Alta	Alta	Media	Baja	Baja
Facilidad de uso	Alto	Alto	Bajo	Alto	Bajo	Alto
Resistencia a Ataques	Alta	Alta	Alta	Media	Baja	Baja
Aceptabilidad	Alta	Alta	Baja	Media	Media	Alta
Costo	Medio	Alto	Alto	Medio	Bajo	Bajo
Tamaño del Lector	Pequeño	Grande	Mediano	Grande	Pequeño	Mediano

De acuerdo a lo anterior, se puede inferir que, de los diferentes dispositivos biométricos y no biométricos para identificación y reconocimiento existentes en el mercado, usados para implementar un sistema de control de acceso, el de huella dactilar es el que cumple con la mayoría de los criterios de evaluación, entre los que se encuentra:

- Unicidad: porque no existen dos individuos que posean la misma característica.
- Fiabilidad: haciendo referencia a la precisión del reconocimiento.
- Facilidad de uso: con respecto al tiempo en el que los usuarios realizan una interacción efectiva con el sistema o producto.
- Resistencia a ataques: se refiere a la preparación y disposición ante posibles intentos de violación al sistema.
- Aceptabilidad: grado de aceptación de las personas ante el sistema o producto.
- Costo aceptable: incluyen hardware y software asociado para capturar la biometría.
- Tamaño del lector: el tamaño del lector biométrico facilita o dificulta su instalación, siendo de fácil instalación los dispositivos más pequeños.

Aunado a lo anterior, el reconocimiento por huella dactilar posee la característica de la permanencia en el mercado, siendo la técnica biométrica más antigua y sin embargo, la más usada en el mundo por su alto grado de madurez tecnológica, permitiendo encontrar una alta gama de precios y funcionalidades competitivas en el mercado. Esta técnica ha sido implementada en un gran número de aplicaciones debido a que se considera que las huellas dactilares son únicas e inalterables, incluso si temporalmente cambian debido a cortes o variaciones en la piel.

De acuerdo a un estudio realizado por el Grupo Internacional Biométrico en el año 2002 los sistemas biométricos basados en el reconocimiento por las huellas dactilares alcanzaron la cifra de 52.1%, dejando en segundo lugar con 12.4% a los sistemas biométricos basados en el reconocimiento del rostro.

En el siguiente gráfico, se puede observar en los resultados del mismo estudio realizado por el Grupo Internacional Biométrico en el año 2009, un incremento porcentual del 15% en sistemas biométricos basados en el reconocimiento por huella dactilar, alcanzando la cifra de 67%.

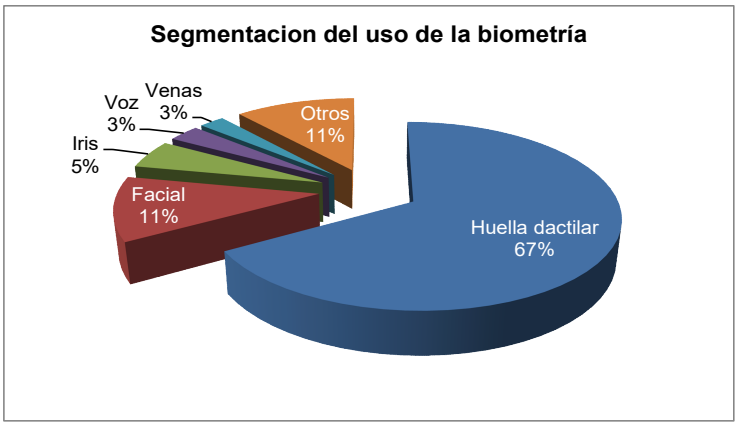


Figura 7: Segmentación del uso de la biometría

Fuente: La Investigadora con datos de Grupo Internacional Biométrico (2009)

Por otra parte, según datos del Grupo Internacional Biométrico, el mercado de la biometría se ha centrado casi exclusivamente en tres tipos de aplicaciones. Por un lado, el control de acceso físico dominó el mercado biométrico con un 42% a principios del año 2000, seguido de la incorporación en aplicaciones de tecnología de información (TI), como portátiles o como interfaces de acceso específicos (25%), y por último, el tercer mayor sector era el de los servicios financieros (15%), el más dado a evolucionar rápidamente debido a la nueva gestión de la identidad digital, los nuevos tipos de fraudes o los cambios en el concepto de banca en sí.

5.2. Determinar la factibilidad técnica del proyecto para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC.

La factibilidad técnica se refiere a los recursos necesarios para efectuar las actividades o procesos que requiere el proyecto. Generalmente nos referimos a elementos tangibles o medibles. El proyecto debe considerar si los recursos técnicos actuales son suficientes o deben complementarse.

De acuerdo a lo expresado por Vivallo (n.d.), la factibilidad técnica es definida por el estudio de varias opciones técnicas que pueden existir para el proyecto pero, además, determina lo que será la inversión, costos, ingresos y egresos que sustentan la rentabilidad. Por su parte, Blanco (2005) expresa que, el estudio técnico persigue determinar las capacidades instaladas y utilizadas de la empresa, así como la de todos los costos de inversión y de operación involucrados en el proceso de producción.

Al momento de implementar el sistema de control de acceso, se debe determinar cuáles son los requerimientos básicos pueda funcionar de manera correcta. Es por ello, que el siguiente estudio técnico tiene como objetivos fundamentales verificar la posibilidad técnica de implementación de un sistema de control de acceso para una empresa de desarrollo tecnológico, así como analizar y determinar aspectos esenciales como requerimientos de equipos, aplicaciones, selección de tecnologías y proveedores.

En la siguiente tabla podemos observar los elementos comunes necesarios para implementar un sistema de control de acceso físico con los componentes biométricos y no biométricos identificados en el objetivo anterior.

Tabla 5: Elementos comunes necesarios para implementar un sistema de control de acceso

#	Elemento	Tipo	Cantidad	Unidad	Descripción
1	Controladora de acceso	Hardware	18	UND	Panel de 1 entrada, 1 salida. Capacidad para controlar 1 puerta. Función antipassback global y local. Almacenamiento local de hasta 1000 eventos en modo sin comunicación con el servidor. Comunicación RS-232/RS-485/Ethernet.

#	Elemento	Tipo	Cantidad	Unidad	Descripción
2	Cerradura electromagnética	Hardware	18	UND	Capacidad máxima de 500 libras. Consumo 12 VDC / 500 mA. / 24 VDC / 250 mA.
3	Fuente de poder	Hardware	18	UND	Fuente de poder 12V 5 A. Con capacidad de carga de batería.
4	Cableado	Hardware	200	MTS	Cables UTP: Categoría 5 utilizable como extensión para la interconexión de las lectoras con las controladoras. Cable 18 AWG: Cable eléctrico medida 18 awg para conexión de fuente de poder/batería/cerradura
5	Servidor	Hardware	1	UND	Procesador Intel Xeon E5-2620 2.00GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C 95W. 8GB RDIMM, 1600MT/s, Low Volt, Dual Rank, x4 Data Width. Disco Duro Hot Plug 500GB 7.2K RPM Near-Line SAS 6Gbps 2.5 pulgadas.
6	Licencia	Software	1	UND	Licencia para Software de Control de Acceso que permita controlar hasta 18 controladoras. Configuración remota de las controladoras. Manejo de base de datos histórica. Aplicación de Niveles de Acceso.

Por otra parte, en la siguiente tabla podemos observar los elementos necesarios para implementar un sistema de control de acceso por tipo de reconocimiento biométrico y no biométrico.

Tabla 6: Elementos necesarios para implementar un sistema de control de acceso por tipo de reconocimiento

#	Sistema de Reconocimiento	Tipo	Cantidad	Unidad	Descripción
1	Huella dactilar	Hardware	36	UND	Lector de huella dactilar: ✓ Método de escaneado: óptico ✓ Ventana de escaneo de huellas digitales: 25,5 * 18 mm. ✓ Resolución: 508 dpi. ✓ Velocidad de escaneado: 1/15 sec. ✓ Tasa de falsa aceptación (FAR - la probabilidad de tolerancia "extranjera"): 10-9 (1 en 1 mil millones)
2	Radiofrecuencia (no biométrico)	Hardware	36	UND	a. Lector de tarjetas de proximidad: ✓ Alimentación: 9 - 12 vdc. ✓ Rango de lectura: 5 - 10 cm. ✓ Soporte para tarjetas rfid 125khz. ✓ Beep para confirmación de lectura. ✓ Antena interna. ✓ Distancia de transmisión 100Mts.
			50	UND	b. Tarjetas de proximidad aptas para funcionar con cualquier sistema que trabaje en 125 KHZ como los ANVIZ, ZKSOFTWARE, SOVICA entre otras.
3	Iris	Hardware	36	UND	Lectora de iris: ✓ Cámara de captura de datos cero contacto de 31 a 35cm de distancia aproximadamente. ✓ Pantalla táctil de 4.3”. ✓ Resolución Iris 210 píxeles. ✓ Doble iris captura y autenticación.

#	Sistema de Reconocimiento	Tipo	Cantidad	Unidad	Descripción
4	Facial	Hardware	36	UND	Lectora facial: ✓ Cámara de alta resolución. ✓ Microprocesador de 16MHz 8 bits. ✓ Energía: 110/220VAC ~ 12VDC. ✓ Velocidad interna de lectura: ≤0 .5s ✓ Velocidad de reconocimiento interna: ≤1s ✓ Capacidad de almacenamiento hasta 1200 rostros y 100,000 transacciones.
5	Palma de la mano	Hardware	36	UND	Lector de palma de mano: ✓ Velocidad de acceso de aproximadamente de 15 usuarios/minuto. ✓ Tiempo del proceso de inscripción no más de 60 segundos.
6	Voz	Hardware	36	UND	Micrófono para el reconocimiento de voz: ✓ Voltaje: 4.5-5.5V

Aunado a los elementos tecnológicos indicados en las tablas anteriores, se requiere de un personal calificado para ejercer cada uno de los siguientes roles al momento de ejecutar la implementación del sistema de control de acceso a las instalaciones de la empresa de desarrollo tecnológico EDTEC:

Tabla 7: Personal requerido para la implementación de un sistema de control de acceso

