

	<b>UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA</b>			
	Documento	Código	Fecha	Revisión
	<b>FORMATO HOJA DE RESUMEN PARA TRABAJO DE GRADO</b>	<b>F-AC-DBL-007</b>	<b>10-04-2012</b>	<b>A</b>
Dependencia	Aprobado		Pág.	
<b>DIVISIÓN DE BIBLIOTECA</b>	<b>SUBDIRECTOR ACADEMICO</b>		<b>i(124)</b>	

## RESUMEN – TRABAJO DE GRADO

AUTORES	<b>ALVARO JAVIER MORENO RIZO</b>
FACULTAD	<b>INGENIERIAS</b>
PLAN DE ESTUDIOS	<b>INGENIERIA DE SISTEMAS</b>
DIRECTOR	<b>ANTON GARCIA BARRETO</b>
TÍTULO DE LA TESIS	<b>DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIAS A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.</b>

### RESUMEN

(70 palabras aproximadamente)

**CON EL CRECIENTE INCREMENTO DE LAS ACTIVIDADES Y PROCESOS INTERNOS QUE SE DEBEN LLEVAR A CABO EN LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA Y TENIENDO EN CUENTA QUE EN A MANERA DE OPTIMIZAR LOS MÚLTIPLES PROCESOS Y FUNCIONES DE LOS ENCARGADOS DE LAS SALAS DE CÓMPUTO, SE VE LA NECESIDAD DE IMPLANTAR UN SISTEMA QUE CONTROLE Y MONITOREE LA ASISTENCIA Y USO DE LAS SALAS DE CÓMPUTO, UTILIZANDO ARTEFACTOS TECNOLÓGICOS QUE FACILITEN EL MANEJO DE LA INFORMACIÓN.**

### CARACTERÍSTICAS

<b>PÁGINAS: 122</b>	<b>PLANOS:</b>	<b>ILUSTRACIONES:96</b>	<b>CD-ROM: 1</b>
---------------------	----------------	-------------------------	------------------



Vía Acolsure, Sede el Algodonal, Ocaña, Colombia - Código postal: 546552  
 Línea gratuita nacional: 01 8000 121 022 - PBX: (+57) (7) 569 00 88 - Fax: Ext. 104  
 info@ufpso.edu.co - www.ufpso.edu.co

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y  
MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD  
FRANCISCO DE PAULA SANTANDER OCAÑA

AUTOR

ALVARO JAVIER MORENO RIZO

Documento presentado como requisito para el título de Ingeniero de Sistemas

DIRECTOR

ANTON GARCIA BARRETO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER

FACULTAD DE INGENIERÍAS

INGENIERÍA DE SISTEMAS

Ocaña, Colombia

Noviembre de 2018

## **DEDICATORIA**

Dedico este proyecto principalmente a Dios, por permitirme lograr esta meta tan importante para mi vida en mi formación como profesional. A mi padre Alvaro Antonio Moreno Amaya, a mi madre Yolanda Rizo, a mis hermanos Fabian Moreno Rizo, Adrian Mauricio Moreno Rizo, Juan Sebastian Moreno Rizo, a mi primo casi hermano Julio Cesar Maldonado Moreno y a M.G por todas esas cosas en las que me ayudo y estuvo conmigo en los buenos y malos momentos. Agradecer a mis familiares por ser el pilar más importante y por demostrarme siempre su cariño y apoyo incondicional y darme a entender que cada momento vivido durante todos estos años, son simplemente únicos, cada oportunidad de corregir un error, la oportunidad de que cada mañana puedo empezar de nuevo sin importar la cantidad de errores o faltas cometidas durante el día anterior y siempre empezar con el pie derecho frente a cualquier situación.

## AGRADECIMIENTOS

Principalmente a Dios por permitirme tener la fuerza y la voluntad de cumplir mi sueño y culminar mi formación como profesional para ser Ingeniero de Sistemas.

Quiero agradecer a todas esas personas que me han ayudado y apoyado en todo este tiempo que concluye con la entrega de mi proyecto de grado. A mis padres y familiares por ese empuje y esa ayuda en todo este proceso, que directa o indirectamente son parte de la culminación de este proyecto.

Al magister Anton Garcia Barreto, que con su experiencia, apoyo y dedicación me asesoro en lo necesario para el desarrollo del proyecto

A los encargados de las salas de servidores de la Universidad Francisco de Paula Santander Ocaña, Leonardo Zambrano, Arley quintero y Numael Angarita por tanto aguante y sobre todo ese apoyo incondicional que me brindaron a lo largo del desarrollo del proyecto

A mi amigo del alma Julio Cesar Maldonado por toda esa motivación que me dio para poder culminar con mi carrera

A mi hermano de otra madre Jorge Arturo torrado por enseñarme y apoyarme mucho.

Finalmente agradezco a cada una de las personas que influyeron en mi vida como universitaria, que me ayudaron a madurar como persona y profesional infinitas gracias.

## ÍNDICE

<b>INTRODUCCIÓN.....</b>	<b>1</b>
<b>CAPÍTULO 1: Título .....</b>	<b>2</b>
1.1 Planteamiento del problema .....	2
1.2 Formulación del problema .....	4
1.3 Objetivos de la investigación.....	4
1.3.1 General.....	4
1.3.1 Específicos.....	5
1.4 Justificación .....	5
1.5 Hipótesis .....	7
1.6 Delimitación .....	8
1.6.1 Geográfica.....	8
1.6.2 Temporal.....	8
1.6.3 Conceptual .....	8
1.2.1 Operativa.....	8
<b>CAPÍTULO 2: Marco Referencial.....</b>	<b>10</b>
2.1. Marco Histórico .....	10
2.1.1 Internacional .....	10
Universidad De Alicante, España. Smart University.....	10
2.1.2 Nacional.....	12
2.2 Marco Contextual .....	14
2.3 Marco Conceptual.....	16
2.3.1. Smart City.....	16
2.3.2 Smart Campus.....	18
2.3.3 Internet of Things, internet de las cosas (IoT).....	18
2.3.4 Tecnologías de la información (TIC).....	20
2.3.5 Biometría .....	20
2.3.6 Big Data.....	21
2.4. Marco Teórico .....	21

2.4.1. Sistemas Biométricos.....	21
2.4.2. Sistema De Reconocimiento De Huellas Dactilares.....	23
2.4.3 Como Funciona.....	23
2.4.4 Sistema De Registro .....	24
2.4.5 Sistema De Autenticación Y Verificación.....	25
2.4.6 Sistemas De Control Utilizado .....	27
2.4.7 Bioentry W .....	28
2.5. Marco Legal.....	29
2.5.1 LEY 1266 DE 2008 (diciembre 31).....	29
2.5.1.1 ARTÍCULO 1 .....	29
2.5.1.2 ARTÍCULO 2 .....	29
2.5.1.3 ARTÍCULO 4 PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS. ....	30
2.5.2 LEY 1341 DE 2009 (Julio 30).....	31
2.5.2.1 Artículo 1 .....	32
2.5.2.2Artículo 3.....	32
2.5.2.3 Artículo 6.....	32
2.5.3 LEY 1286 DE 2009 (Enero 23).....	33
2.5.3.1 Artículo 1 .....	33
2.5.3.2 Artículo 2.....	33
<b>CAPÍTULO 3. Diseño Metodológico .....</b>	<b>36</b>
3.1. Tipo De Investigación.....	36
3.2. Población .....	36
3.2.1. Selección de muestra .....	37
3.3. Recolección de Información .....	37
3.4. Análisis de información .....	38
<b>CAPÍTULO 4: Administración Del Proyecto .....</b>	<b>44</b>
4.1.2. Recursos Institucionales (Materiales).....	45
4.3. Recurso financiero .....	51
<b>CAPITULO 5: Resultados.....</b>	<b>53</b>

5.1. Identificar los requisitos funcionales y no funcionales que cumplan con los requisitos del proyecto. ....	53
5.2. Definir un modelo de entidad relación para la base de datos que contenga la información necesaria para su uso lógico.....	56
5.3. Implantar una aplicación que permita interactuar con los datos.....	56
5.4. Realizar el análisis de recorrido y funciones que cumplen los asistentes de sala de cómputo. ....	63
5.5. Almacenar en una base de datos los patrones biométricos de los docentes que imparten clases en las salas de cómputo de bloque A y edificio Carlos Rizo.....	66
5.6 Generar informes de cumplimiento de horario a docentes y utilización de las salas de cómputo en las horas establecidas. ....	67
5.6.1. Emparejar patrones biométricos con horarios y otorgar permisos a los docentes .....	71
5.7. Instalar el sistema de control en la sala de servidores y comunicación social de la Universidad Francisco de Paula Santander Ocaña.....	72
<b>CAPÍTULO 6: Conclusiones .....</b>	<b>79</b>
<b>Referencias Bibliográficas .....</b>	<b>81</b>
<b>Apéndice .....</b>	<b>84</b>
Apéndice A: Encuesta realizada a los docentes de la Universidad Francisco de Paula Santander Ocaña utilizando la plataforma encuesta.ufpso.edu.co. ....	84
Apéndice B: Guía de uso .....	87
Apéndice C: Conexión de componentes.....	101

## Lista de figuras

Figura 1. Organización de Smart University. Fuente ibíd. ....	10
Figura 2. Consumo eléctrico Universidad de Alicante. Fuente ibíd. ....	11
Figura 3. Árbol de departamentos. Fuente ibíd. ....	12
Figura 4. Interfaz de control de acceso personal. Fuente ibíd. ....	12
Figura 5. Infraestructura de comunicaciones de redes basada en IoT. Fuente Universidad Nacional de Bogotá, 2015 .....	13
Figura 6. Mapa Universidad Francisco de Paula Santander Ocaña, fuente, división de investigación y extensión (DIE) UFPSO, 2016.....	14
Figura 7. Bloque de aulas A y B. fuente, división de investigación y extensión (DIE) UFPSO, 2016. ....	15
Figura 8. Características de Smart City, vienna. Fuente Ranking of European medium-sized .....	16
Figura 9. Características y factores de Smart City, vienna. Fuente Ranking of European medium-sized .....	17
Figura 10. Arquitectura de capas IoT. Fuente Comité Consultivo Internacional Telegráfico y Telefónico (ITU-T). ....	19
Figura 11. Comparación de técnicas Biométricas. Fuente Dept. Of Comput. Sci., Michigan State	22
Figura 12. Detalles Huella dactilar. Fuente Universidad Militar Nueva Granada.....	23
Figura 13. Funcionamiento sistema de registro. Fuente autor del proyecto. ....	24
Figura 14. Funcionamiento de autenticación. Fuente Universidad Politécnica de Madrid .....	26
Figura 15. Funcionamiento verificación del usuario. Fuente Universidad Politécnica de Madrid...	27
Figura 16. Ciclo de Funcionamiento Bioentry. Fuente SUPREMA-BIOSTAR.....	28

Figura 17. Cálculo del tamaño de la muestra.....	37
Figura 18. Pregunta 1. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	39
Figura 19. Pregunta 2. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	40
Figura 20. Pregunta 3. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	41
Figura 21. Pregunta 4. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	42
Figura 22. Pregunta 5. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	43
Figura 23. Pregunta 6. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor .....	44
Figura 24. Sujetadores de aluminio reforzados. Fuente autor. ....	46
Figura 25. Lector biométrico BioEntry W. Fuente autor.....	47
Figura 26. Cable UPT CAT6 con topología conexión directa y conector RJ45. Fuente autor.....	47
Figura 27. Interfaz Biostar. Fuente autor software Biostar.....	48
Figura 28. Canaleta 2x2. Fuente Telnet.....	48
Figura 29. Botón del pánico. Fuente autor.....	49
Figura 30. Batería en gel. Fuente autor.....	49
Figura 31. Cable UTP categoría 6. Fuente autor .....	49
Figura 32. Conector de corriente directa AC/AC. Fuente autor .....	50
Figura 33. SK-910RBQ canal de conexión. Fuente autor .....	50
Figura 34. ST-1206-1.5AQ fuente de alimentación. Fuente autor .....	51
Figura 35. Modelo entidad relación (MER) sobre modelo de negocio. Fuente autor del proyecto..	56