Cargo	Perfil	Rol
Gerente de proyecto	Educación: Profesional con carrera: Ingeniero Industrial, Ingeniero Civil, Ingeniero de Sistemas o Informática, Ingeniero Mecánico Eléctrico. Experiencia: al menos 3 años en administración y control de proyectos. Conocimientos de: -Administración y Control de Proyectos - Metodología Project Management - Manejo de software de administración y control de proyectos - Windows y Ofimática; Microsoft Project - Planeación Estratégica - Sistemas de Gestión de Calidad ISO 9000	Planear, dirigir y controlar las operaciones de la Gerencia a su cargo, determinando, conjuntamente con el equipo de trabajo, las líneas de acción para la prospección del proyecto de acuerdo al alcance; coordinando a la vez la estrategia operativa del proyecto y evaluando la rentabilidad del mismos a través del seguimiento oportuno y preciso de los costos de operación y el avance en los resultados obtenidos.
Administrador	Educación: Licenciado en Administración. Experiencia: Cinco (5) años de experiencia progresiva de carácter operativo, supervisor y estratégico en el área de Administración. Redactar y analizar informes técnicos. Realizar cálculos numéricos. Analizar problemas presupuestarios.	Controlar las actividades administrativas, de presupuesto, contabilidad, mantenimiento y proveeduría de los servicios y los recursos materiales y financieros asignados al proyecto, planificando, coordinando y ejecutando los sistemas y procedimientos contables y financieros, a fin de satisfacer las necesidades del proyecto y administrar efectivamente sus recursos.
Jefe de compras	Educación: Licenciatura en Administración Pública, Administración de Empresa y Contabilidad o Economía. Experiencia: Dos (2) años de experiencia en procura y adquisiciones en empresas. Habilidades: -Realizar cálculos numéricos. -Redactar y analizar órdenes de compra. -Expresarse en forma oral y escrita fluidamente. -Capacidad de organización. -Para supervisar. -Para dar instrucciones.	Supervisar las compras a fin de garantizar la procura oportuna, eficiente y correcta del material para operaciones, sobre una base de calidad requerida y precio competitivo. - Revisar los sustentos de compra y aprobar las órdenes de compra - Coordinar importación de equipos y materiales (facilitar documentos e información de órdenes de compra, indicar modo de envío) - Evaluar proveedores
Consultor técnico	Educación: especialista sistemas de información. Experiencia: 5 años. Ofrece una opinión experta, pericia o conocimientos relativos a los requisitos técnicos y de usuario que han de tenerse en cuenta en la implementación de un sistema de control de acceso.	Es responsable del levantamiento de requerimientos técnicos necesarios para la instalación y puesta en marcha del hardware y software en la implementación del sistema de control de acceso.

Cargo	Perfil	Rol
Instaladores	Educación: Profesional en Ingeniería Electrónica, Eléctrica o en una carrera del área de Computación e Informática. Experiencia: 1 año en instalación de sistemas de información, de cableado estructurado y servidores. Conocimientos de: Electrónica digital. Arquitectura de equipos electrónicos y redes. Normas sobre cableado estructurado y fibra óptica. Manejo de programas de computación afines al cargo.	Es responsable de la instalación y puesta en marcha del hardware y software en la implementación del sistema de control de acceso

Las tecnologías biométricas surgieron como alternativa o complemento a otras técnicas de identificación y autenticación no biométricas, como lo son el uso de contraseñas o tarjetas de identificación por radiofrecuencia. Por ello es posible establecer una comparación directa entre ambas, destacando beneficios que resultan del uso de cada una de ellas. De acuerdo al Instituto Nacional de Ciberseguridad de España (2016) se han de considerar los siguientes aspectos:

a. “Necesidad de secreto: las tarjetas no deben de estar al alcance de terceros y las contraseñas deben ocultarse y mientras que la biometría no requiere de estas medidas de protección.

b. Posibilidad de robo: las contraseñas han de ocultarse y las tarjetas pueden ser robadas. Sin embargo, robar un rasgo biométrico es extremadamente complejo.

c. Posibilidad de pérdida: las contraseñas son fácilmente olvidables y las tarjetas se pueden perder. Los rasgos biométricos permanecen invariables.

d. Registro inicial y posibilidad de regeneración: la facilidad con la que se puede cambiar una contraseña contrasta con la complejidad que supone el registro en un sistema biométrico. Hay que añadir que los rasgos biométricos son por definición limitados, mientras que la generación de contraseñas es ilimitada, lo cual es una ventaja.

e. Proceso de comparación: la comparación de dos contraseñas es un proceso sencillo. Sin embargo, comparar dos rasgos biométricos requiere de mayor capacidad computacional.

f. Comodidad del usuario: el usuario ha de memorizar una o múltiples contraseñas y, en el caso de que use una tarjeta, ha de llevarse siempre consigo. Utilizando tecnología biométrica no se necesita realizar estos esfuerzos.

g. Vulnerabilidad ante el espionaje: una discreta vigilancia de nuestra actividad podría servir para obtener nuestra contraseña o robar nuestra tarjeta. Ese método no es válido ante los sistemas biométricos.

h. Vulnerabilidad a un ataque por fuerza bruta: las contraseñas tienen una longitud de varios caracteres. Por su parte, una muestra biométrica emplea cientos de bytes, lo que complica mucho los ataques por fuerza bruta.

i. Medidas de prevención: los ataques contra sistemas protegidos por contraseña o tarjeta se producen desde hace años, y las medidas de prevención contra ellos ya se encuentran maduras. Por el contrario, los ataques a los sistemas biométricos es un área reciente.

j. Autenticación de usuarios «reales»: la autenticación de usuarios mediante contraseña o tarjeta y su efectividad, dependen absolutamente de la voluntad del usuario a la hora de hacerlas personales e intransferibles. La biometría está altamente relacionada con el propio usuario pues no puede ser prestada ni compartida.

k. Coste de implantación: en el momento de la implantación, el hecho de instalar un sistema de contraseñas tiene un coste bajo, mientras que en el caso de un sistema basado en muestras biométricas es más costoso.

l. Coste de mantenimiento: el coste de mantenimiento de un sistema biométrico, una vez está implantado con éxito, es menor al de un sistema de contraseña o tarjeta ya que no conlleva gastos de gestión asociados a la pérdida u olvido de credenciales.” (p. 22-23).

Tabla 8: Comparación entre el uso de elementos biométricos y no biométricos

Aspecto	Biometría	Contraseña/ Tarjetas De Identificación
Necesidad de secreto	x	
Posibilidad de robo (baja)	x	
Posibilidad de pérdida (baja)	x	
Registro inicial y posibilidad de regeneración		x
Proceso de comparación (fácil)		x
Comodidad del usuario	x	
Vulnerabilidad ante el espionaje (baja)	x	
Vulnerabilidad a un ataque por fuerza bruta (baja)	x	
Medidas de prevención		x
Autenticación de usuarios reales	x	
Coste de implantación (bajo)		x
Coste de mantenimiento (bajo)	x	

Fuente: La Investigadora con datos del Instituto Nacional de Ciberseguridad (2016)

En la tabla anterior se puede observar la comparación entre el uso de componentes biométricos y no biométricos, siendo notorio que el uso de componentes no biométricos como contraseñas o tarjetas de identificación en un sistema de control de acceso, posee desventajas en aspectos de seguridad, entre los que podemos mencionar: la posibilidad de robo o pérdida, vulnerabilidad ante el espionaje o ante un ataque por fuerza bruta, etc. Al poseer estas debilidades sobre los sistemas que incorporan elementos biométricos en el control de acceso, un individuo, mediante el robo de credenciales o tarjetas identificativas, puede acceder a zonas restringidas o realizar operaciones no permitidas, inculpando a terceros.

A través de la implementación de sistemas biométricos, se aumenta la seguridad reduciendo la probabilidad de que alguien no autorizado acceda a zonas o a aplicaciones restringidas, ya que los rasgos biométricos se encuentran exclusivamente ligados a su legítimo usuario.

Si bien los sistemas biométricos poseen ventajas sobre los no biométricos a la hora de implementar un sistema de control de acceso, tienen algunas vulnerabilidades que afectan negativamente su operación o rendimiento. De acuerdo al Instituto Nacional de Ciberseguridad de España (2016), estas vulnerabilidades se dividen según sean comunes a todas las técnicas biométricas o específicas de alguna de ellas y se encuentran en la tabla a continuación.

Tabla 9: Vulnerabilidades que afectan a los sistemas de reconocimiento biométrico

Tecnología Biométrica	Vulnerabilidades
Vulnerabilidades comunes a todas las tecnologías biométricas.	✓ Calidad baja de los dispositivos de captura ✓ Ubicación inadecuada del dispositivo de captura ✓ Desconocimiento de la calidad o del abanico de productos y utilidades disponibles. ✓ Percepción de ausencia de privacidad por parte de los usuarios.
Huella dactilar	✓ Condición del dedo en el momento de tomar la muestra: mojado, seco, manchado. ✓ Condiciones climatológicas que afectan al lector: humedad, temperatura, luz, suciedad y contaminantes. ✓ Otros factores que afectan al lector como: variaciones de voltaje, golpes y vibraciones. ✓ Condiciones de la huella: cortes, heridas o inflamaciones. ✓ Actividad laboral: trabajos que puedan afectar a la huella, por ejemplo el uso habitual de productos químicos que puedan deteriorarla.
Reconocimiento de voz	✓ Enfermedades de la voz: bronquitis, faringitis, gripe, laringitis, afonías, etc. ✓ Variación entre el dispositivo de registro y el usado en la captura de muestras. ✓ Variación entre entornos de registro y captura de muestras (por ejemplo: interior y exterior) ✓ Volumen del habla.

Tecnología Biométrica	Vulnerabilidades
	✓ Factores que afectan al sistema de reconocimiento como: ruido, variaciones de voltaje, golpes y vibraciones.
Reconocimiento facial	✓ Variación en el peso y aspecto facial: peinado, vello, gafas, sombrero, etc. ✓ Condiciones climatológicas que afectan al lector: luz, suciedad y contaminantes. ✓ Otros factores que afectan al lector como: variaciones de voltaje, golpes y vibraciones. Uso de pañuelos, bufandas, etc, que puede dificultar la localización o visión de la cara.
Escáner de iris	✓ Excesivo movimiento ocular o de la cabeza ✓ Enfermedades oculares. ✓ Uso de gafas. ✓ Problemas debidos al uso de lentes de contacto (iris). ✓ Condiciones climatológicas que afectan al lector: luz, suciedad y contaminantes. ✓ Otros factores que afectan al lector como: variaciones de voltaje, golpes y vibraciones.
Palma de la mano	✓ Uso de joyería, bisutería o abalorios, vendajes o guantes ✓ Condiciones de la mano: inflamaciones en las articulaciones, heridas, etc. ✓ Condiciones climatológicas que afectan al lector: humedad, temperatura, luz, suciedad y contaminantes. ✓ Otros factores que afectan al lector como: variaciones de voltaje, golpes y vibraciones.