Figura 36. Instalación sistema Biostar, click a setup. Fuente autor software Biostar.....	57
Figura 37. Primera pantalla de instrucción. Fuente autor software Biostar.....	58
Figura 38. Segunda pantalla de instrucción. Fuente autor software Biostar.....	58
Figura 39. Tercera pantalla de instrucción. Fuente autor software Biostar. ....	59
Figura 40. Cuarta pantalla de instrucción. Fuente autor software Biostar.....	59
Figura 41. Creando base de datos sistema Biostar. Fuente autor, software Biostar. ....	60
Figura 42. Configurando base de datos sistema Biostar. Fuente autor, software Biostar.....	61
Figura 43. Migrar información a la base de datos. Fuente autor, sistema Biostar.....	62
Figura 44. Primer recorrido, Fuente Autor, mapa UFPSO 2016. ....	63
Figura 45. Segundo recorrido, Fuente Autor, mapa UFPSO 2016. ....	64
Figura 46. Tercer recorrido, Fuente Autor, mapa UFPSO 2016.....	64
Figura 47. Cuarto recorrido, Fuente Autor, mapa UFPSO 2016. ....	65
Figura 48. Modelo de almacenamiento de datos biométricos. Fuente autor, software Biostar 1.9 ..	67
Figura 49. Informe de llegada de los usuarios. Fuente Autor, software Biostar.....	68
Figura 50. Lectores biométricos asociados al sistema de monitoreo. Fuente Autor, software Biostar. .....	69
Figura 51. Asistencia sala de servidores, Fuente autor, software Biostar.....	70
Figura 52. Prueba de funcionamiento asistencia sala de cómputo comunicación social. Fuente autor, software Biostar. ....	71
Figura 53. Sensor en estado pendiente, sala de servidores. Fuente autor. ....	72
Figura 54. Sensor apagado, sala comunicación social. Fuente autor.....	73
Figura 55. Usuario no identificado o acceso no permitido, sala de servidores. Fuente autor.....	74
Figura 56. Sensor escaneando huella, sala de servidores. Fuente autor.....	74
Figura 57. Usuario autenticado o acceso permitido, sala de servidores. Fuente autor. ....	75
Figura 58. Acceso entrada permitido. Fuente Autor.....	76

Figura 59. Botón del pánico, sala de servidores. Fuente autor. ....	76
Figura 60. Botón del pánico, sala de comunicación social. Fuente autor. ....	77
Figura 61. Botón de pánico y funcionamiento. Fuente autor. ....	77
Figura 62. Portada encuesta docente UFPSO. Fuente autor del proyecto. ....	84
Figura 63. Pregunta uno, encuesta UFPSO. Fuente autor del proyecto. ....	84
Figura 64. Pregunta dos, encuesta UFPSO. Fuente autor del proyecto. ....	85
Figura 65. Pregunta tres, encuesta UFPSO. Fuente autor del proyecto. ....	85
Figura 66. Pregunta cuatro, encuesta UFPSO. Fuente autor del proyecto. ....	86
Figura 67. Pregunta cinco, encuesta UFPSO. Fuente autor del proyecto. ....	86
Figura 68. Pregunta seis, encuesta UFPSO. Fuente autor del proyecto. ....	87
Figura 69. Conexión a escritorio remoto. Fuente autor del proyecto. ....	88
Figura 70. Ventada de contraseña y certificado de seguridad. Fuente autor del proyecto. ....	89
Figura 71. Ventada de logueo interfaz Biostar. Fuente autor del proyecto. ....	90
Figura 72. Interfaz de usuario inicial Biostar. Fuente autor del proyecto. ....	91
Figura 73. Menú de creación y configuración de puertas. Fuente autor del proyecto. ....	92
Figura 74. Asignando dispositivo a puerta lógica. Fuente autor del proyecto. ....	93
Figura 75. Asignación de dispositivo a puerta lógica. Fuente autor del proyecto. ....	94
Figura 76. Menú administración de horarios. Fuente autor. ....	95
Figura 77. Horario con su respectiva línea de tiempo. Fuente autor del proyecto. ....	96
Figura 78. Timezone creados por lapso de una hora. Fuente autor del proyecto. ....	97
Figura 79. Crear Access group. Fuente autor del proyecto. ....	98
Figura 80. Access group con nombre de usuario. Fuente autor del proyecto. ....	98
Figura 81. Agregando usuario al grupo de acceso. Fuente autor del proyecto. ....	99
Figura 82. Proceso de asignación de hora de entrada. Fuente autor del proyecto. ....	100
Figura 83. Manera en cómo se almacenan los cambios en el dispositivo. Fuente autor. ....	101

Figura 84. Cable UTP directo y switch. Fuente autor del proyecto.....	102
Figura 85. Instalación caja de suspensión lector Bioentry W. Fuente autor del proyecto. ....	103
Figura 86. Instalación lector Bioentry W. Fuente autor del proyecto.....	103
Figura 87. Instalación Electroimán. Fuente autor del proyecto. ....	104
Figura 88. Instalación soporte en puerta para barra metálica. Fuente autor del proyecto. ....	104
Figura 89. Caja protectora de implementos. Fuente autor del proyecto. ....	105
Figura 90. Distribuidor de corriente. Fuente autor del proyecto.....	105
Figura 91. Batería. Fuente autor del proyecto. ....	106
Figura 92. Electroimán. Fuente autor del proyecto.....	106
Figura 93. Controlador. Fuente autor del proyecto.....	106
Figura 94. Bioentry W. Fuente autor del proyecto. ....	107
Figura 95. Circuito de instalación de implementos. Fuente autor del proyecto.....	108
Figura 96. Circuito de control. Fuente autor del proyecto.....	109

## Lista de tablas

Tabla 1. Implementos utilizados.....	52
Tabla 2 Funciones por color del lector biométrico Bioentry W. ....	73

## INTRODUCCIÓN

Con el pasar de cada década se van desarrollando múltiples maneras que permitan un manejo útil y adecuado para la información. Las nuevas tendencias de desarrollo que utilizan la implantación de dispositivos electrónicos que almacenen datos y tengan interactividad continua con el personal de entidades donde se trabajan múltiples procesos simultáneamente ha venido en incremento, como lo es el uso de sensores que nos permitan encender una luz, abrir una puerta u otorgar una especie de seguridad sobre estas.

La ideología Smart campus, donde las universidades son tomadas como pequeñas ciudades y estas poseen un número elevado de tareas simultáneas a realizar y poco personal que pueda suplir esas exigencias, busca la forma de interactuar con la tecnología y adaptarla a las necesidades que deben suplir dichos procesos.

Al implementar una investigación descriptiva en los diferentes procesos llevados a cabo en la Universidad Francisco de Paula Santander Ocaña permitió examinar las características del problema a resolver, el cumplimiento y puntualidad de los docentes, además de representar una situación concreta se ha indicado que aspecto se debe mejorar o corregir y de qué manera puede hacerse.

Con el creciente incremento de las actividades y procesos internos que se deben llevar a cabo en la Universidad Francisco de Paula Santander Ocaña y teniendo en cuenta que en A manera de optimizar los múltiples procesos, actividades y funciones laborales de los encargados de las salas de cómputo, se ve la necesidad de implantar un sistema que controle y monitoree la asistencia y uso de las salas de cómputo, utilizando artefactos tecnológicos que faciliten el manejo de la información.

## **CAPÍTULO 1: Título**

Desarrollo e implementación de un sistema de control y monitoreo de asistencia a las salas de cómputo de la Universidad Francisco de Paula Santander Ocaña.

### **1.1 Planteamiento del problema**

Con el creciente incremento de las actividades y procesos internos que se deben llevar a cabo en la Universidad Francisco de Paula Santander Ocaña y la necesidad de abarcar dichos procesos, se ha incrementado las labores del personal para suplir el funcionamiento continuo de estas tareas que influyen con el funcionamiento de la universidad.

La manera como en la actualidad se está abordando el tema de la automatización y optimización de procesos utilizando la tecnología como medio de desarrollo, se centra en un ámbito llamado *Smart Cities* en español ciudades inteligentes, este término fue adoptado por numerosas compañías desde el año 2005 en las cuales están [Cisco, 2005], [IBM, 2009] [Siemens, 2004] para la aplicación de sistemas de información compleja, integrar la operación de la infraestructura urbana y servicios, tales como edificios, transporte, eléctrica y distribución de agua y seguridad pública.

Las universidades son tomadas como pequeñas ciudades, en este caso situamos la Universidad Francisco de Paula Santander Ocaña como un ambiente en donde se trabajan múltiples procesos en conjunto, unas actividades dependen de otras para ser analizadas y desarrolladas.

Donald Shoup (2006) afirma que: “Las grandes universidades son como pequeñas

ciudades. Disponen de instalaciones deportivas, auditorios, viviendas, centros médicos, biblioteca, oficinas, restaurantes” (p. 4.) Teniendo en cuenta que las Universidades son como pequeñas ciudades, nos centramos en un contexto llamado Smart Campus, el cual se entiende como un campus que toma y aprovecha las ventajas tecnológicas como medio de gestión integral y manejo de recursos e información de forma eficiente mediante la implementación de desarrollos tecnológicos.

La forma en cómo podemos interactuar con la tecnología, adaptarla a las necesidades que debemos suplir en los procesos y actividades a mejorar que se llevan a cabo en el campus universitario y que sea compatible y complementario con el término de Smart Campus es Internet de las cosas (IoT). Atzori, Iera y Morabito (2010) informan que: “La idea básica de este concepto es la presencia omnipresente alrededor de una gran variedad de cosas u objetos, tales como etiquetas de identificación de Radiofrecuencia (RFID), dispositivo de interfaz humana o HID (Human Interface Device), sensores, actuadores, teléfonos móviles, etc., que, a través de esquemas de direccionamiento únicos, son capaces de interactuar con los demás y cooperar con sus vecinos para alcanzar metas comunes” (Párr. 2).

En la Universidad Francisco de Paula Santander Ocaña dos de los múltiples procesos que posee el campus y consume tiempo y recurso humano es el monitoreo de los docentes sobre el cumplimiento y puntualidad de sus horas de clase, la apertura de las salas de cómputo por medio de los monitores de sala. Esta actividad se hace a diario recorriendo el campus a pie durante los lapsos de tiempo de las clases he inicios de ellas verificando que los docentes estén dando la clase y hayan llegado con puntualidad donde este no se ve tan reflejado en el proceso puesto que las últimas aulas a revisar ya tendría tiempo tardío de llegada a monitorear. Al utilizar un

desarrollo tecnológico que implemente IoT y la ideología de Smart Campus ayudaría a optimizar estos procesos utilizando la huella como identificador biométrico y el carnet institucional que posea HID (Human Interface Device) para hacer una comprobación de llegada y almacenamiento de esta con una base de datos que tenga almacenado en ella los datos necesarios para esta comprobación. Generando con esta información indicadores e informes que muestren que docente están cumpliendo a cabalidad con sus horarios de clase establecidos. Con el fin de mostrar la eficiencia de este desarrollo se deberá comprobar con la toma de datos a mano y la mostrada en los informes que generará el desarrollo tecnológico una estadística que muestre la rapidez con la que se manejan los datos y por ende la mejora del proceso en el campus.

## **1.2 Formulación del problema**

¿Qué mejora podría generar un lector biométrico-HID con cerradura electrónica que permita la apertura de las salas sin necesidad de los técnicos encargados y agilice la comprobación de la asistencia a clase de los docentes de la Universidad Francisco de Paula Santander Ocaña?

## **1.3 Objetivos de la investigación**

**1.3.1 General.** Implementar un sistema de control biométrico-HID para el control de apertura y asistencia de las salas de cómputo en la Universidad Francisco de Paula Santander Ocaña.

### **1.3.2 Específicos.**

- Identificar los requisitos funcionales y no funcionales para este tipo de herramienta tecnológica.
- Definir un modelo entidad relación para una base de datos que contenga los datos de acceso a las salas de cómputo.
- Implantar una aplicación que permita interactuar con los datos.
- Generar informes de cumplimiento de horario a docentes y utilización de las salas de cómputo en las horas establecidas.
- Instalar el sistema de control en la sala de servidores y comunicación social.