En la tabla anterior, se observan las vulnerabilidades comunes e individuales de cada uno de los elementos de reconocimiento biométricos. Sin embargo, estas vulnerabilidades pueden mitigarse haciendo uso de las siguientes recomendaciones:

a. Realizar una buena captura y almacenamiento de muestra para su posterior reconocimiento. Esta captura y almacenamiento de la muestra debe realizarse en el mismo entorno donde posteriormente se colocará el dispositivo para el reconocimiento y control de acceso; esto debido a las condiciones que puedan variar en entornos internos y externos como luz, ruido, etc.
b. La temperatura idónea para la instalación de dispositivos de reconocimiento biométrico es de -20 ~ 50°C (-4°F ~ 122°F)
c. La humedad relativa para el óptimo funcionamiento de los dispositivos biométricos debe ser menor a 90% RH.
d. Para minimizar las vulnerabilidades de ruido, luz, suciedad y contaminantes los dispositivos de reconocimiento no deben ser instalados en lugares expuestos a la intemperie o directamente a los elementos naturales como el sol, lluvia, nieve o polvo excesivo. Si se instala en el exterior es importante que esté protegido dentro de un gabinete.
e. Incluir un protector para evitar las variaciones de voltaje que puedan afectar los dispositivos de reconocimiento biométrico.
f. Realizar una buena implementación del dispositivo biométrico: no todas las empresas son iguales, por ello la adaptación a las circunstancias de cada caso es esencial para evitar futuros problemas. De acuerdo a lo expresado por el Instituto Nacional de Ciberseguridad de España (2016):

> “Si una empresa va a incorporar un control de acceso en base a la huella dactilar y cuenta con empleados que realizan trabajos manuales o utilizan productos abrasivos, puede ser aconsejable registrar las huellas de la mano que menos utilicen (izquierda en el caso de los diestros y derecha en el caso de los zurdos) y de los dedos que menos se utilicen (generalmente anular y meñique). Con esta simple adaptación, se podrán evitar en buena medida futuros problemas relacionados con cortes o deterioros en la huella.” (p. 29)

g. Adquirir tecnología de calidad: La obtención de muestras adecuadas y la realización de comparativas fiables es importante para evitar falsos

positivos, falsos negativos y altas tasas de error, y esto depende en gran medida de la calidad y fiabilidad de los sistemas utilizados. Una elección adecuada de dispositivos biométricos evita que se materialicen las vulnerabilidades antes mencionadas.

h. Formación de los usuarios: Un factor clave en el éxito de las tecnologías biométricas es que sus usuarios las utilicen correctamente. Para la consecución de este objetivo se puede informar a los usuarios sobre las tecnologías biométricas y recomendaciones para su uso.
i. Una vez implementado el sistema de control de acceso con componentes biométricos, para garantizar la durabilidad del mismo, realizar mantenimiento periódico del mismo. En el caso del lector de huella, palmar, iris y facial, después de un uso repetido por parte de los usuarios pueden aparecer sedimentos grasosos acumulados en el sensor, para esto es recomendable usar un paño de algodón humedecido con alcohol isopropílico.

A pesar de poseer las vulnerabilidades antes mencionadas, la inclusión de componentes biométricos en los sistemas de control de acceso tienen mayores beneficios que los sistemas con contraseñas o tarjetas de identificación por radiofrecuencia. Alguno de los beneficios son los siguientes:

a. Incremento en los niveles de seguridad para el control de acceso tradicional por tarjeta de aproximación o contraseña.
b. Reducción de costos de mantenimiento del sistema de control de acceso.
c. Aumento de la eficiencia del sistema de control de acceso.
d. Posibilidad de incluir un control de horario en el sistema de control de acceso.
e. Mejora de la imagen corporativa de la institución.

Por consiguiente, de acuerdo al análisis técnico realizado comparando el uso de elementos biométricos y no biométricos y de acuerdo al incremento en el uso de estas tecnologías en el mercado actual, siendo el componente biométrico de huella dactilar, el más usado en el mundo, técnicamente los dispositivos

biométricos tienen más ventajas que los dispositivos por contraseña o lector de tarjeta de proximidad.

5.3. Realizar el estudio de factibilidad económica financiero que permita determinar la viabilidad de implementar un sistema de control de acceso a las instalaciones de la empresa EDTEC.

El objetivo del estudio financiero es determinar el monto de los recursos económicos necesarios para la realización del proyecto, el costo total de la implementación de la solución a un problema que no son más que un reflejo de las determinaciones realizadas en el estudio técnico y si la inversión propuesta es económicamente rentable (Baca, 2010, p.160).

A continuación se indican los costos para implementar un sistema de control de acceso biométrico o por tarjeta de proximidad. Los montos están expresados en bs calculados a una tasa de 69000 bs por dólar americano de acuerdo al Convenio Cambiario N° 38 (c) publicado por el Banco Central de Venezuela para el segundo trimestre del año 2018.

Tabla 10: Costos de implementación de un sistema de control de acceso por tarjetas de proximidad

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Lector de proximidad	36 un.	39.524.000,00	1.422.864.000,00
Tarjetas de proximidad	50 un.	450.000,00	22.500.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Total Hardware			**10.452.430.000,00**
Licencia	1 un.	2.000.000,00	2.000.000,00
Total Software			**2.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	20.700.000,00
Costo de instalación	18 un.	20.700.000,00	621.000.000,00
Total			**10.840.830.000,00**

Tabla 11: Costos de implementación de un sistema de control de acceso por reconocimiento de voz

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Micrófono para el reconocimiento de voz	36 un.	55.200.000,00	1.987.200.000,00
Total Hardware			**10.994.266.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	6.900.000,00	9.660.000,00
Costo de instalación	18 un.	13.800.000,00	248.400.000,00
Total			**11.252.566.000,00**

Tabla 12: Costos de implementación de un sistema de control de acceso por reconocimiento de huella dactilar

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de huella dactilar	36 un.	105.000.000,00	3.780.000.000,00
Total Hardware			**12.787.066.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	10.350.000,00	13.800.000,00
Costo de instalación	18 un.	27.600.000,00	621.000.000,00
Total			**13.297.216.000,00**

Tabla 13: Costos de implementación de un sistema de control de acceso por reconocimiento facial

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector facial	36 un.	117.300.000,00	4.222.800.000,00
Total Hardware			**13.229.866.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	13.800.000,00
Costo de instalación	18 un.	34.500.000,00	683.100.000,00
Total			**13.867.666.000,00**

Tabla 14: Costos de implementación de un sistema de control de acceso por reconocimiento de iris

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de iris	36 un.	124.200.000,00	4.471.200.000,00
Total Hardware			**13.478.266.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	20.700.000,00
Costo de instalación	18 un.	37.950.000,00	869.400.000,00
Total			**14.178.166.000,00**

Tabla 15: Costos de implementación de un sistema de control de acceso por reconocimiento de palma de la mano

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de palma de la mano	36 un.	975.000.000,00	35.100.000.000,00
Total Hardware			**44.107.066.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	10.350.000,00
Costo de instalación	18 un.	41.400.000,00	745.200.000,00
Total			**44.869.066.000,00**

El desarrollo del estudio económico financiero están orientados a la selección de una solución que satisfaga las necesidades planteadas por la empresa de desarrollo tecnológico EDTEC, considerando variables adicionales a las evaluadas en el estudio técnico como, tiempo de procura, costos de hardware, costos de software, costos de instalación, costos de mantenimiento y el uso de la tecnología a nivel mundial para la selección de la alternativa, incluyendo, en los costos de instalación al personal requerido para la misma (instaladores).

Alternativa 1 - Implementación de un sistema de control de acceso haciendo uso de tarjetas de proximidad:

Los sistemas de control de acceso por tarjeta de proximidad son de los más utilizados en el mundo después de los dispositivos biométricos, esto por su fácil instalación, rapidez y comodidad en su uso dado que el usuario solo debe acercar la tarjeta al lector, o incluso, sin sacarla de bolsillo o cartera puede acceder al área requerida, siempre y cuando esté autorizado para ello. Al ser un sistema de control de acceso de gran demanda comercial, requiere mayor especificación en las

características técnicas para su adquisición y por tanto un tiempo de procura mayor. Los costos asociados al hardware, software, instalación y mantenimiento son bajos en comparación con cualquier otro sistema de control de acceso.

Alternativa 2 - Implementación de un sistema de control de acceso por reconocimiento de voz:

Al posicionarse, junto con el reconocimiento de palma de la mano de último lugar dentro del uso de la biometría en el mundo y no tener elementos de hardware y software competitivos en el mercado, dificulta encontrar una alta gama de precios y funcionalidades por lo que requiere un tiempo mayor de procura. Los costos asociados al hardware, software, instalación y mantenimiento son bajos en comparación con otros sistemas biométricos.

Alternativa 3 - Implementación de un sistema de control de acceso por reconocimiento de huella dactilar:

La técnica biométrica por reconocimiento de huella dactilar es la más antigua y sin embargo, la más usada en el mundo, permitiendo conocer los proveedores, precios y funcionalidades competitivas en el mercado invirtiendo poco tiempo en la fase de procura. Los costos asociados al hardware, software, instalación y mantenimiento son de medio nivel en comparación con otros sistemas de control de acceso por biometría.

Alternativa 4 - Implementación de un sistema de control de acceso por reconocimiento facial:

La técnica biométrica por reconocimiento facial mundialmente se encuentra posicionada en el segundo lugar seguida de la técnica de reconocimiento de huella dactilar. Al ser un sistema de control de acceso de gran demanda comercial, requiere mayor especificación en las características técnicas para su adquisición y por tanto un tiempo de procura mayor. Los costos asociados al hardware, software, instalación y mantenimiento son de medio nivel en comparación con otros sistemas de control de acceso por biometría.

Alternativa 5 - Implementación de un sistema de control de acceso por reconocimiento de iris:

Aunque es el tercer sistema de identificación biométrica más usado a nivel mundial, no se encuentra gran variedad en el mercado en cuanto a funcionalidades, por lo que el tiempo para la procura es menor. Los costos asociados al hardware, software, instalación y mantenimiento son altos en comparación con otros sistemas de control de acceso por biometría.

Alternativa 6 - Implementación de un sistema de control de acceso por reconocimiento de palma de la mano:

Es el sistema de reconocimiento biométrico menos usado a nivel mundial, posicionándose en el último lugar junto con el sistema de reconocimiento de voz a pesar de ser el sistema biométrico más rápido. Por no ser usados con tanta frecuencia, no se encuentra gran variedad en el mercado en cuanto a funcionalidades, por lo que el tiempo para la procura es menor.

Los costos asociados al hardware, software, instalación y mantenimiento son los más altos en comparación con cualquier otro sistema de control de acceso.

Las alternativas para la implementación de un sistema de control de acceso son evaluadas en este estudio de factibilidad económica financiera mediante las variables: tiempo de procura, costo de hardware, costo de software, costo de instalación, costo de mantenimiento y el uso de la tecnología a nivel mundial. Para analizar estas alternativas de manera cualitativa y cuantitativa. En las siguientes tablas, se puede observar el valor cuantitativo y cualitativo de las variables así como el resultado de las alternativas.

Tabla 16: Valor cuantitativo y cualitativo de las variables empleadas para la evaluación de las alternativas

Variables	Alto	Medio	Bajo
Tiempo de procura	1	2	3
Costo de hardware	1	2	3
Costo de software	1	2	3
Costo de instalación	1	2	3
Costo de mantenimiento	1	2	3
Uso de la tecnología a nivel mundial	3	2	1

Como se observa en la siguiente tabla, de acuerdo a la evaluación técnica y la económica financiera, la implementación de un sistema de control de acceso por reconocimiento de huella dactilar es la alternativa que más se adapta a las necesidades de la empresa de desarrollo tecnológico EDTEC, siendo a su vez la más empleada a nivel mundial.

Tabla 17: Evaluación cualitativa y cuantitativa de las alternativas

	Alternativas					
Variables	**1**	**2**	**3**	**4**	**5**	**6**
Tiempo de procura	Alto 1	Medio 2	Bajo 3	Alto 1	Medio 2	Bajo 3
Costo de hardware	Bajo 3	Bajo 3	Medio 2	Medio 2	Medio 2	Alto 1
Costo de software	Bajo 3	Medio 2	Medio 2	Medio 2	Medio 2	Medio 2
Costo de instalación	Bajo 3	Bajo 3	Medio 2	Medio 2	Alto 1	Alto 1
Costo de mantenimiento	Medio 2	Bajo 3	Bajo 3	Medio 2	Medio 2	Medio 2
Uso de la tecnología a nivel mundial	Bajo 1	Bajo 1	Alto 3	Alto 3	Medio 2	Bajo 1
Total evaluación cuantitativa	**13**	**14**	**15**	**12**	**11**	**10**

Inversión Total

Tabla 18: Estimación de la inversión total para implementar un sistema de control de acceso por reconocimiento de huella dactilar

Elementos	Total (Bs)	%
Controladoras de acceso	1.260.000.000,00	9,48
Cerraduras electromagnéticas	208.656.000,00	1,57
Fuentes de poder	130.410.000,00	0,98
Cableado UTP	7.800.000,00	0,06
Cable 18 AWG	200.000,00	0,00
Servidor	7.400.000.000,00	55,65
Lector de huella dactilar	3.780.000.000,00	28,43
Total Hardware	**12.787.066.000,00**	**96,16**
Licencia	3.000.000,00	0,02
Total Software	**3.000.000,00**	**0,02**
Costo de mantenimiento (anual)	10.350.000,00	0,08
Costo de implantación	496.800.000,00	3,74
Total	**13.297.216.000,00**	**100,00**

Depreciación

En la Tabla 18, a continuación, se presenta una proyección de la depreciación estimándose un período de depreciación de 5 años motivado a que la implementación de un sistema de control de acceso por reconocimiento de huella dactilar debe realizarse con los criterios de calidad tecnológica en cuanto al sensor de reconocimiento y la eficiencia del algoritmo de comparación en las muestras obtenidas; a su vez, los sistemas de control de acceso por huella dactilar son los más antiguos en el mercado y aun así siguen siendo los más empleados, por lo que se estima un mayor tiempo de vida del mismo.

Tabla 19: Depreciación de los activos de la inversión

Depreciación	Valor de los activos (Bs)	Años de vida útil	Valor de salvamento	Primer año (Bs)	Segundo año (Bs)	Tercer año (Bs)	Cuarto año (Bs)	Quinto año (Bs)
Controladoras de acceso	1.260.000.000	5	252.000.000	201.600.000	201.600.000	201.600.000	201.600.000	201.600.000
Cerraduras electromagnéticas	208.656.000	5	41.731.200	33.384.960	33.384.960	33.384.960	33.384.960	33.384.960
Fuentes de poder	130.410.000	5	26.082.000	20.865.600	20.865.600	20.865.600	20.865.600	20.865.600
Cableado UTP	7.800.000	5	1.560.000	1.248.000	1.248.000	1.248.000	1.248.000	1.248.000
Cable 18 AWG	200.000	5	40.000	32.000	32.000	32.000	32.000	32.000
Servidor	7.400.000.000	5	1.480.000.000	1.184.000.000	1.184.000.000	1.184.000.000	1.184.000.000	1.184.000.000
Lector de huella dactilar	3.780.000.000	5	756.000.000	604.800.000	604.800.000	604.800.000	604.800.000	604.800.000
Licencia	3.000.000	5	600.000	480.000	480.000	480.000	480.000	480.000
Total Depreciación				2.046.410.560	2.046.410.560	2.046.410.560	2.046.410.560	2.046.410.560

Parámetros usados para el cálculo		
	Método	Línea Recta
	Valor del salvamento	20%
	Años de depreciación	5

CAPITULO VI: LA PROPUESTA

6.1 Título

Plan para la implementación de un sistema de control de acceso a las instalaciones de la empresa EDTEC.

6.2 Propósito

El propósito de este documento “Plan para la implementación de un sistema de control de acceso” es brindar a la empresa de desarrollo tecnológico EDTEC, un instrumento de vital importancia para realizar todas las actividades relacionadas a la implementación de un sistema de control de acceso a sus instalaciones.

6.3 Objetivo

El objetivo de la propuesta es disponer de un instrumento guía que facilite la ejecución del proyecto “Implementación de un sistema de control de acceso a las instalaciones de una empresa de desarrollo tecnológico EDTEC”.

6.4 Justificación

La propuesta “Plan para la implementación de un sistema de control de acceso”, servirá para garantizarle a la empresa de desarrollo tecnológico una exitosa implementación de un sistema de control de acceso, brindándole a su vez, la seguridad necesaria a los equipos tecnológicos y al talento humano de la empresa para seguir ofreciendo apoyo a sus clientes en alcanzar sus objetivos empresariales.

6.5 Alcance

La utilización del presente documento es única y exclusivamente para realizar la implementación de un sistema de control de acceso a las instalaciones de la empresa de desarrollo tecnológico.

Para la elaboración de este plan se han tomado en consideración las áreas de conocimiento alcance, costo y tiempo, establecidas en la Guía de fundamentos para la Dirección de Proyectos del PMI (2013).

6.6 Modo de uso

Las actividades descritas en este plan son referenciales al tipo de tecnología que seleccione la empresa de desarrollo tecnológico EDTEC para la implementación del sistema de control de acceso, bien sea por biometría o tarjetas de identificación de acuerdo a las alternativas de solución evaluadas técnica, financiera y económicamente.

6.7 Estructura de la propuesta

A continuación, se presenta el Plan del proyecto propuesto para la implementación de un sistema de control de acceso, el cual será utilizado por la empresa de desarrollo EDTEC y por el proveedor seleccionado para realizar la implementación.

El plan propuesto es un documento de uso exclusivo para la empresa de desarrollo tecnológico EDTEC y podrá ser utilizado en cualquiera de las alternativas propuestas para la implementación de un sistema de control de acceso, bien sea por componente biométrico o tarjetas de identificación.

Este plan incluye estructuralmente los principales aspectos que deben ser considerados, tomando en cuenta las áreas de conocimiento de la Gerencia de Proyecto detalladas en la guía de fundamentos para la dirección de proyectos en el PMI (2013), específicamente las áreas de alcance, tiempo y costo.

a. Encabezado

Debe contener:

- Logo de la empresa de desarrollo tecnológico EDTEC ubicado en la parte superior izquierda.

- Identificación o nombre del documento, debajo del logo de la empresa de desarrollo tecnológico EDTEC.
- Número de revisiones al documento al lado del nombre del documento.
- Número de página, en la parte superior derecha del encabezado, debajo del logotipo de la empresa de desarrollo tecnológico EDTEC.

Figura 8: Encabezado del documento: Plan para la implementación de un sistema de control de acceso

Plan de Implementación de Sistema de Control de Acceso	Revisión 0	Página de

b. Sección de aprobación

Debe estar ubicada en la primera hoja del documento, centrado en la parte inferior del mismo y contiene las firmas de las personas que elaboran, validan y aprueban el plan así como la fecha de elaboración y vigencia del mismo.

Figura 9: Sección aprobación del plan

Elaborado	Revisado	Aprobado	Fecha de Vigencia
Firma	Firma	Firma	Desde
Fecha	Fecha	Fecha	Hasta

c. Sección información del plan

Incluye toda la información del plan para el entendimiento y uso adecuado del mismo, tales como:

1. Objetivo.
2. Alcance.
3. Modo de uso.

d. Sección actividades y tareas del plan

Se describen las actividades y tareas involucradas en el proceso de implantación de un software para control de acceso a las instalaciones de la empresa de desarrollo tecnológico EDTEC.

PLAN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO A LAS INSTALACIONES DE UNA EMPRESA DE DESARROLLO TECNOLÓGICO EDTEC

Elaborado	Revisado	Aprobado	Fecha de Vigencia
Firma	Firma	Firma	Desde
Fecha	Fecha	Fecha	Hasta

INDICE DE TABLAS

TABLA 1: ACTIVIDADES Y TAREAS DEL PLAN 4

TABLA 2: ELEMENTOS COMUNES NECESARIOS PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESO 5

TABLA 3: ELEMENTOS NECESARIOS PARA IMPLEMENTAR UN SISTEMA DE CONTROL DE ACCESO POR TIPO DE RECONOCIMIENTO 7

TABLA 4: ESTRUCTURA DESAGREGADA DE TRABAJO 11

TABLA 5: PERSONAL REQUERIDO PARA LA IMPLEMENTACIÓN 15

TABLA 6: ESTIMACIÓN DE TIEMPO PARA LA EJECUCIÓN DEL PLAN 17

TABLA 7: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR TARJETAS DE PROXIMIDAD 20

TABLA 8: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE VOZ 21

TABLA 9: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE HUELLA DACTILAR 21

TABLA 10: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL 22

TABLA 11: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE IRIS 22

TABLA 12: COSTOS DE IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO DE PALMA DE LA MANO 23

INDICE DE ILUSTRACIONES

ILUSTRACIÓN 1: FORMULARIO DE SOLICITUD DE CAMBIO 13

Actividades y tareas del plan

Tabla 1: Actividades y tareas del plan

Área de Conocimiento	Actividades	Tareas
Alcance	Definir el alcance	Recopilar requisitos para la implementación del sistema de control de acceso
		Desarrollar el enunciado del alcance del proyecto
	Crear la estructura desagregada de trabajo	Identificar los entregables
		Identificar las actividades y las secuencias entre ellas para obtener los entregables
		Identificar las fases mediante las cuales se realizaran las actividades y se obtendrán los entregables
	Validar el alcance	Verificar los entregables
		Verificar si existe cambios de requerimientos
	Controlar el alcance	Evaluar solicitudes de cambio
		Actualizar el alcance
Tiempo	Estimar los recursos de la actividades	Definir los recursos requeridos para las actividades
	Estimar la duración de las actividades	Definir la duración de las actividades
	Desarrollar del cronograma	Elaborar el cronograma
Costo	Estimar los costos de implementación	Preparar el presupuesto necesario para llevar a cabo la implementación del software de control de acceso

1. Definir el alcance

Consiste en desarrollar una descripción detallada del proyecto y del producto. El beneficio clave de este proceso es que describe las tareas necesarias para asegurarse de que el proyecto de implementación de un sistema para el control de acceso a la empresa de desarrollo tecnológico EDTEC, incluya todo lo requerido para su exitosa puesta en marcha.

El alcance del presente plan comprende todo lo necesario para la implementación de un sistema de control de acceso, con todos los pasos necesarios para aplicarlo de una manera eficaz y trasparente.

I. Recopilar requisitos para la implementación del sistema de control de acceso

Esta tarea permite identificar cada uno de los requisitos necesarios para llevar a cabo la implementación, específicamente aquellos asociados a la plataforma tecnológica para la satisfactoria implementación del sistema de control de acceso a las instalaciones de la empresa de desarrollo tecnológico EDTEC.

Los requisitos para la implementación de un sistema de control de acceso se encuentran en la factibilidad técnica de este proyecto, clasificado en elementos comunes y no comunes para implementación de un sistema de control de acceso. Los elementos no comunes requeridos para la implementación del sistema de control de acceso dependerán de la alternativa que sea seleccionada por el cliente, por componente biométrico o tarjeta de proximidad.