### **1.4 Justificación**

A manera de optimizar los múltiples procesos, actividades y funciones laborales de los encargados de las salas de cómputo en la Universidad Francisco de Paula Santander Ocaña, se ve la necesidad de implantar un sistema que controle y monitoree la asistencia y uso de las salas de cómputo, utilizando artefactos tecnológicos que faciliten el manejo de la información.

Aprovechando los recursos con los que cuenta la universidad, en este caso los lectores biométricos que están repartidos por diferentes puntos en el campus para el registro de estudiantes y docentes por medio de la huella dactilar donde se obtienen y almacenan los datos personales de estudiantes y docentes en una base de datos.

La eficiencia en cómo se maneje la información hace posible que los recursos con los que se cuenta una institución sean optimizados y utilizados de la mejor forma. Es importante llevar

un control de los recursos utilizados en la universidad para su óptima utilización. Laudon (1996) afirma: “Es por esto, que se vuelve indispensable contar con una solución que les permita gestionar de manera eficiente su información, de tal forma en que puedan organizar sus datos de forma estandarizada, integrar la información de las diferentes áreas y compartirla, reducir tiempos y optimizar los recursos, incluyendo cada una de las actividades que se realizan dentro de la organización.” (P. 11).

“El mayor valor de los Big Data puede producirse cuando se los combinan con otros datos corporativos. Colocándolos en un contexto más grande se puede conseguir que la calidad del conocimiento del negocio se incremente exponencialmente. Incluso la estrategia del Big Data dentro de la estrategia global de la compañía es mucho más rentable que tener una estrategia independiente.”

(Aguilar, 2016, p. 16).

Brindar acceso automatizado a las salas de cómputo a los docentes, almacenando su hora de llegada y autenticando la información con la base de datos para un control continuo generando reportes de horas cumplidas u horas tardías (llegar puntual o no). Con la implementación de este proyecto se puede hacer un análisis a la información, donde al tomar los datos se pueden realizar indicadores de asistencia y puntualidad, la utilización de las salas de cómputo en las horas establecidas por los docentes correspondientes, al analizar estos datos saber si se está dando un uso y desempeño óptimo a los recursos que se cuentan en las salas de cómputo. Mejorar las funciones que deben suplir los monitores de salas y optimizar su labor haciendo automática la toma de datos importante para la universidad.

### **1.5 Hipótesis**

La información obtenida por la base de datos será más confiable que la tomada a pie por los monitores de salas, esta puede ser procesada para generar indicadores de asistencia y puntualidad.

las clases inician después de la hora establecida por el tiempo que les toma a los encargados de las salas ir a abrir las diferentes aulas, donde esta actividad se ve afectada cuando llegan múltiples docentes a la vez solicitando sus aulas de clase afectando el tiempo de trabajo que poseen los docentes para impartir las clases. La apertura automatizada en tiempo real con lector de huella disminuirá el tiempo desperdiciado en las clases.

## **1.6 Delimitación**

**1.6.1 Geográfica.** El sistema de control para la apertura de aulas y monitoreo de la asistencia a las clases por parte de los docentes se sitúa en la sala de cómputo de comunicación social del bloque B, edificio Carlos Rizo en su tercer piso y a la sala de servidores en la Universidad Francisco de Paula Santander Ocaña.

**1.6.2 Temporal.** El sistema será probado durante un mes, donde cinco días hábiles se estará generando un informe general del cumplimiento de los horarios, al finalizar la jornada diaria de clases para un reporte del funcionamiento y cada hora para hacer pruebas y correcciones.

**1.6.3 Conceptual.** Se debe tener en cuenta que se nombraran conceptos como metodologías ágiles, estudios correlacionales, lector biométrico, software, hardware, confiabilidad de la información, base de datos, big data, ingeniería de software, Smart Campus, Smart Grids, Smart City, internet de las cosas (IoT), cloud data, human interface device (HID).

**1.6.4 Operativa.** El sistema brindará al docente acceso automático a la salas de cómputo donde impartirá la clase, este acceso se obtiene con el uso de la identificación biométrica de su huella dactilar, por medio de la conexión que nos ofrece Internet de las cosas (IoT) podemos realizar la autenticación del usuario y almacenar su hora de llegada donde por medio de esta información y aplicando la filosofía de Smart Campus se comprobará en una base de datos que aula debe abrirse dependiendo del horario que se le haya asignado a al docente, con estos datos obtenidos se harán informes de manera semanal, diaria y por horas para poder tener un control sobre este proceso.



## CAPÍTULO 2: Marco Referencial

### 2.1 Marco Histórico

**2.1.1 Internacional, Universidad De Alicante, España. Smart University.** El proyecto Smart University engloba las principales áreas o ámbitos integradores de cualquier Smart City: Smart Economy, Smart Mobility, Smart Environment, Smart People, Smart Living y Smart Government , ayudando a desarrollar Smart Communities, Smart Campus o Smart Cities de nueva creación desde cero o actualizando las existentes, es un modelo de universidad que mejora la calidad de vida haciendo uso intensivo, global, eficiente y sostenible de las TI para interconectar todos los actores y servicios que se ven involucrados en la universidad.

Sus funciones a partir de lo dicho por (Universidad de alicante 2015) se dividen en:

- Ciudadanos – *Smart People*
- Administración y gobierno – *Smart Government*
- Entorno y eficiencia – *Smart Environment*
- Movilidad - *Smart Mobility*
- Economía – *Smart Economy*
- Forma de vida – *Smart Living*

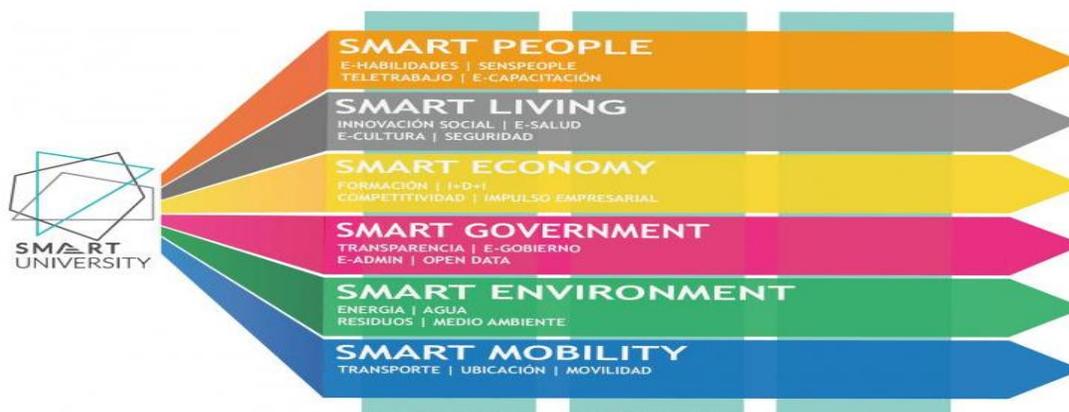


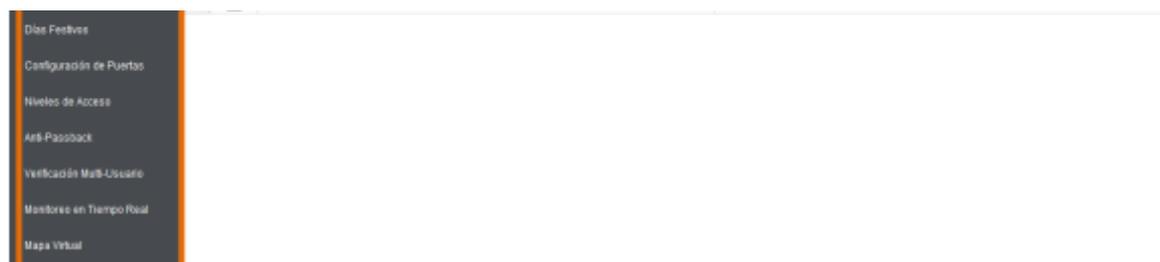
Figura 1. Organización de Smart University. Fuente ibíd.



**2.1.2 Nacional. Universidad Distrital Francisco José de caldas, Bogotá. Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad distrital Francisco José de Caldas mediante el uso de torniquetes controlados por carnet con tecnología nfc y lector biométrico de huella dactilar. (Meneses & García, 2016).** El sistema permite un control de acceso por medio de autenticación por huella o carnet que posea lector NFC para el ingreso de los funcionarios y la comunidad estudiantil a la sede de ingeniería para generar un mayor flujo de entrada y un nivel de seguridad óptimo teniendo control a la hora de verificar el personal que ingresa.



**Figura 3. Árbol de departamentos. Fuente ibíd.**



**Figura 4. Interfaz de control de acceso personal. Fuente ibíd.**

Universidad Nacional de Colombia, Bogotá. Implementación de un sistema de seguridad para las comunicaciones en medidores inteligentes de baja tensión en Smart Grids. (Leguizamón, 2015) Presenta la integración de un sistema de seguridad basado en Iot, para el manejo de la comunicación de medidores inteligentes una red inteligente con mejor administración de la energía; implementando estas tecnologías se espera reducir significativamente los tiempos de lectura en las mediciones, los reportes de fallas y los cambios en la red. Logrando la integración del hardware y software con un sistema embebido para la iteración entre estas.

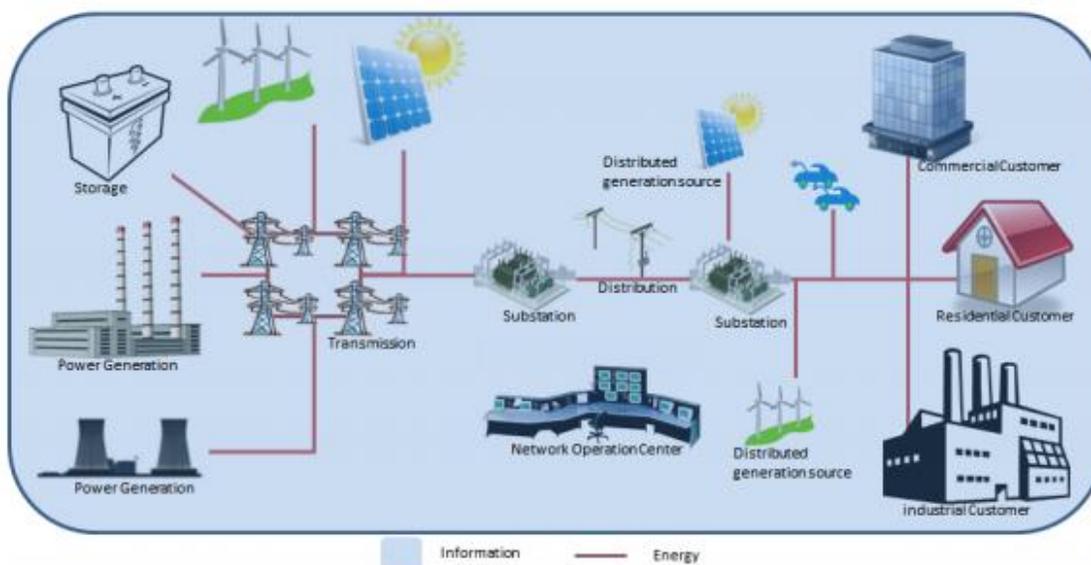


Figura 5. Infraestructura de comunicaciones de redes basada en IoT. Fuente Universidad Nacional de Bogotá,

## 2.2 Marco Contextual

Las salas de cómputo de la Universidad Francisco de Paula Santander Ocaña son de uso continuo debido a la intensidad horaria que se asignan, con el incremento continuo de los estudiantes ingresados a las diferentes carreras se debe tener un control más adecuado a la hora de entregar a los docentes las salas de cómputo a utilizar. Los encargados de las aulas deben dar la autorización de ingreso, muchas veces esta tarea se ve retrasada por el continuo monitoreo que deben hacer a la asistencia de los docentes. Por ende un acceso automatizado a las salas es necesario.

Las salas de cómputo situadas en el edificio Carlos Rizo, donde se encuentran las salas específicas, el bloque de aulas situadas cerca del laboratorio de redes y telecomunicaciones, llamados salas de cómputo (SC). En el siguiente esquema se puede mostrar el campus universitario.