Los elementos comunes que serán requeridos para la implementación del sistema de control de acceso son:

Tabla 2: Elementos comunes necesarios para implementar un sistema de control de acceso

#	Elemento	Cantidad	Unidad	Descripción
1	Controladora de acceso	18	UND	Panel de 1 entrada, 1 salida. Capacidad para controlar 1 puerta. Función antipassback global y local.

#	Elemento	Cantidad	Unidad	Descripción
				Almacenamiento local de hasta 1000 eventos en modo sin comunicación con el servidor. Comunicación RS-232/RS-485/Ethernet.
2	Cerradura electromagnética	18	UND	Capacidad máxima de 500 libras. Consumo 12 VDC / 500 mA. / 24 VDC / 250 mA.
3	Fuente de poder	18	UND	Fuente de poder 12V 5 A. Con capacidad de carga de batería.
4	Cableado	200	MTS	Cables UTP: Categoría 5 utilizable como extensión para la interconexión de las lectoras con las controladoras. Cable 18 AWG: Cable eléctrico medida 18 awg para conexión de fuente de poder/batería/cerradura
5	Servidor	1	UND	Procesador Intel Xeon E5-2620 2.00GHz, 15M Cache, 7.2GT/s QPI, Turbo, 6C 95W. 8GB RDIMM, 1600MT/s, Low Volt, Dual Rank, x4 Data Width. Disco Duro Hot Plug 500GB 7.2K RPM Near-Line SAS 6Gbps 2.5 pulgadas.
6	Licencia	1	UND	Licencia para Software de Control de Acceso que permita controlar hasta 18 controladoras. Configuración remota de las controladoras. Manejo de base de datos histórica. Aplicación de Niveles de Acceso.

Los elementos que serán requeridos de acuerdo a la alternativa que sea seleccionada (componentes biométricos o tarjetas de proximidad o radiofrecuencia) son:

Tabla 3: Elementos necesarios para implementar un sistema de control de acceso por tipo de reconocimiento

#	Sistema de Reconocimiento	Cantidad	Unidad	Descripción
1	Huella dactilar	36	UND	Lector de huella dactilar: ✓ Método de escaneado: óptico ✓ Ventana de escaneo de huellas digitales: 25,5 * 18 mm. ✓ Resolución: 508 dpi. ✓ Velocidad de escaneado: 1/15 sec. ✓ Tasa de falsa aceptación (FAR - la probabilidad de tolerancia "extranjera"): 10-9 (1 en 1 mil millones)
2	Radiofrecuencia (no biométrico)	36	UND	a. Lector de tarjetas de proximidad: ✓ Alimentación: 9 - 12 vdc. ✓ Rango de lectura: 5 - 10 cm. ✓ Soporte para tarjetas rfid 125khz. ✓ Beep para confirmación de lectura. ✓ Antena interna. ✓ Distancia de transmisión 100Mts.
		50	UND	b. Tarjetas de proximidad aptas para funcionar con cualquier sistema que trabaje en 125 KHZ como los ANVIZ, ZKSOFTWARE, SOVICA entre otras.

#	Sistema de Reconocimiento	Cantidad	Unidad	Descripción
3	Iris	36	UND	Lectora de iris: ✓ Cámara de captura de datos cero contacto de 31 a 35cm de distancia aproximadamente. ✓ Pantalla táctil de 4.3". ✓ Resolución Iris 210 píxeles. ✓ Doble iris captura y autenticación.
4	Facial	36	UND	Lectora facial: ✓ Cámara de alta resolución. ✓ Microprocesador de 16MHz 8 bits. ✓ Energía: 110/220VAC ~ 12VDC. ✓ Velocidad interna de lectura: ≤0 .5s ✓ Velocidad de reconocimiento interna: ≤1s ✓ Capacidad de almacenamiento hasta 1200 rostros y 100,000 transacciones.
5	Palma de la mano	36	UND	Lector de palma de mano: ✓ Velocidad de acceso de aproximadamente de 15 usuarios/minuto. ✓ Tiempo del proceso de inscripción no más de 60 segundos.
6	Voz	36	UND	Micrófono para el reconocimiento de voz: ✓ Voltaje: 4.5-5.5V

II. Desarrollar el enunciado del alcance del proyecto

El enunciado del alcance del proyecto es la descripción del alcance, de los supuestos, de las restricciones del proyecto, de los entregables principales y el trabajo necesario para crear los entregables.

La empresa de desarrollo tecnológico EDTEC requiere de la implementación de un sistema de control de acceso para gestionar el acceso al personal autorizado a sus instalaciones, obteniendo seguridad de sus equipos tecnológicos y de su talento humano para seguir brindando apoyo a los clientes en alcanzar sus objetivos empresariales.

El alcance del presente plan se limita a la implementación de un sistema de control de acceso en las instalaciones de una empresa de desarrollo tecnológico EDTEC. Este alcance depende de la alternativa de solución que la empresa de desarrollo tecnológico seleccione, bien sea radiofrecuencia mediante tarjetas de proximidad o por componente biométrico mediante huella dactilar, reconocimiento de voz, reconocimiento palmar, facial y de iris, entre otros, los cuales se encuentran en la sección de alternativas de solución en el estudio económico financiero del presente proyecto.

Los principales entregables de este proyecto son: el plan para la implementación del sistema de control de acceso y en él toda la documentación y los pasos necesarios para aplicarlo de una manera eficaz y trasparente, así como la estimación de los recursos y la duración de las actividades mediante el cronograma y la estimación de los costos mediante el presupuesto de las alternativas de implementación.

2. Crear la estructura desagregada de trabajo

En esta actividad se identifican los entregables por medio de la descomposición del proyecto de implantación del sistema para el control de acceso de una empresa de desarrollo tecnológico en componentes más pequeños y fáciles de manejar.

I. Identificar los entregables

En esta sección del documento se describen los entregables que se obtendrán durante el proceso de implantación del sistema. Incluye toda aquella documentación importante para el cumplimiento de los objetivos, entre ellos podemos mencionar: el plan de implementación del sistema de control de acceso donde se encuentra a su vez, el enunciado del alcance del plan, la estructura desagregada de trabajo, el cronograma de implementación, el formato de solicitudes de cambios al alcance y el formato para la elaboración de órdenes de compra de materiales y equipos.

II. Identificar las actividades necesarias para obtener los entregables

En esta sección se incluyen sólo las actividades que se requieren como parte del alcance del proyecto de implementación del sistema de control de acceso. Se identifican y describen todas las actividades específicas que deben ser cumplidas, las cuales, son agrupadas en fases o etapas, se evalúan y documentan sus dependencias o interrelación entre ellas. Las actividades necesarias para obtener los entregables se encuentran identificadas en el cuadro 4 estructura desagregada de trabajo.

III. Identificar las fases mediante las cuales se realizaran las actividades y se obtendrán los entregables.

Como producto de la descomposición del proyecto en componentes más pequeños y fáciles de manejar, en esta etapa se identifican y describen los módulos en los cuales serán agrupadas las distintas tareas que darán como resultado cada uno de los entregables. Entre las fases establecidas para ejecutar todas las actividades, identificadas en la estructura de trabajo desagregada se encuentran: Inicio y planificación, Control y seguimiento, Selección de proveedores para la procura de equipos, Instalación de los equipos en las diferentes oficinas de la empresa de desarrollo EDTEC y Pruebas de certificación de control de acceso.

Tabla 4: Estructura Desagregada de Trabajo

EDT Estructura Desagregada de Trabajo	
0	**Plan de Implementación de un sistema de control de acceso**
1	***Inicio y Planificación***
1.1	Identificación necesidades del cliente
1.2	Revisión del análisis de los diferentes dispositivos de control de acceso en el mercado.
1.3	Revisión del estudio de factibilidad económica financiero de los diferentes dispositivos de control de acceso.
1.4	Revisión del análisis de los riesgos asociados al plan para la implementación del sistema de control de acceso.
1.5	Definir el alcance del plan para la implementación.
1.5.1	Recopilar requisitos para la implementación del sistema de control de acceso.
1.5.2	Desarrollar el enunciado del alcance del proyecto.
1.6	Crear la estructura desagregada de trabajo.
1.6.1	Identificar los entregables.
1.6.2	Identificar las actividades necesarias para obtener los entregables.
1.6.3	Identificar las fases mediante las cuales se realizaran las actividades y se obtendrán los entregables.
1.7	Estimar los recursos de las actividades.
1.8	Estimar la duración de las actividades.
1.9	Desarrollar el cronograma.
1.10	Evaluar los costos de implementación.

EDT Estructura Desagregada de Trabajo	
1.11	Evaluación de propuestas y selección del dispositivo de control de acceso a implementar.
2	***Control de seguimiento***
2.1	Validar el alcance
2.1.1	Verificar los entregables
2.1.2	Verificar si existe cambios de requerimientos
2.2	Controlar y actualizar el alcance
2.2.1	Evaluar solicitudes de cambio
2.2.2	Actualizar el alcance
3	***Selección de proveedores para la procura de equipos.***
3.1	Evaluación de proveedores de acuerdo al dispositivo de control de acceso seleccionado.
3.2	Elaboración de orden de pago al proveedor seleccionado
3.3	Registro de entrada de inventario de los equipos
3.4	Traslado de equipos a las diferentes oficinas donde serán implementados
4	***Instalación de los equipos en las diferentes oficinas de la empresa de desarrollo EDTEC.***
4.1	Gestión de permisos para la instalación
4.2	Instalación del sistema de control de acceso
4.2.1	Hardware
4.2.1.1	Controladora de acceso
4.2.1.2	Cerradura electromagnética
4.2.1.3	Fuente de poder
4.2.1.4	Cableado
4.2.1.5	Servidor
4.2.1.6	Dispositivo de reconocimiento seleccionado
4.2.2	Software
5	***Pruebas de certificación de control de acceso***

3. Validar el alcance

En esta sección del documento se realizan las revisiones a cada uno de los entregables del proceso de implementación del sistema de control de acceso con el propósito de determinar el nivel de aceptación formal por parte de la empresa. A continuación se detallan las tareas correspondientes a esta actividad:

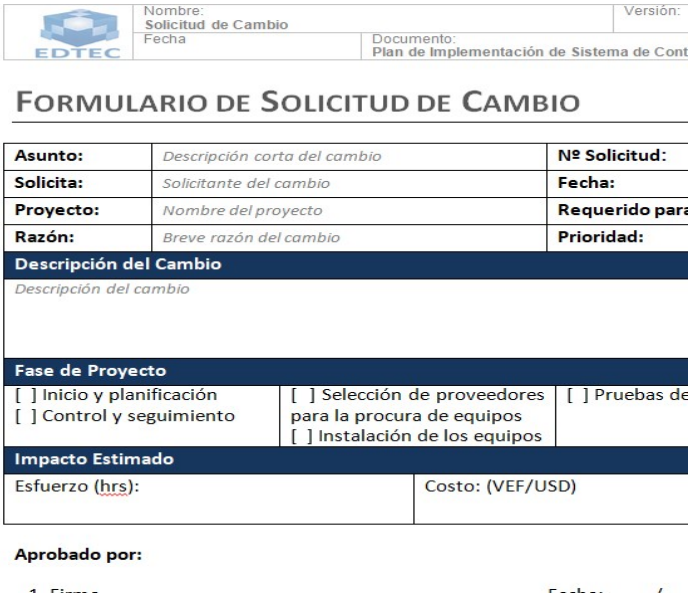
I. Verificar los entregables

Se realizan revisiones a cada uno de los productos o entregables del proceso de implementación del sistema de control de acceso con la finalidad de evaluar el nivel de cumplimiento satisfactorio y documentar los detalles al respecto, pudiendo surgir en esta etapa solicitudes de cambio en alguno de ellos.

II. Verificar si existe cambios de requerimientos

Las solicitudes de cambio generadas en la revisión de cada uno de los entregables deben ser aprobadas o rechazadas para realizar dichos cambios al alcance del proyecto de implementación del sistema de control de acceso. En esta sección del documento se verifica si existen solicitudes de cambio formalizadas mediante el formato establecido para las mismas (formulario de solicitud de cambio).

Ilustración 1: Formulario de solicitud de cambio



EDTEC | Nombre: Solicitud de Cambio | Versión: | Fecha | Documento: Plan de Implementación de Sistema de Cont

FORMULARIO DE SOLICITUD DE CAMBIO

Asunto:	*Descripción corta del cambio*	**Nº Solicitud:**
Solicita:	*Solicitante del cambio*	**Fecha:**
Proyecto:	*Nombre del proyecto*	**Requerido para**
Razón:	*Breve razón del cambio*	**Prioridad:**

Descripción del Cambio

Descripción del cambio

Fase de Proyecto

[ ] Inicio y planificación [ ] Control y seguimiento	[ ] Selección de proveedores para la procura de equipos [ ] Instalación de los equipos	[ ] Pruebas de

Impacto Estimado

Esfuerzo (hrs):	Costo: (VEF/USD)

Aprobado por:

1. Firma: Fecha: /

4. Controlar y actualizar el alcance

En esta sección del documento, al igual que en la sección validar el alcance, se procede a verificar y evaluar los entregables a fin de establecer actualizaciones en el alcance en caso de ser necesario.

I. Evaluar solicitudes de cambio

En esta sección, en caso de que exista alguna solicitud de cambio, se asigna un estatus a cada una de ellas (aprobada, rechazada) y se documentan los detalles por medio de minutas de reunión y actualización de formulario de solicitud de cambio.

II. Actualizar el alcance

Se determinan los cambios a realizar en el alcance y se realizan las actualizaciones necesarias al alcance establecido inicialmente.

5. Estimar los recursos de las actividades

En esta sección del documento, se indican los recursos necesarios para cumplir con las actividades que darán como resultados los entregables establecidos en el alcance. Entre los recursos necesarios para cumplir con dichos entregables se pueden mencionar: equipos, personas y materiales.

I. Definir los recursos requeridos para las actividades

Se determinan los recursos necesarios para llevar a cabo cada una de las actividades y tareas establecidas para la implementación del sistema de control de acceso.

Aunado a los elementos tecnológicos comunes y no comunes requeridos para la instalación del sistema de control de acceso indicados en el alcance del presente documento, específicamente en el cuadro 2 y 3, se requiere de un personal calificado para ejercer cada uno de los siguientes

roles al momento de ejecutar la implementación del sistema de control de acceso a las instalaciones de la empresa de desarrollo tecnológico EDTEC:

Tabla 5: Personal requerido para la implementación

Cargo	Perfil	Rol
Gerente de proyecto	Educación: Profesional con carrera: Ingeniero Industrial, Ingeniero Civil, Ingeniero de Sistemas o Informática, Ingeniero Mecánico Eléctrico Experiencia: al menos 3 años en administración y control de proyectos. Conocimientos de: -Administración y Control de Proyectos - Metodología Project Management - Manejo de software de administración y control de proyectos - Windows y Ofimática; Microsoft Project - Planeación Estratégica - Sistemas de Gestión de Calidad ISO 9000	Planear, dirigir y controlar las operaciones de la Gerencia a su cargo, determinando, conjuntamente con el equipo de trabajo, las líneas de acción para la prospección del proyecto de acuerdo al alcance; coordinando a la vez la estrategia operativa del proyecto y evaluando la rentabilidad del mismos a través del seguimiento oportuno y preciso de los costos de operación y el avance en los resultados obtenidos.
Administrador	Educación: Licenciado en Administración. Experiencia: Cinco (5) años de experiencia progresiva de carácter operativo, supervisor y estratégico en el área de Administración. Redactar y analizar informes técnicos. Realizar cálculos numéricos. Analizar problemas presupuestarios.	Controlar las actividades administrativas, de presupuesto, contabilidad, mantenimiento y proveeduría de los servicios y los recursos materiales y financieros asignados al proyecto, planificando, coordinando y ejecutando los sistemas y procedimientos contables y financieros, a fin de satisfacer las necesidades del proyecto y administrar efectivamente sus recursos.

Cargo	Perfil	Rol
Jefe de compras	Educación: Licenciatura en Administración Pública, Administración de Empresa y Contabilidad o Economía. Experiencia: Dos (2) años de experiencia en procura y adquisiciones en empresas. Habilidades: -Realizar cálculos numéricos. -Redactar y analizar órdenes de compra. -Expresarse en forma oral y escrita fluidamente. -Capacidad de organización. -Para supervisar. -Para dar instrucciones.	Supervisar las compras a fin de garantizar la procura oportuna, eficiente y correcta del material para operaciones, sobre una base de calidad requerida y precio competitivo. - Revisar los sustentos de compra y aprobar las órdenes de compra - Coordinar importación de equipos y materiales (facilitar documentos e información de órdenes de compra, indicar modo de envío) - Evaluar proveedores
Consultor técnico	Educación: especialista sistemas de información. Experiencia: 5 años. Ofrece una opinión experta, pericia o conocimientos relativos a los requisitos técnicos y de usuario que han de tenerse en cuenta en la implementación de un sistema de control de acceso.	Es responsable del levantamiento de requerimientos técnicos necesarios para la instalación y puesta en marcha del hardware y software en la implementación del sistema de control de acceso
Instaladores	Educación: Profesional en Ingeniería Electrónica, Eléctrica o en una carrera del área de Computación e Informática. Experiencia: 1 año en instalación de sistemas de información, de cableado estructurado y servidores. Conocimientos de: Electrónica digital. Arquitectura de equipos electrónicos y redes. Normas sobre cableado estructurado y fibra óptica. Manejo de programas de computación afines al cargo.	Es responsable de la instalación y puesta en marcha del hardware y software en la implementación del sistema de control de acceso

6. Estimar la duración de las actividades

Para estimar la duración de cada actividad establecida en el alcance, es de vital importancia tener en consideración toda la documentación asociada al mismo y a los recursos requeridos para la implementación del software de control de acceso.

I. Definir la duración de las actividades

Se define la cantidad de tiempo que transcurre desde el inicio de cada actividad o tarea. Para estimar la duración del tiempo puede usarse la siguiente herramienta:

- Juicio de expertos: Se caracteriza por la experiencia de los proveedores de los sistemas de control de acceso.

Partiendo de la estructura desagregada de trabajo EDT donde se indican los entregables para la implementación de un sistema de control de acceso a la empresa de desarrollo tecnológico EDTEC y haciendo uso de la herramienta juicio de expertos para estimar la duración del tiempo de cada una de las actividades, se tiene que, ejecutar el siguiente plan hasta la implementación y puesta en marcha del sistema de control de acceso tiene una duración de 62 días.

En el siguiente cuadro se puede observar de forma detallada la estimación de cada una de las actividades:

Tabla 6: Estimación de tiempo para la ejecución del plan

Actividades		Duración
0	**Plan de Implementación de un sistema de control de acceso**	**62 días**
1	***Inicio y Planificación***	**20 días**
1.1	Identificación necesidades del cliente	1 día
1.2	Revisión del análisis de los diferentes dispositivos de control de acceso en el mercado	3 días
1.3	Revisión del estudio de factibilidad económica financiero de los diferentes dispositivos de control de acceso	1 día
1.4	Revisión del análisis de los riesgos asociados al plan para la implementación del sistema de control de acceso	1 día
1.5	Definir el alcance del plan para la implementación	**3 días**
1.5.1	Recopilar requisitos para la implementación del sistema de control de acceso	2 días
1.5.2	Desarrollar el enunciado del alcance del proyecto	1 día
1.6	Crear la estructura desagregada de trabajo	**5 días**

	Actividades	Duración
1.6.1	Identificar los entregables	2 días
1.6.2	Identificar las actividades necesarias para obtener los entregables	2 días
1.6.3	Identificar las fases mediante las cuales se realizaran las actividades y se obtendrán los entregables	1 día
1.7	Estimar los recursos de las actividades	1 día
1.8	Estimar la duración de la actividades	1 día
1.9	Desarrollar el cronograma	2 días
1.10	Evaluar los costos de implementación	2 días
1.11	Evaluación de propuestas y selección del dispositivo de control de acceso a implementar.	1 día
2	***Control de seguimiento***	**3 días**
2.1	Validar el alcance	**1 día**
2.1.1	Verificar los entregables	1 día
2.1.2	Verificar si existe cambios de requerimientos	1 día
2.2	Controlar y actualizar el alcance	**3 días**
2.2.1	Evaluar solicitudes de cambio	1 día
2.2.2	Actualizar el alcance	2 días
3	***Selección de proveedores para la procura de equipos.***	**12 días**
3.1	Evaluación de proveedores de acuerdo al dispositivo de control de acceso seleccionado.	7 días
3.2	Elaboración de orden de pago al proveedor seleccionado	1 día
3.3	Registro de entrada de inventario de los equipos	2 días
3.4	Traslado de equipos a las diferentes oficinas donde serán implementados	2 días
4	***Instalación de los equipos en las diferentes oficinas de la empresa de desarrollo EDTEC***	**24 días**
4.1	Gestión de permisos para la instalación	2 días
4.2	Instalación del sistema de control de acceso	**22 días**
4.2.1	Hardware	**20 días**
4.2.1.1	Controladora de acceso	10 días
4.2.1.2	Cerradura electromagnética	10 días
4.2.1.3	Fuente de poder	1 día
4.2.1.4	Cableado	3 días
4.2.1.5	Servidor	3 días
4.2.1.6	Dispositivo de reconocimiento seleccionado	3 días
4.2.2	Software	2 días
5	***Pruebas de certificación de control de acceso***	6 días

7. Desarrollar el cronograma

Se indican las fechas iniciales y finales de cada actividad planificada para realizar la implementación del sistema de control de acceso.

I. Elaborar el cronograma

El desarrollo del cronograma debe ser revisado y aprobado, en él se debe indicar la duración de cada una de las actividades.