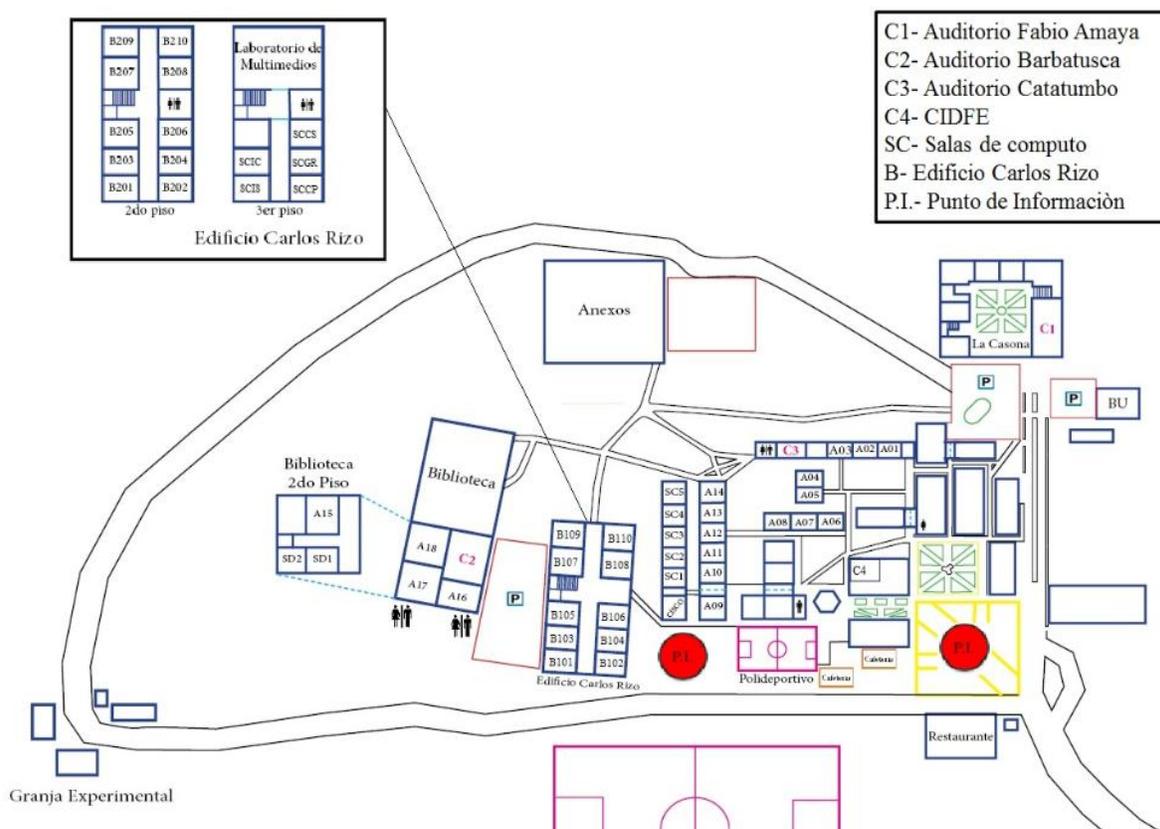


Figura 6. Mapa Universidad Francisco de Paula Santander Ocaña, fuente, división de investigación y extensión (DIE) UFPSO, 2016.

Donde podemos apreciar las salas de Cómputo del bloque A y B. donde el bloque A se identifican como SC (sala de cómputo) y el bloque B con las siglas de las salas específicas como SCIS (sala de computo Ingeniería de Sistemas).

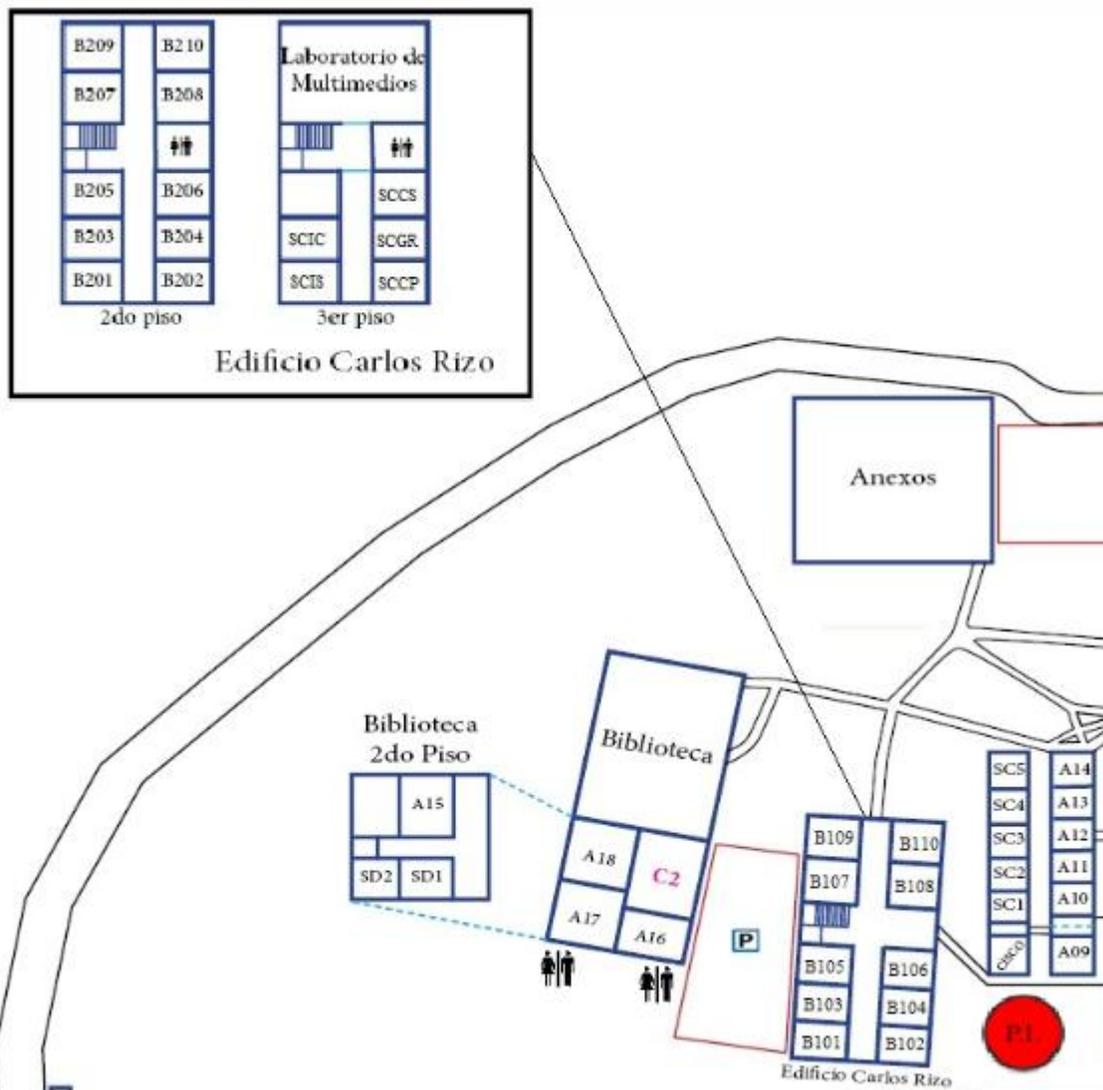


Figura 7. Bloque de aulas A y B. fuente, división de investigación y extensión (DIE) UFPSO, 2016.

## 2.3 Marco Conceptual

**2.3.1. Smart City.** “Se define Smart city (en castellano Ciudad inteligente) como aquella ciudad que usa las tecnologías de la información y las comunicaciones para hacer que tanto su infraestructura crítica, como sus componentes y servicios públicos ofrecidos sean más interactivos, eficientes y los ciudadanos puedan ser más conscientes de ellos”. (Telefónica, F, 2011, P. 13)

“En su origen, el componente fundamental de las Smart Cities fue el energético; es decir, la aplicación de la tecnología a la sostenibilidad energética de la ciudad. Sin embargo, el concepto ha ido ampliándose hasta incluir en algunos casos el empleo de las TIC en el Gobierno de la ciudad o en la prestación de servicios públicos como la Sanidad”. (AMETIC, 2013, P. 27)

Según Giffinger, R. (2007, P. 11). las funciones de Smart city en las ciudades se pueden caracterizar en:

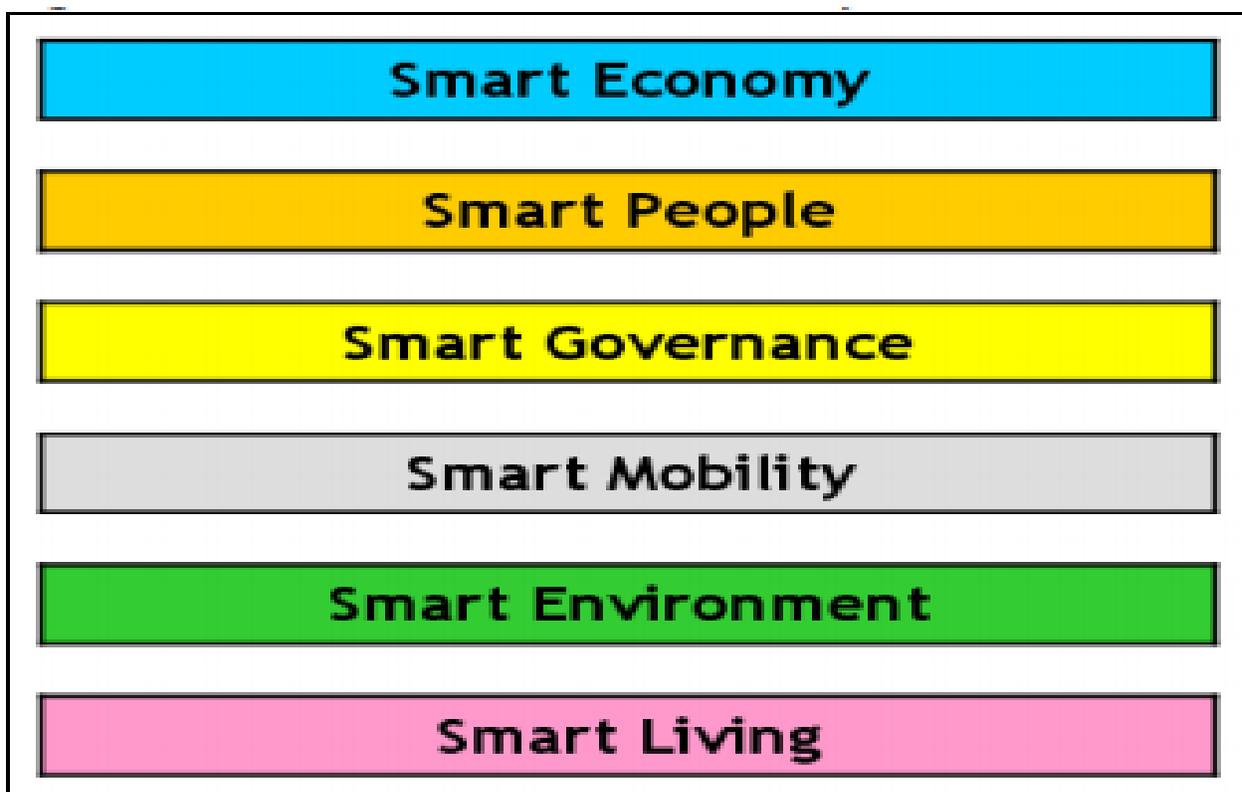


Figura 8. Características de Smart City, vienna. Fuente Ranking of European medium-sized

La manera en cómo los diferentes aspectos que constituyen una ciudad inteligente depende más de las personas que de la tecnología, la interconectividad y el análisis de datos es importante para poder desarrollar la parte innovadora pero para poder acoplar la tecnología a la vida cotidiana las personas deben poseer ciertos criterios. Según Enerlys, Ernst & Young (2012) El éxito reside en la cooperación entre las autoridades y todos los agentes económicos y sociales, con una implicación crucial de los ciudadanos. De esta manera, las teorías de la sostenibilidad se podrán convertir en realidades. (P. 18)