La elaboración del cronograma para la implementación del sistema de control de acceso a las instalaciones de la empresa de desarrollo EDTEC, dependerá de la aprobación de la empresa para implementar dicho sistema y así satisfacer su necesidad de incrementar los niveles de seguridad.

Para el desarrollo del cronograma, se debe tomar en consideración el cuadro de estimación de tiempo para cada una de las actividades, así como la fecha de inicio en la ejecución del presente plan.

8. Estimar los costos de implementación

Para la estimación de los costos de implementación se puede utilizar alguna herramienta que facilite su desarrollo como hojas de cálculo. A su vez es importante conocer la alternativa seleccionada para ser implementada ya sea por componente biométrico o tarjetas de aproximación.

I. Preparar el presupuesto necesario para llevar a cabo la implementación del sistema de control de acceso

El presupuesto se desarrolla a partir de una aproximación del costo de los recursos necesarios para culminar cada actividad. Se debe tomar en consideración posibles variaciones que puedan suscitarse. El desarrollo del presupuesto necesario para llevar a cabo la implementación del sistema de

control de acceso, dependerá del tipo de alternativa de solución que la empresa de desarrollo EDTEC seleccione, por biometría o tarjeta de aproximación para la identificación y reconocimiento, por lo que en este punto solo se incluye los datos obtenidos en el estudio de factibilidad económica financiera realizado para este proyecto.

A continuación se indican los costos para implementar un sistema de control de acceso biométrico o por tarjeta de proximidad. Los montos están expresados en bs calculados a una tasa de 69000 bs por dólar americano de acuerdo al Convenio Cambiario N° 38 (c) publicado por el Banco Central de Venezuela para el segundo trimestre del año 2018:

Tabla 7: Costos de implementación de un sistema de control de acceso por tarjetas de proximidad

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Lector de proximidad	36 un.	39.524.000,00	1.422.864.000,00
Tarjetas de proximidad	50 un.	450.000,00	22.500.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Total Hardware			**10.452.430.000,00**
Licencia	1 un.	2.000.000,00	2.000.000,00
Total Software			**2.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	20.700.000,00
Costo de instalación	18 un.	20.700.000,00	621.000.000,00
Total			**10.840.830.000,00**

Tabla 8: Costos de implementación de un sistema de control de acceso por reconocimiento de voz

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Micrófono para el reconocimiento de voz	36 un.	55.200.000,00	1.987.200.000,00
Total Hardware			**10.994.266.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	6.900.000,00	9.660.000,00
Costo de instalación	18 un.	13.800.000,00	248.400.000,00
Total			**11.252.566.000,00**

Tabla 9: Costos de implementación de un sistema de control de acceso por reconocimiento de huella dactilar

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de huella dactilar	36 un.	105.000.000,00	3.780.000.000,00
Total Hardware			**12.787.066.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	10.350.000,00	13.800.000,00
Costo de instalación	18 un.	27.600.000,00	621.000.000,00
Total			**13.297.216.000,00**

Tabla 10: Costos de implementación de un sistema de control de acceso por reconocimiento facial

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector facial	36 un.	117.300.000,00	4.222.800.000,00
Total Hardware			**13.229.866.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	13.800.000,00
Costo de instalación	18 un.	34.500.000,00	683.100.000,00
Total			**13.867.666.000,00**

Tabla 11: Costos de implementación de un sistema de control de acceso por reconocimiento de iris

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de iris	36 un.	124.200.000,00	4.471.200.000,00
Total Hardware			**13.478.266.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	20.700.000,00
Costo de instalación	18 un.	37.950.000,00	869.400.000,00
Total			**14.178.166.000,00**

Tabla 12: Costos de implementación de un sistema de control de acceso por reconocimiento de palma de la mano

Elementos	Cantidad	Costo por unidad (Bs)	Total (Bs)
Controladora de acceso	18 un.	70.000.000,00	1.260.000.000,00
Cerradura electromagnética	18 un.	11.592.000,00	208.656.000,00
Fuente de poder	18 un.	7.245.000,00	130.410.000,00
Cableado UTP	200 m.	39.000,00	7.800.000,00
Cable 18 AWG	200 m.	1.000,00	200.000,00
Servidor	1 un.	7.400.000.000,00	7.400.000.000,00
Lector de palma de la mano	36 un.	975.000.000,00	35.100.000.000,00
Total Hardware			**44.107.066.000,00**
Licencia	1 un.	3.000.000,00	3.000.000,00
Total Software			**3.000.000,00**
Costo de mantenimiento (anual)	1 un.	13.800.000,00	10.350.000,00
Costo de instalación	18 un.	41.400.000,00	745.200.000,00
Total			**44.869.066.000,00**

6.8 Determinar los riesgos asociados al plan diseñado para la implementación del sistema de control de acceso.

El riesgo de un proyecto es un evento o condición incierta que, si ocurre, tiene un efecto positivo o negativo en al menos un objetivo del proyecto, sea éste de tiempo, costo, alcance o calidad. Las normas ISO/DIS 9001:2015 e ISO/DIS 9000:2015, definen el riesgo como el efecto de la incertidumbre, entendiéndose por efecto, una desviación de lo esperado positiva o negativamente y por incertidumbre el estado, aunque sea parcial, de la deficiencia de información relacionada con el conocimiento de un evento, su consecuencia, o probabilidad.

Tabla 20: Riesgos asociados al plan diseñado

#	Causa	Evento	Consecuencia	Área de Impacto	Acción Pre-Evento	Acción Post-Evento
1	Fallas en la documentación del plan	Falta de documentos o registro de documentos incompletos	Información desactualizada u obsoleta.	Alcance / Calidad	Revisar constantemente las actividades del plan para cerciorarse que se están realizando dentro de lo establecido y lo que se encuentra con retraso para corregir el curso del proyecto a tiempo.	Reducir la periodicidad entre las reuniones de avances y seguimiento para detectar a tiempo futuras irregularidades y corregir de manera rápida cualquier desviación que se presente.
2	Deficiencias en la gestión de comunicaciones	Falta de procedimientos de comunicación entre los interesados	Vacíos de información o información redundante.	Alcance / Calidad	Realizar un plan de comunicaciones entre los responsables del proyecto a fin de evitar el retrabajo entre ellos y conocer los avances en la realización del plan.	Reducir la periodicidad entre las reuniones de avances y seguimiento para detectar a tiempo futuras irregularidades y corregir de manera rápida cualquier desviación que se presente.

#	Causa	Evento	Consecuencia	Área de Impacto	Acción Pre-Evento	Acción Post-Evento
3	Deficiencias en la gestión de la calidad	Falla en el cumplimiento de acuerdos, requerimientos y estándares de calidad mínimos para la entrega del plan de implementación	Plan fuera de los estándares de calidad solicitados por el cliente y no apto para su futura implementación.	Calidad	Realizar una debida gestión de la calidad que incluya un seguimiento en las funcionalidades del software requeridas por el usuario	Reducir la periodicidad entre las reuniones de avances y seguimiento para detectar a tiempo futuras irregularidades y corregir de manera rápida cualquier desviación que se presente
4	Demora en la entrega del plan para la implementación del proyecto	Planificaciones no ajustadas a la realidad. Aumento en los tiempos de entrega e incumplimiento del cronograma	Cierre de proyecto extemporáneo	Tiempo / Costo	Para las actividades a realizar en el proyecto, tomar como referencia el tiempo que se han tomado en proyectos similares y así poder establecer un cronograma de entrega ajustado a la realidad	Rediseñar el cronograma
5	Falla en la identificación de necesidades de los usuarios	Falla en la documentación de las necesidades del usuario	Necesidades del cliente mal documentadas o sin la aprobación del cliente	Alcance / Calidad	Realizar reuniones, entrevistas y encuestas con los clientes para plasmar sus requerimientos en la ejecución de la solución.	Efectuar reuniones de seguimiento para mostrar los avances y aprobarlos si estos cumplen con los requerimientos esto permitirá realizar correcciones a tiempo.
6	Diseño de alternativas de solución incorrectas	Diseño de propuestas con elementos diferentes a los requeridos para satisfacer las necesidades del cliente	Alternativas que no cumplen con las necesidades de los clientes	Alcance / Calidad	Realizar reuniones, entrevistas y encuestas con los clientes para plasmar sus requerimientos en la ejecución de la solución.	Efectuar reuniones de seguimiento para mostrar los avances y aprobarlos si estos cumplen con los requerimientos esto permitirá realizar correcciones a tiempo.

#	Causa	Evento	Consecuencia	Área de Impacto	Acción Pre-Evento	Acción Post-Evento
7	Falla en el establecimiento de los indicadores de cumplimiento para el análisis de los proveedores	Fallas en el análisis de proveedores y aprobación incorrecta del mismo	Análisis incorrecto de proveedores y aprobación de proveedor que no cumpla con los requerimientos del usuario	Alcance / Calidad	Analizar y seleccionar fuentes alternativas de equipos y suministros que cumplan con los requerimientos del cliente (Software y Hardware).	Considerar la inclusión de un experto para validar los requerimientos de software y hardware y desarrollar relaciones de colaboración con los proveedores.
8	Levantamiento inadecuado de las funcionalidades requeridas para el software y hardware	Fallas en el análisis de proveedores y futura aprobación incorrecta del mismo.	Análisis incorrecto de proveedores y aprobación de proveedor que no cumpla con los requerimientos del usuario.	Alcance / Calidad / Costo	Investigar las opciones de software y de hardware existentes con los diferentes proveedores en el mercado, asegurándose de que funcionen de acuerdo a los requerimientos del usuario.	Considerar la inclusión de un experto para validar los requerimientos de software y hardware.

En la tabla anterior, se indican los riesgos asociados al plan para la implementación de un sistema de control de acceso a la empresa de desarrollo tecnológico EDTEC, estableciendo la causa, consecuencia, área de impacto y lo que debe realizarse antes y después de materializarse cada uno de estos riesgos. La importancia de conocer los riesgos asociados al diseño de un plan radica en poder prevenir los efectos negativos de la incertidumbre y garantizar que se alcancen todos los resultados previstos cumpliendo con los estándares mínimos de calidad exigidos para su entrega.

6.9 Factibilidad de la propuesta

Factibilidad Técnica

El plan propuesto es factible porque proporciona diferentes alternativas entre los recursos técnicos necesarios para efectuar las actividades o procesos que requiere la ejecución del proyecto. A su vez, determina lo que será la inversión y costos que sustentan la rentabilidad de cada una de esas alternativas.

Factibilidad Operativa

Operativamente hablando, el plan propuesto es factible porque no acarrea ningún costo a la empresa de desarrollo tecnológico EDTEC. Por otra parte, en caso de realizar la implementación del sistema de control de acceso, facilita la ejecución del proyecto y garantiza que la misma sea de manera exitosa.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

La propuesta desarrollada en esta investigación “Plan para la implementación de un sistema de control de acceso”, podrá ser utilizada con cualquier dispositivo de reconocimiento que la empresa de desarrollo tecnológico desee implementar.

Cada uno de los criterios de satisfacción de la empresa de desarrollo tecnológico EDTEC en cuanto a los elementos y componentes que debe tener el sistema de control de acceso, fueron evaluados y revisados de acuerdo a conocimientos y experiencias en el desarrollo e implementación de proyectos de esta índole.

El plan propuesto en esta investigación, está alineado con las políticas, requerimientos y objetivos estratégicos de la empresa de desarrollo tecnológico EDTEC.

Con la propuesta desarrollada en la presente investigación “Plan para la implementación de un sistema de control de acceso”, se dio respuesta a cada uno de los objetivos planteados inicialmente.

El estudio realizado implicó una amplia documentación bibliográfica para analizar los diferentes dispositivos de reconocimiento usados en los sistemas de control de acceso a nivel mundial, realizando comparaciones entre los beneficios y desventajas de cada uno de ellos, resultando el dispositivo de huella dactilar, el que cumple con la mayoría de los criterios de evaluación, entre los que se encuentra unicidad, fiabilidad, facilidad de uso, resistencia a ataques, aceptabilidad, costo y permanencia en el mercado, entre otros.

Las áreas de alcance, tiempo y costo, representan para el plan propuesto un aspecto de vital importancia para su éxito, ya que las mismas permiten tener una visión más amplia y objetiva de qué es lo que se va a hacer, cómo se va a hacer y a donde se va a llegar con lo que va a hacer.

Recomendaciones

Con la finalidad de satisfacer la necesidad de la empresa de desarrollo tecnológico EDTEC de incrementar los niveles de seguridad a sus instalaciones, se recomienda implementar un sistema de control de acceso que garantice la integridad y protección de sus activos tecnológicos y talento humano, haciendo uso adecuado del plan propuesto, ya que permitirá administrar eficientemente los recursos disponibles para ello.

Para la implementación del sistema de control de acceso a las instalaciones de la empresa de desarrollo EDTEC, se recomienda el uso de la tecnología biométrica reconocimiento de huella dactilar, ya que de acuerdo a la evaluación técnica y la económica financiera, la implementación de un sistema de control de acceso por reconocimiento de huella dactilar es la alternativa que más se adapta a las necesidades de la empresa de desarrollo tecnológico EDTEC, siendo a su vez la más empleada a nivel mundial.

Dar a conocer el plan propuesto a cada uno de los responsables e interesados en la ejecución del mismo.

Utilizar las técnicas y herramientas de la gerencia de proyectos propuestas en el plan tal como: la estructura desagregada de trabajo, el cronograma y el formulario de control de cambios entre otras que son necesarias para llevar a cabo la implementación del sistema de control de acceso de manera exitosa.

Tomar en cuenta que en todo proceso de implementación, es de gran relevancia fijar metas viables y realistas que formen la base para determinar el alcance, presupuesto y tiempo. De esto depende el éxito en la ejecución de cualquier proyecto.

REFERENCIAS BIBLIOGRÁFICAS

Alves, C., Benedetto, M., Etchart, G., Luna, L., Leal, C., Fernández, M., Berón, G. y Loggio, S. (2014). Identificación de Personas Mediante Sistemas Biométricos.

Estudio de Factibilidad y su Implementación en Organismos Estatales. *Ciencia, Docencia y Tecnología Suplemento*. Argentina: Universidad Nacional de Entre Ríos. [en línea] Disponible en: http://pcient.uner.edu.ar/index.php/Scdyt/article/viewFile/7/18 [Revisado 30 Octubre 2017].

Arias, F. (2004). *El Proyecto de Investigación. Introducción a la Metodología Científica* (4ta ed.). Caracas: Epísteme

Arias, F. (2006). *El Proyecto de Investigación. Introducción a la Metodología Científica* (5ta ed.). Caracas: Epísteme

Baca Urbina, G. (2010). *Evaluación de Proyectos*. 6ta ed. México: McGraw-Hill.

Balestrini, M. (2002). *Como se elabora el proyecto de investigación*. Caracas: Consultores Asociados BL.

Bernal, D. (2012). *Estudio de Factibilidad para la Instalación de una Franquicia de Lavado Ecológico de Automóviles en la Ciudad de Puerto Ordaz, Estado Bolívar.* Trabajo Especial de Grado. Universidad Católica Andrés Bello: Puerto Ordaz.

Blanco, A. (2010). *Formulación y Evaluación de Proyectos*. 8va ed. Caracas.

Blanco, A. (2005). *Formulación y evaluación de proyectos.* Madrid: Edisofer.

Chamoun, Y. (2002). *Administración Profesional de Proyectos la Guía*. México: McGraw-Hill.

Cobo, A., Gómez, P., Pérez, D. y Rocha, R. (2005). *PHP y MySQL. Tecnologías para el Desarrollo de Aplicaciones Web.* Madrid: Díaz de Santos.

Colegio de Ingenieros de Venezuela (1996). *Código de Ética Profesional.* [en línea] Disponible en: http://www.civ.net.ve/uploaded_pdf/cep.pdf [Revisado 16 Noviembre 2017].

Coronel, R. (2017). *El reinado de la biometría - Revista ¿Cómo ves? - Dirección General de Divulgación de la Ciencia de la UNAM.* [en línea] Comoves.unam.mx. Disponible en: http://www.comoves.unam.mx/numeros/articulo/104/el-reinado-de-la-biometria [Revisado 16 Noviembre 2017].

Cortés, J., Medina, F. y Muriel, J. (2010). Sistemas de Seguridad Basados en Biometría. *Scientia et Technica*. Colombia: Universidad Tecnológica de Pereira. Recuperado de: http://www.redalyc.org/pdf/849/84920977016.pdf [Revisado 11 Octubre 2017].

Gray, C. y Larson, E. (2009). *Administración de proyectos*. México: McGraw-Hill.

Gómez, M. (2006). *Introducción a la Metodología de la Investigación Científica.* Argentina: Editorial Brujas.

Gutiérrez, J. (2007). *Estudio de Factibilidad para el Control de Acceso Biométrico, en una Empresa Empleando Lectores de Huella Digital.* Trabajo Especial de Grado Universidad la Salle: Bogotá.

Hernández, R., Fernández, C. y Baptista, M. (2003). *Metodología de la investigación*. 5ra. ed. México: McGraw-Hill.

Hurtado, J. (2000). *Metodología de la investigación*. Caracas, Venezuela: Quirón Ediciones.

Hurtado, J. (2010). *El proyecto de investigación* (6ta ed.). Caracas, Venezuela: Quirón Ediciones.

Incibe.es. (2016). *Instituto Nacional de Ciberseguridad: Tecnologías biométricas aplicadas a la ciberseguridad* [en línea] Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf [Revisado 20 Abril 2018].

International Standard Organization, *ISO 9000:2015: Quality management systems, Fundamentals and vocabulary.*

International Standard Organization, *ISO 9001:2015: Quality management systems, Fundamentals and vocabulary.*

Ley Especial Contra Delitos Informáticos. Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

Ley Sobre Mensajes de Datos y Firmas Electrónicas. Gaceta oficial N° 37.148 de Febrero 28, 2001, mediante el decreto N° 1.181

Lledó, P. y Rivarola, G. (2007). *Gestión de Proyectos.* Argentina: Prentice Hall y Pearson Education.

Llorens Fabregas, J. (2005). *Gerencia de Proyectos de Tecnología de Información.* Caracas, Venezuela: El Nacional.

Mecalux.es. (2018). *Grupo Internacional Biométrico: Identificación (casi) infalible.* [en línea] Disponible en: https://www.mecalux.es/articulos-de-logistica/biometria-identificacion-casi-infalible [Revisado 20 Abril 2018].

Palacios, L. (2009). *Gerencia de Proyectos. Un Enfoque Latino.* Caracas: Publicaciones UCAB. 5ta Edición.

Peru.com, R. (2017). *Gallup: Los diez países de Latinoamérica más peligrosos*. [en línea] Disponible en: https://peru.com/actualidad/los-diez/gallup-diez-paises-latinoamerica-mas-peligrosos-fotos-noticia-278193-891471 [Revisado 10 Noviembre 2017].

Portillo, Juan (2014). *Plan para el Desarrollo de una Aplicación para la Gestión de Proyectos de Desarrollo de Software*. Trabajo Especial de Grado. Universidad Católica Andrés Bello: Caracas.

Poveda, M. y Merchán, F. (2015). Implementación de un Sistema de Control de Acceso Basado en Reconocimiento Facial*. Prisma Tecnológico.* Panamá:

Universidad Tecnológica de Panamá. [en línea] Disponible en: http://revistas.utp.ac.pa/index.php/prisma/article/view/609/html [Revisado 11 Octubre 2017].

Project Management Institute (PMI) (2006). *Código de Ética y Conducta Profesional.* [en línea] Disponible en: http://www.pmi.org/-/media/pmi/documents/public/pdf/ethics/pmi-code-of-ethics.pdf?sc_lang_temp=es-ES [Revisado 19 Noviembre 2017].

Project Management Institute (PMI) (2013). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK)*. Pennsylvania: Project Management Institute, Inc.

Rada G. (2007). *Unidades de análisis.* [en línea] Disponible en: http://escuela.med.puc.cl/Recursos/recepidem/introductorios6.htm [Revisado 27 Noviembre 2017].

Real Academia Española. (2001). *Diccionario de la lengua española (22.a ed*.). [en línea] Disponible en: http://dle.rae.es/?w=diccionario [Revisado 27 Noviembre 2017].

Rodríguez Moguel, E. (2005). *Metodología de la investigación. Villahermosa*, Tab.: Universidad Juárez Autónoma de Tabasco.

Sapag Chain, N. y Sapag Chain, R. (2007). *Preparación y Evaluación de proyectos.* Bogotá: McGraw-Hill Interamericana.

Tecnicas-de-estudio.org. (2017). *Técnicas de Estudio*. [en línea] Disponible en: http://www.tecnicas-de-estudio.org/investigacion/investigacion38.htm [Revisado 17 Noviembre 2017].

Tamayo y Tamayo (2004). *El Proceso de la Investigación Científica.* 4ta ed. México: Limusa.

Torres Hernández, Z. y Torres Martínez, H. (2014). *Administración de proyectos.*

Universidad Pedagógica Libertador (UPEL). (1990). *Manual de Trabajos de Grado de Maestría y Tesis Doctorales.* Caracas: Autor.

Valarino, E., Yáber, G. y Cemborain, M. (2010). *Metodología de la investigación*. México: Editorial Trillas.

Vargas, Z. (2013) *Sistema de Control de Acceso y Monitoreo con la tecnología RFID para el Departamento de Sistemas de la Universidad Politécnica Salesiana Sede Guayaquil.* Trabajo Especial de Grado. Universidad Politécnica Salesiana: Guayaquil.

Veliz, A. (2007). *Cómo hacer y defender una tesis.* (7ma. ed.). Caracas: Texto

Villafranca D. (2002) *Metodología de la Investigación.* [en línea] Disponible en: https://bianneygiraldo77.wordpress.com/. [Revisado 05 Noviembre 2017].

Vivallo, A.G. (n.d.). *Formulación y Evaluación de Proyectos.* [en línea] Disponible en: https://asesoresenturismoperu.files.wordpress.com/2016/05/216-evaluacion-y-formulacion-de-proyectos.pdf [Revisado 04 Enero 2018].