<p><b>SMART ECONOMY (Competitiveness)</b></p> <ul style="list-style-type: none"> <li>▪ Innovative spirit</li> <li>▪ Entrepreneurship</li> <li>▪ Economic image &amp; trademarks</li> <li>▪ Productivity</li> <li>▪ Flexibility of labour market</li> <li>▪ International embeddedness</li> <li>▪ <i>Ability to transform</i></li> </ul>	<p><b>SMART PEOPLE (Social and Human Capital)</b></p> <ul style="list-style-type: none"> <li>▪ Level of qualification</li> <li>▪ Affinity to life long learning</li> <li>▪ Social and ethnic plurality</li> <li>▪ Flexibility</li> <li>▪ Creativity</li> <li>▪ Cosmopolitanism/Open-mindedness</li> <li>▪ Participation in public life</li> </ul>
<p><b>SMART GOVERNANCE (Participation)</b></p> <ul style="list-style-type: none"> <li>▪ Participation in decision-making</li> <li>▪ Public and social services</li> <li>▪ Transparent governance</li> <li>▪ <i>Political strategies &amp; perspectives</i></li> </ul>	<p><b>SMART MOBILITY (Transport and ICT)</b></p> <ul style="list-style-type: none"> <li>▪ Local accessibility</li> <li>▪ (Inter-)national accessibility</li> <li>▪ Availability of ICT-infrastructure</li> <li>▪ Sustainable, innovative and safe transport systems</li> </ul>
<p><b>SMART ENVIRONMENT (Natural resources)</b></p> <ul style="list-style-type: none"> <li>▪ Attractivity of natural conditions</li> <li>▪ Pollution</li> <li>▪ Environmental protection</li> <li>▪ Sustainable resource management</li> </ul>	<p><b>SMART LIVING (Quality of life)</b></p> <ul style="list-style-type: none"> <li>▪ Cultural facilities</li> <li>▪ Health conditions</li> <li>▪ Individual safety</li> <li>▪ Housing quality</li> <li>▪ Education facilities</li> <li>▪ Touristic attractivity</li> <li>▪ Social cohesion</li> </ul>

Figura 9. Características y factores de Smart City, vienna. Fuente Ranking of European medium-sized

**2.3.2 Smart Campus.** Es un campus inteligente, capaz de aprovechar los datos que produce en su funcionamiento diario para generar información nueva que le permita mejorar su gestión y ser más sostenible, más competitivo y ofrecer mejor calidad de servicio, es la versión más pequeña de Smart City se toman las funciones y la operatividad de los aparatos tecnológicos y se conectan entre sí para un mejor usos de los recursos. (Figueroa, Acevedo Pinedo, 2017, p39).

Para llamarse Smart campus se deben mezclar dos términos un tanto similares los cuales son, Internet de las cosas (Iot) y tecnologías de la información.

**2.3.3 Internet of Things, internet de las cosas (IoT).** Partiendo de una compleja red que conecta millones de dispositivos y personas en una infraestructura de multitecnología, multiprotocolo y multiplataforma, la visión principal de Internet de las cosas (IoT) es la creación de un mundo inteligente donde lo real, lo digital y lo virtual convergen para crear un entorno inteligente que proporcione más inteligencia a la energía, la salud, el transporte, las ciudades, la industria, los edificios y muchas otras áreas de la vida diaria.(Zennaro, 2015, P. 2).

Internet de las cosas (IoT) comprende dispositivos que funcionan como sensores, actuadores, Controladores y registradores de actividad. Estos dispositivos suelen interactuar con software funcionando en otro lugar de la red, como en un teléfono móvil, un propósito general (computadora portátil), una máquina en la Internet pública (la nube), O una combinación de estos. Los dispositivos IoT suelen funcionar de forma autónoma, sin Intervención humana.

El término "IoT" tiene alcance potencialmente amplio. IoT puede referirse a despliegues en hogares, Negocios, instalaciones de manufactura, industrias de transporte y otros lugares. Así,

IoT puede referirse a mucho más que simplemente dispositivos orientados al consumidor.

(BITAD, 2016, P. 2)

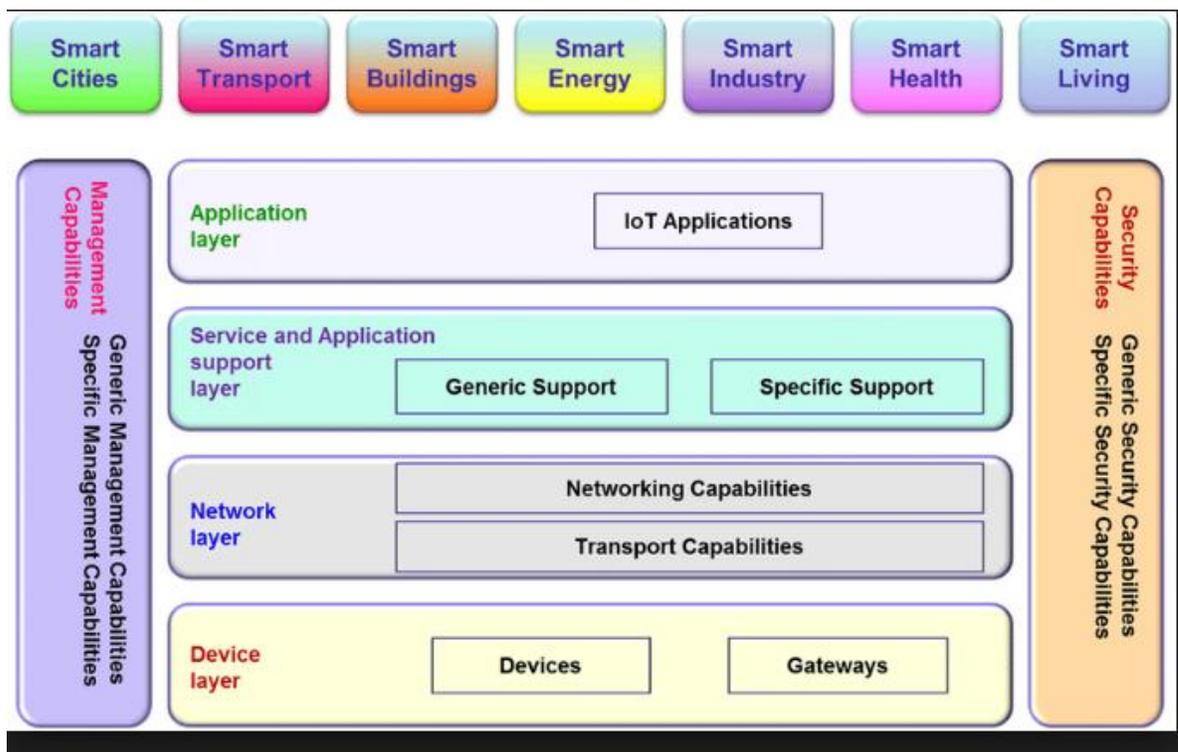


Figura 10. Arquitectura de capas IoT. Fuente Comité Consultivo Internacional Telegráfico y Telefónico (ITU-T).

IoT puede concebirse como una estructura que ofrece servicios de aplicación habilitados por varias tecnologías.

**2.3.4 Tecnologías de la información (TIC).** Las Tecnologías de la información y la comunicación tienen una especial importancia porque afectan a prácticamente todos los ámbitos de la vida de las personas, desde las formas y prácticas de organización social, hasta la manera de comprender el mundo, organizar esa comprensión y transmitirla a otras personas. (Coll, 2008, P. 22)

La interactividad de espacios, medios, recursos y personas; su complejidad; la tendencia progresiva a la automatización; la globalización; la potenciación del ritmo del cambio como elemento y valor en sí mismo; la inmediatez de los productos y resultados; y la que aquí a nosotros más nos interese, el girar alrededor de las denominadas nuevas tecnologías de la información y comunicación. (Almenara, 1998, P. 2)

**2.3.5 Biometría.** La biometría es una ciencia que analiza las distancias y posiciones entre las partes del cuerpo para poder identificar o clasificar a las personas. (Serratosa, 2008, P. 8)

El reconocimiento biométrico responde a un sistema automático basado en la inteligencia artificial y el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo, conocidas como autenticadores. Como principales autenticadores podemos mencionar las huellas dactilares, la geometría de la mano, la cara, el termograma facial, el iris, la retina, la voz, el estilo de escritura...etc.(Duro, 2001, P. 1)

**2.3.6 Big Data.** Big Data describe una estrategia holística de gestión de la información que incluye e integra muchos nuevos tipos de Datos y gestión de datos junto con los datos tradicionales. Si bien muchas de las técnicas para procesar y analizar estos Los tipos de datos han existido desde hace algún tiempo, ha sido la proliferación masiva de datos y la computación de menor costo.

Modelos que han fomentado una adopción más amplia. Además, Big Data ha popularizado dos sistemas de almacenamiento y Tecnologías de procesamiento: Apache Hadoop y la base de datos NoSQL. (ORACLE, 2016 P. 4)

## **2.4. Marco Teórico**

**2.4.1. Sistemas Biométricos.** Los sistemas biométricos están hechos específicamente para la identificación, comparación y comprobación de ciertos aspectos del cuerpo humano para verificar a quién pertenece, utilizando distintas partes ya sean por medio del iris, huella dactilar o reconocimiento facial. Benedetto, M. G., & Alvez, C. E. (2011) afirman que: “Los sistemas biométricos, en general, están compuestos de dispositivos para recopilar datos en formato digital; algoritmos de procesamiento de los datos recolectados, que efectúan control de calidad de los datos y van conformando las plantillas biométricas.”(Párr. 5) donde las plantillas biométricas son las que se almacenan en la base de datos.

Borja, C. T. afirma que: “Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad”. (P. 4) Es decir a base de la

información el sistema fundamenta sus acciones, decisiones y funcionalidades mediante una característica personal que pueda ser conocida y verificada de manera automatizada.

Según B. Miller, 1994(P. 22) las características y requerimientos que deben suplir los sistemas biométricos son:

- Universalidad, que significa que cada persona debe tener esas características.
- Unicidad, dos personas no deben ser la misma en términos de características específicas.
- Permanencia, indica que las características deben ser invariantes con el tiempo.
- Colectividad, que indica que las características pueden ser medibles cuantitativamente

Actualmente existen muchos tipos de identificación biométrica Pankanti, S., & Bolle, R. (1997) afirman que: “existen nueve técnicas biométricas fundamentales que son ampliamente usadas o que se están investigando; las técnicas se basan en: rostro, huella dactilar, geometría de la mano, venas de la mano, iris, patrón renal, firma, voz, y termograma facial”

<b>Técnicas Biométricas</b>	<b>Universalidad</b>	<b>Unicidad</b>	<b>Permanencia</b>	<b>Colectibilidad</b>
Rostro	Alta	Baja	Media	Alta
Huella Dactilar	Media	Alta	Alta	Media
Geometría de la mano	Media	Media	Media	Alta
Venas de la mano	Media	Media	Media	Media
Iris	Alta	Alta	Alta	Media
Exploración de retina	Alta	Alta	Media	Baja
Firma	Baja	Baja	Baja	Alta
Voz	Media	Baja	Baja	Media
Termograma facial	Alta	Alta	Baja	Alta

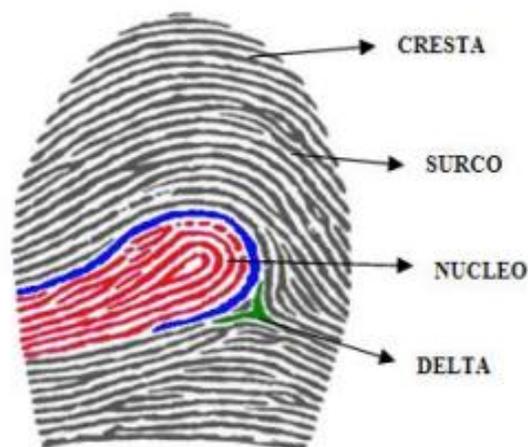
Figura 11. Comparación de técnicas Biométricas. Fuente Dept. Of Comput. Sci., Michigan State

Al analizar los diferentes tipos de reconocimientos biométricos que se encuentran actualmente, lo que más se adapta a las necesidades del proyecto y a los recursos que cuenta la universidad son los sistemas de reconocimiento de huellas dactilares.

## 2.4.2. Sistema De Reconocimiento De Huellas Dactilares

El sistema de reconocimiento por huella dactilar es el más utilizado para la comprobación y autenticación de los datos de una persona, solo necesita sus manos o en muchos casos solo un dedo. La huella dactilar es uno de los aspectos que con el pasar del tiempo no cambia ni se altera. Según Galton, F. (1904) “las huellas dactilares nunca cambian, haciéndolas instrumentos útiles para la identificación personal.”

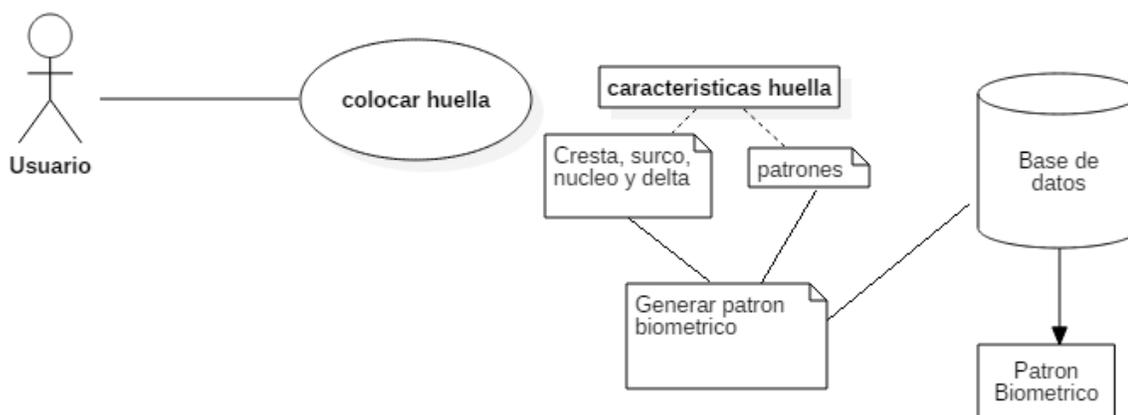
**2.4.3 Como Funciona.** Según VARGAS, A. M., & DE LA SEGURIDAD, E. E. A. “La huella dactilar en su estructura como método de identificación Está formada por crestas papilares y surcos interpapilares están localizados en la piel los cuales forman los dibujos en la falange distal de los dedos de las manos, lo que hace que se formen puntos característicos, un núcleo y uno o varios deltas, con el fin de llevar a cabo la verificación de identidad” (P. 12).



**Figura 12. Detalles Huella dactilar. Fuente Universidad Militar Nueva Granada**

La necesidad de poder analizar toda la información de los usuarios en la que estén almacenados los patrones biométricos de cada persona hace referencia a la utilización de una base de datos, el sistema tiene una tarea importante por cumplir, la inscripción o registro de cada usuario donde se genera el patrón o modelo biométrico de la huella dactilar.

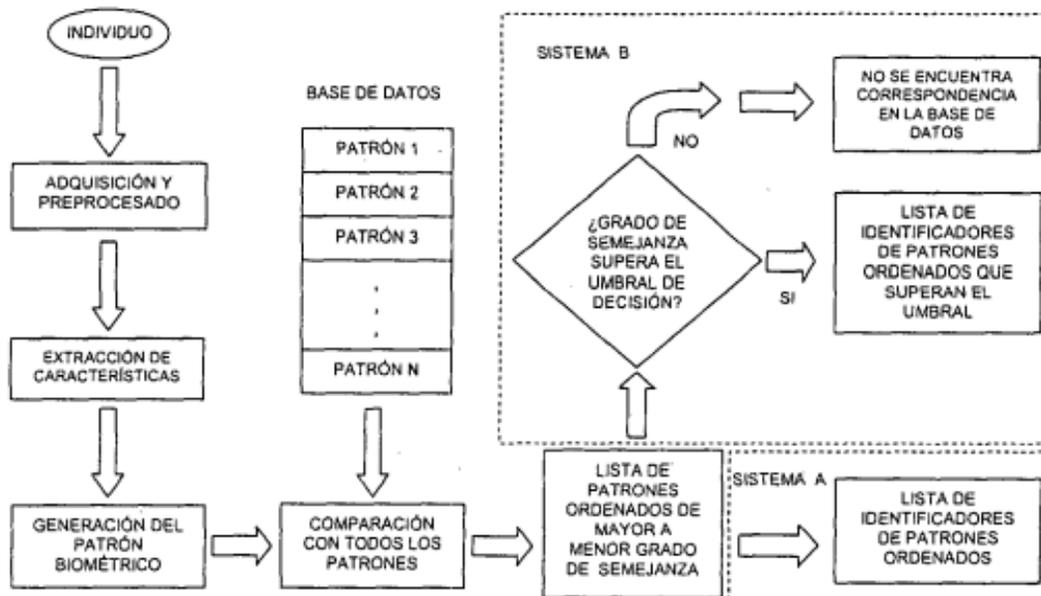
**2.4.4 Sistema De Registro.** En esta actividad o función se inscriben los patrones biométricos de los usuarios del sistema, ya que este no podrá comprobar sin los patrones de los usuarios almacenados, es posible eliminar o dar privilegios a los usuarios ya registrados. El sistema de registro obtiene la señal biométrica, los patrones y características de la huella dactilar del usuario, en el siguiente esquema se resume el ciclo que cumplen los sistemas de almacenamiento de huella dactilar.



**Figura 13. Funcionamiento sistema de registro. Fuente autor del proyecto.**

**2.4.5 Sistema De Autenticación Y Verificación.** En esta función el sistema debe comparar y decidir qué características son iguales a las del patrón que el usuario ingresa al sistema para poder acceder a él. El usuario al ingresar la huella no está pidiendo acceso, está pidiendo al sistema ser identificado para que este le conceda el acceso. El sistema debe comparar el patrón que el usuario está ingresando con los patrones biométricos almacenados en la base de datos. Según Zorita, D. S., & García, J. O. (2003) este proceso puede efectuarse de dos maneras:

- Identificación en conjunto cerrado: como resultado del proceso de comparación el sistema asigna la identidad demandada a uno de los posibles usuarios del sistema, y devuelve, por tanto, el identificador del patrón de la base de datos que obtiene mayor semejanza en la comparación
- Identificación en conjunto abierto: en este caso, el sistema contempla la posibilidad de que el individuo que demanda ser identificado pueda no ser usuario del sistema, y por tanto, como resultado del proceso, se puede producir también una no correspondencia con ninguno de los patrones almacenados en la base de datos.



**Figura 14. Funcionamiento de autenticación. Fuente Universidad Politécnica de Madrid**

Para la verificación del usuario el sistema debe constatar si la identidad solicitada por el usuario es falsa o verdadera. el sistema al obtener el patrón biométrico del individuo que solicita la autenticación, al compararla con el patrón biométrico almacenado en la base de datos y la semejanza de las características de la huella supera un determinado porcentaje de decisión se le da veracidad a la información y por ende la autenticación del usuario que desea ingresar al sistema, si la información no cumple con los criterios establecidos se toma como falsa y por ende el sistema no permite el ingreso del individuo.

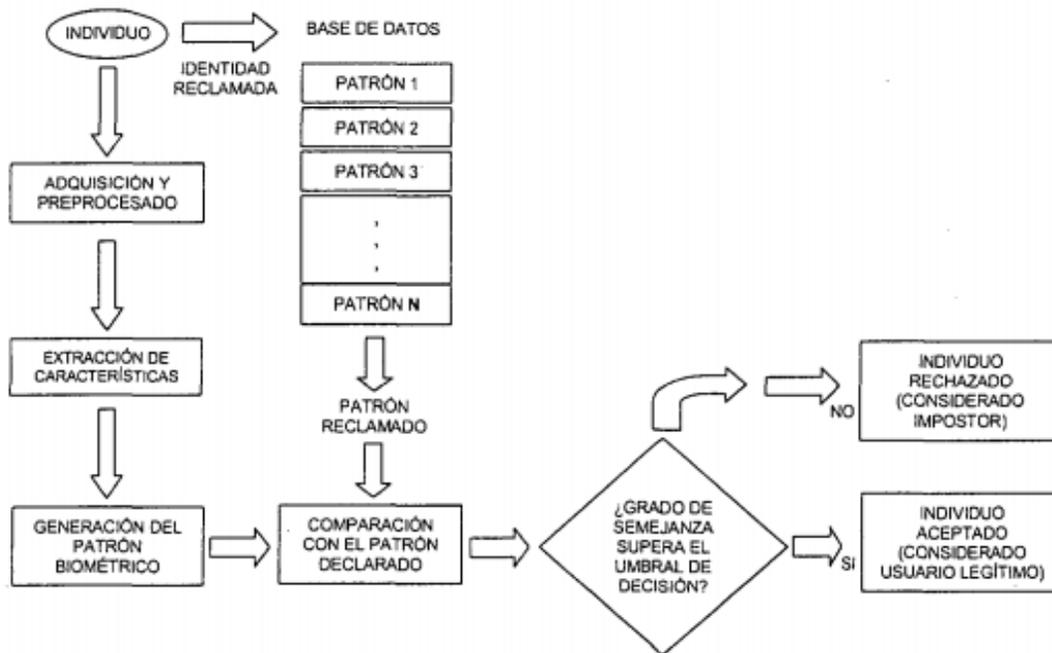


Figura 15. Funcionamiento verificación del usuario. Fuente Universidad Politécnica de Madrid

**2.4.6 Sistemas De Control Utilizado.** Para este proyecto dado los continuos cambios que se hacen referentes a la tecnología de lector de huellas y al continuo incremento de las necesidades de este se utilizara la tecnología desarrollada por la empresa BIOSTAR SUPREMA, su dispositivo BIOENTRY W.

**2.4.7 Bioentry W.** BioEntry W es un robusto dispositivo biométrico de huella, de control de acceso y alto desempeño que ofrece protección triple contra polvo, agua y vandalismo. BioEntry W también incorpora capacidades Power-over-Ethernet (PoE), haciéndolo la solución ideal para una fácil instalación. Es ideal para aplicaciones que requieren tecnología de huella dactilar y puede ser usado en diferentes entornos de instalación.

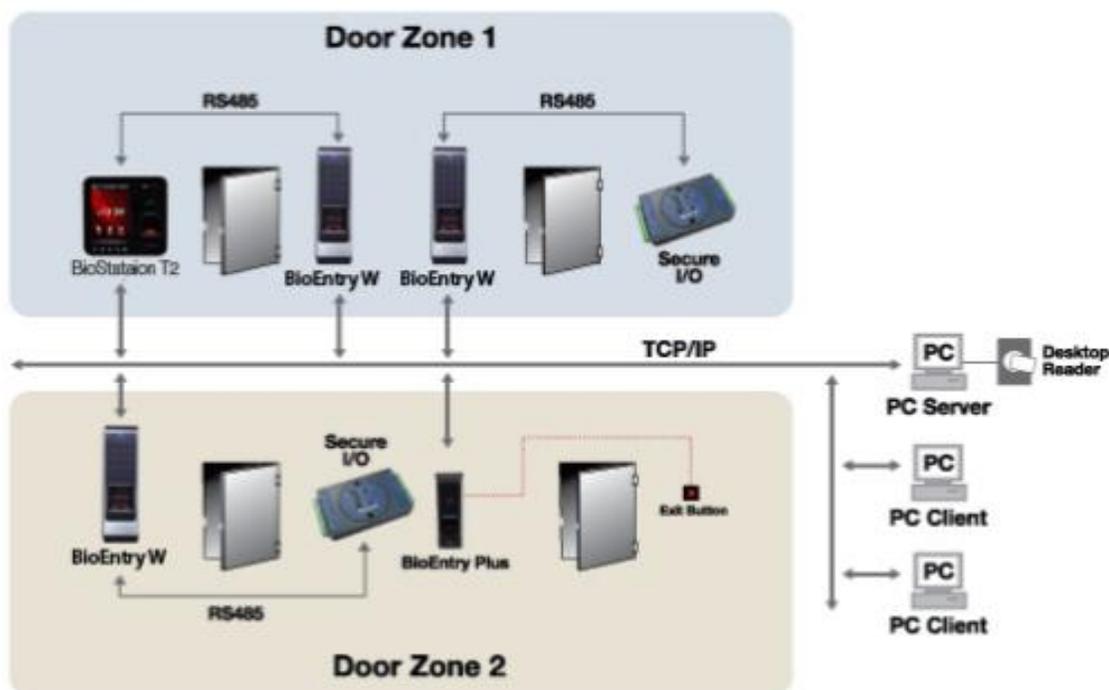


Figura 16. Ciclo de Funcionamiento Bioentry. Fuente SUPREMA-BIOSTAR

## **2.5. Marco Legal**

**2.5.1 LEY 1266 DE 2008 (diciembre 31).** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Congreso de la república, 2008)

**2.5.1.1 ARTÍCULO 1.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales

**2.5.1.2 ARTÍCULO 2.** La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada.

Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa

**2.5.1.3 ARTÍCULO 4 PRINCIPIOS DE LA ADMINISTRACIÓN DE DATOS.** En el desarrollo, interpretación y aplicación de la presente ley, se tendrán en cuenta, de manera armónica e integral, los principios que a continuación se establecen:

a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error;

b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto;

c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos.

Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley;

d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos;

e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como

son el hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables;

f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;

g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

**2.5.2 LEY 1341 DE 2009 (Julio 30).** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones. (MINTIC, 2009)

**2.5.2.1 Artículo 1.** La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.

**2.5.2.2 Artículo 3.** Sociedad de la información y del conocimiento. El Estado reconoce que el acceso y uso de las Tecnologías de la Información y las Comunicaciones, el despliegue y uso eficiente de la infraestructura, el desarrollo de contenidos y aplicaciones, la protección a los usuarios, la formación de talento humano en estas tecnologías y su carácter transversal, son pilares para la consolidación de las sociedades de la información y del conocimiento.

**2.5.2.3 Artículo 6.** Definición de TIC. Las Tecnologías de la Información y las Comunicaciones (en adelante TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

**2.5.3 LEY 1286 DE 2009 (Enero 23).** Por la cual se modifica la Ley 29 de 1990, se transforma a Colciencias en Departamento Administrativo, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación en Colombia y se dictan otras disposiciones.  
(MINEEDUCACION, 2009)

**2.5.3.1 Artículo 1.** El objetivo general de la presente ley es fortalecer el Sistema Nacional de Ciencia y Tecnología y a Colciencias para lograr un modelo productivo sustentado en la ciencia, la tecnología y la innovación, para darle valor agregado a los productos y servicios de nuestra economía y propiciar el desarrollo productivo y una nueva industria nacional.

**2.5.3.2 Artículo 2.** Objetivos específicos. Por medio de la presente Ley se desarrollan los derechos de los ciudadanos y los deberes del Estado en materia del desarrollo del conocimiento científico, del desarrollo tecnológico y de la innovación, se consolidan los avances hechos por la Ley 29 de 1990, mediante los siguientes objetivos específicos:

1. Fortalecer una cultura basada en la generación, la apropiación y la divulgación del conocimiento y la investigación científica, el desarrollo tecnológico, la innovación y el aprendizaje permanentes.
2. Definir las bases para la formulación de un Plan Nacional de Ciencia, Tecnología e Innovación.
3. Incorporar la ciencia, la tecnología y la innovación, como ejes transversales de la política económica y social del país.
4. Transformar el Instituto Colombiano para el Desarrollo de la Ciencia y la Tecnología "Francisco José de Caldas" -Colciencias-, actualmente establecimiento público del orden

nacional, en el Departamento Administrativo de Ciencia, Tecnología e Innovación que se denominará Colciencias.

5. Transformar el Sistema Nacional de Ciencia Tecnología en el Sistema Nacional de Ciencia, Tecnología e Innovación -SNCTI-.

6. Fortalecer la incidencia del SNCTI en el entorno social y económico, regional e internacional, para desarrollar los sectores productivo, económico, social y ambiental de Colombia, a través de la formación de ciudadanos integrales, creativos, críticos, proactivos e innovadores, capaces de tomar decisiones trascendentales que promuevan el emprendimiento y la creación de empresas y que influyan constructivamente en el desarrollo económico, cultural y social.

7. Definir las instancias e instrumentos administrativos y financieros por medio de los cuales se promueve la destinación de recursos públicos y privados al fomento de la Ciencia, Tecnología e Innovación.

8. Articular y optimizar las instancias de liderazgo, coordinación y ejecución del Gobierno y la participación de los diferentes actores de la política de Ciencia, Tecnología e Innovación.

9. Fortalecer el desarrollo regional a través de políticas integrales de descentralización e internacionalización de las actividades científicas, tecnológicas y de innovación, de acuerdo con las dinámicas internacionales.

10. Orientar el fomento de actividades científicas, tecnológicas y de innovación hacia el mejoramiento de la competitividad en el marco del Sistema Nacional de Competitividad.

11. Establecer disposiciones generales que conlleven al fortalecimiento del conocimiento científico y el desarrollo de la innovación para el efectivo cumplimiento de la presente ley.



## **CAPÍTULO 3. Diseño Metodológico**

### **3.1. Tipo De Investigación**

Para este proyecto se ve la necesidad de implementar una investigación descriptiva ya que nos permite examinar las características del problema a resolver, además representa una situación concreta identificando así los rasgos más sobresalientes y característicos sobre el fenómeno o la situación concreta indicando que aspecto se debe mejorar o corregir.

Supo, J. (2012) afirma “Los estudios descriptivos buscan desarrollar una imagen o fiel representación (descripción) del fenómeno estudiado a partir de sus características. Describir en este caso es sinónimo de medir. Miden variables o conceptos con el fin de especificar las propiedades importantes de comunidades, personas, grupos o fenómeno bajo análisis. El énfasis está en el estudio independiente de cada característica, es posible que de alguna manera se integren las mediciones de dos o más características con el fin de determinar cómo es o cómo se manifiesta el fenómeno. Pero en ningún momento se pretende establecer la forma de relación entre estas características. En algunos casos los resultados pueden ser usados para predecir” (párr. 8)

### **3.2. Población**

La población a la cual se le realizará el estudio es a los 152 docentes que poseen clases en las salas de cómputo del bloque A y el bloque B edificio Carlos Rizo.

### 3.2.1. Selección de muestra

$$\frac{\frac{z^2 \times p(1-p)}{e^2}}{1 + \left(\frac{z^2 \times p(1-p)}{e^2 N}\right)}$$

**Figura 17. Cálculo del tamaño de la muestra**

Dónde:

N: Tamaño de la población valor: 152

Z: Nivel de confianza valor: 0.90

P: Probabilidad de éxito o proporción esperada valor: 0.5

Q: Probabilidad de fracaso (1 - p) valor: 0.5

D: precisión (error máximo admisible en términos de proporción) valor: 0.25

El tamaño de la muestra para este proyecto es de 108 personas

### 3.3. Recolección de Información

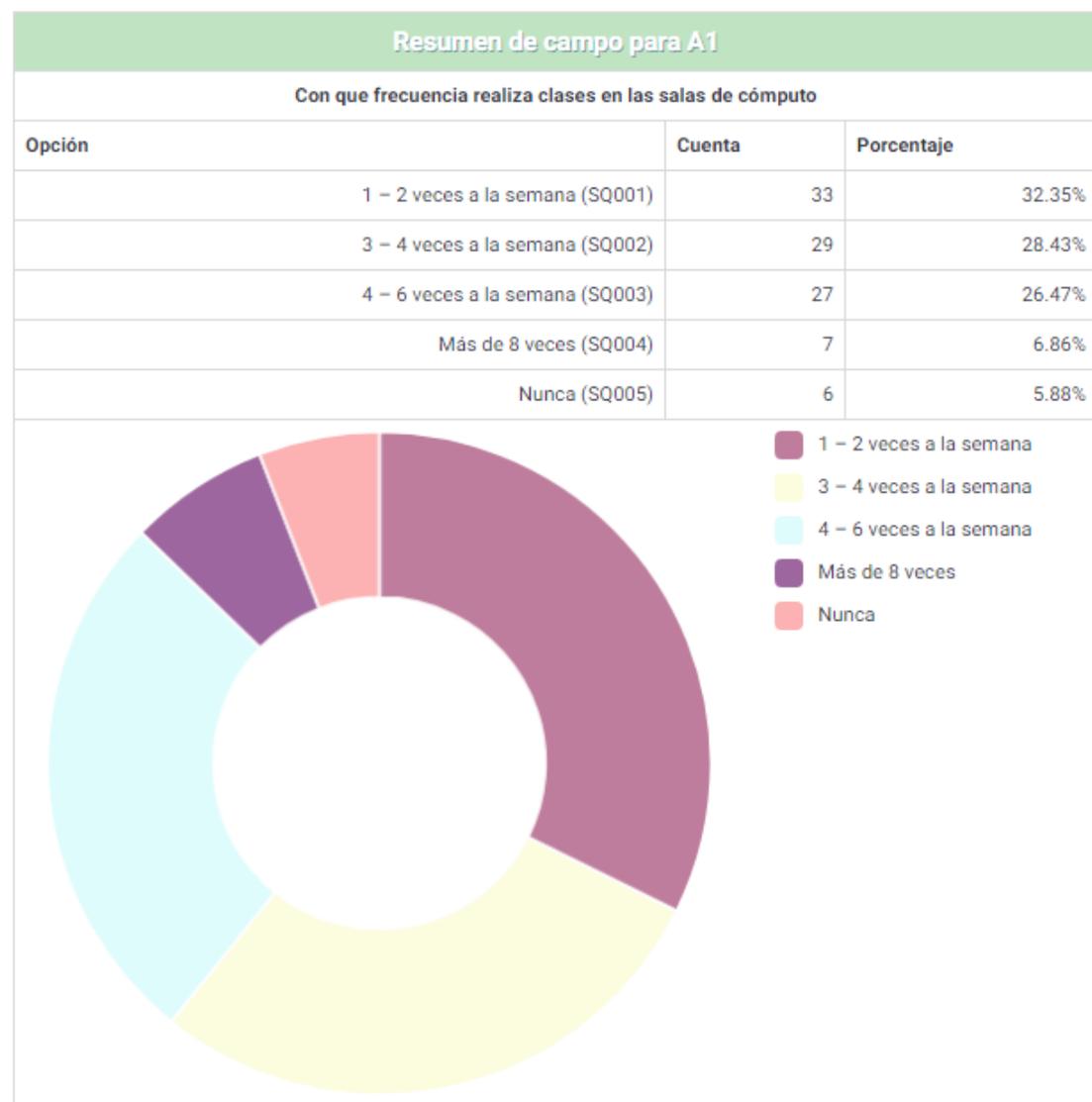
Al recolectar la información se utilizara la encuesta, con el fin de dar solución al problema de acceso a las salas de cómputo, estas encuestas van dirigidas a los docentes de la Universidad Francisco de Paula Santander Ocaña que se les hayan sido asignadas las salas de cómputo para impartir sus clases, la encuesta se verá enfocada al funcionamiento y mejoramiento del rápido acceso a las salas, preguntas de selección múltiple para analizar la información por medio de gráficas.

Los datos pueden extraerse a partir de toda la población o de una muestra cuidadosamente seleccionada. La información recogida puede referirse a un gran número de factores relacionados con el fenómeno o sólo a unos pocos aspectos recogidos. Su alcance y profundidad dependen de la naturaleza del problema. (Van Dalen, 2006. Párr 8). **Ver apéndice A**

### **3.4. Análisis de información**

Por medio de la herramienta virtual que posee la Universidad Francisco de Paula Santander Ocaña, <https://encuesta.ufps.edu.co> que permite realizar encuestas, formularios y enviarlos a los contactos por vía mensajería Web.

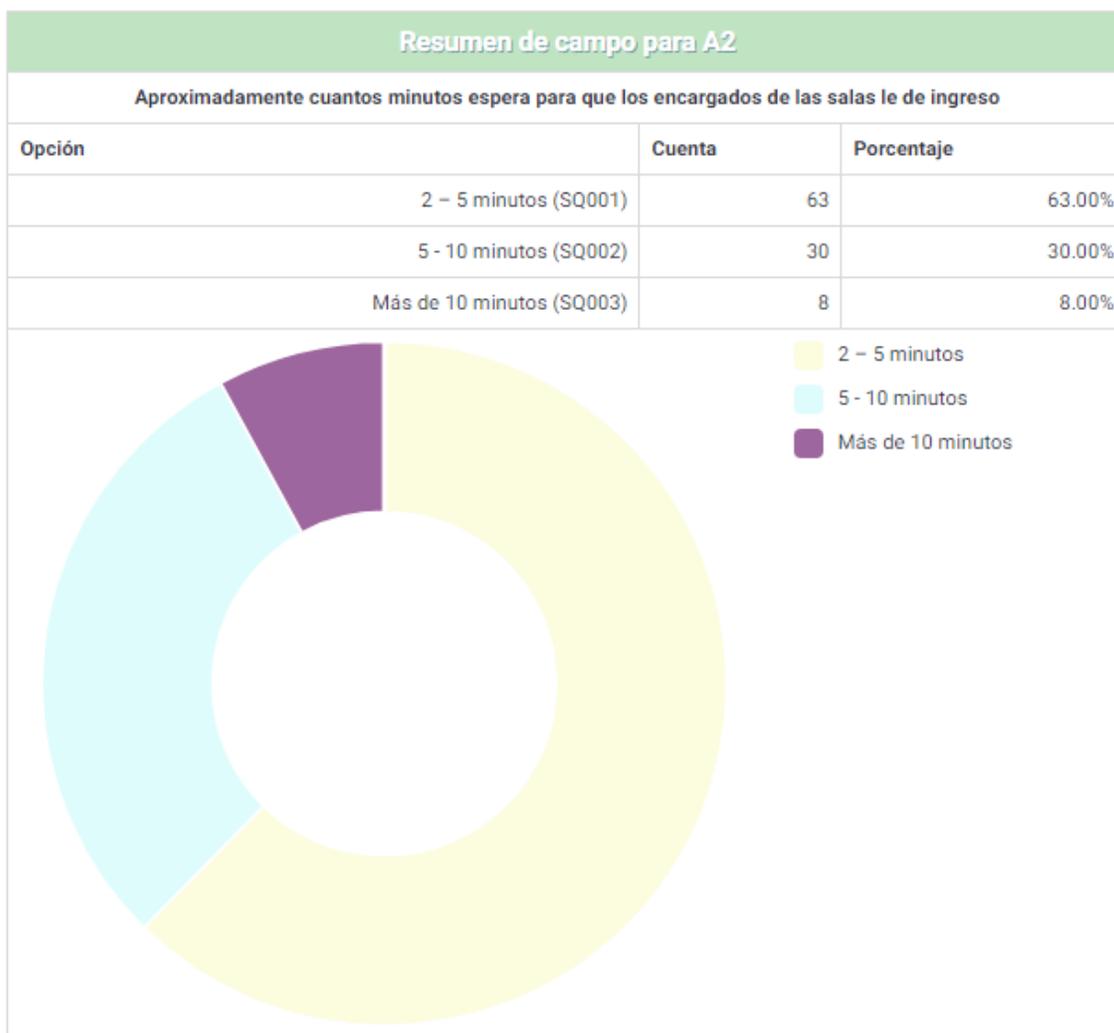
A continuación se muestran por medio de figuras los respectivos resultados que se obtuvieron al momento de desarrollar la encuesta por medio de la plataforma con su respectiva explicación.



**Figura 18. Pregunta 1. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor**

La finalidad de la pregunta es identificar con qué frecuencia la población de docentes utiliza los recursos universitarios por semana, las salas de cómputo y sus componentes.

Basado en los porcentajes arrojados por la encuesta podemos afirmar que el uso constante de estos recursos universitarios es de manera prolongada puesto que el 32% de los encuestados usa estos recursos por lo menos dos veces a la semana y un 26.47% más de 4 veces a la semana.

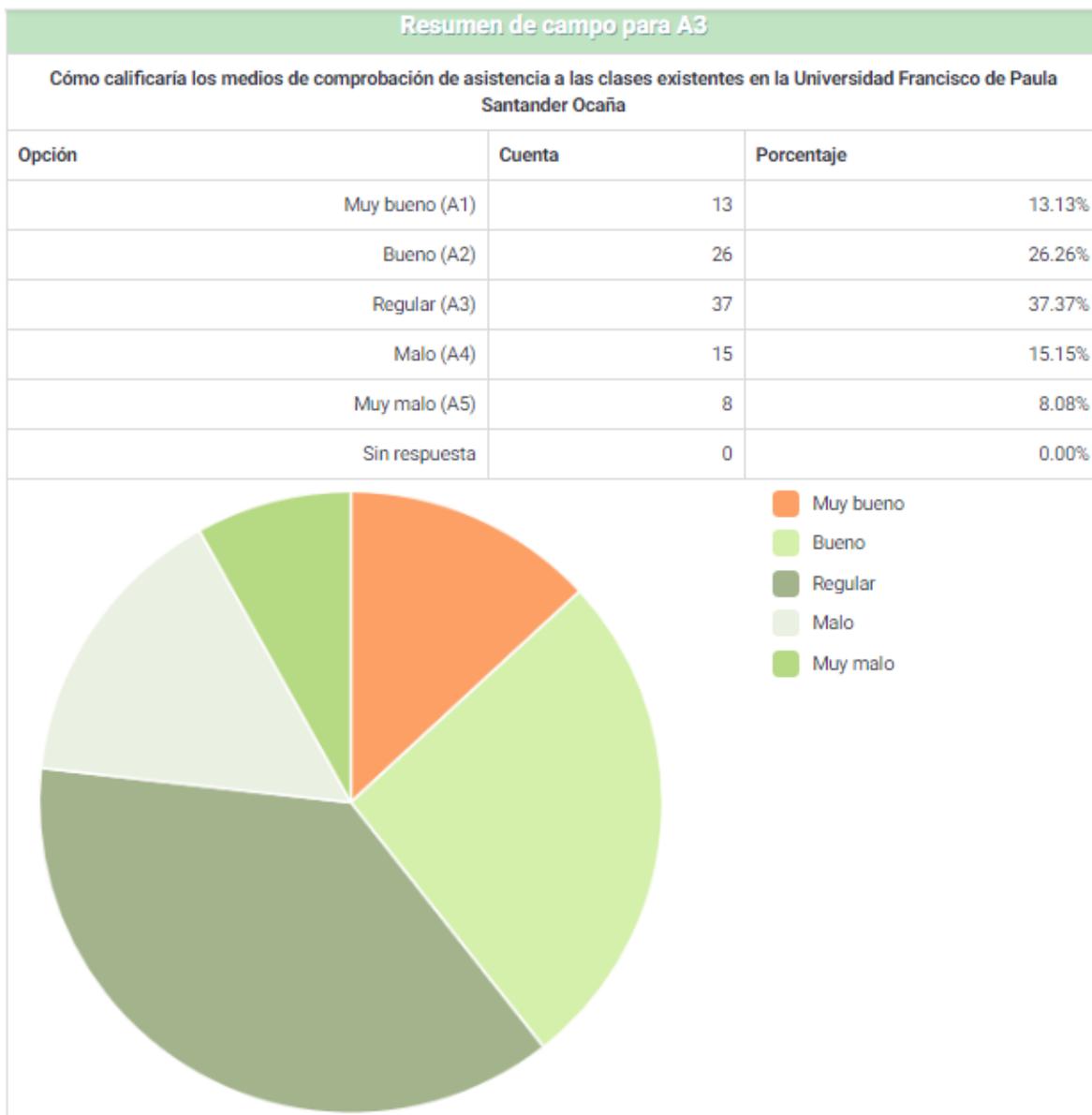


**Figura 19. Pregunta 2. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor**

La finalidad de esta pregunta es definir el tiempo de espera a los que generalmente se enfrentan los docentes a la hora de ingresar a las aulas a impartir las clases correspondientes.

Según las respuestas arrojadas por la empresa los lapsos de tiempo de espera varían, esto de da dependiendo de la ubicación de la sala con respecto a la de los encargados donde un 63% de los encuestados dice que esperan aproximadamente 5 minutos y un 30% dice que espera de 6 a 10 minuto el ingreso a la sala generando así un retarlo a la hora de dar las clases he impidiendo

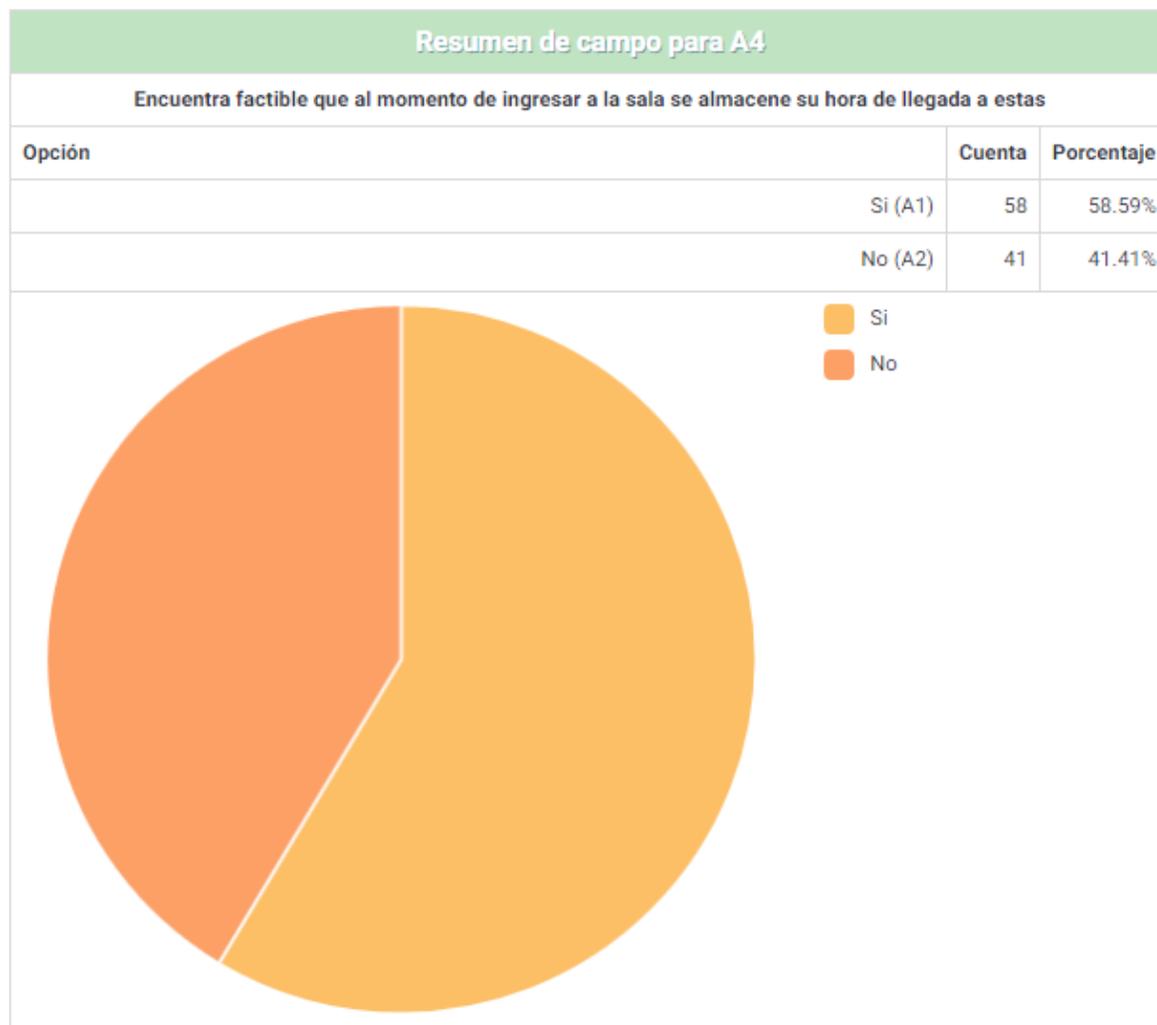
así la toma de los datos sobre la puntualidad de llegada de los docentes.



**Figura 20. Pregunta 3. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor**

Arraigado al problema visto con las respuestas de la pregunta anterior se establece el porcentaje de conformidad o inconformidad con los medios de comprobación de asistencia existentes hasta el momento. La cantidad de docentes encuestados indica una inconformidad con

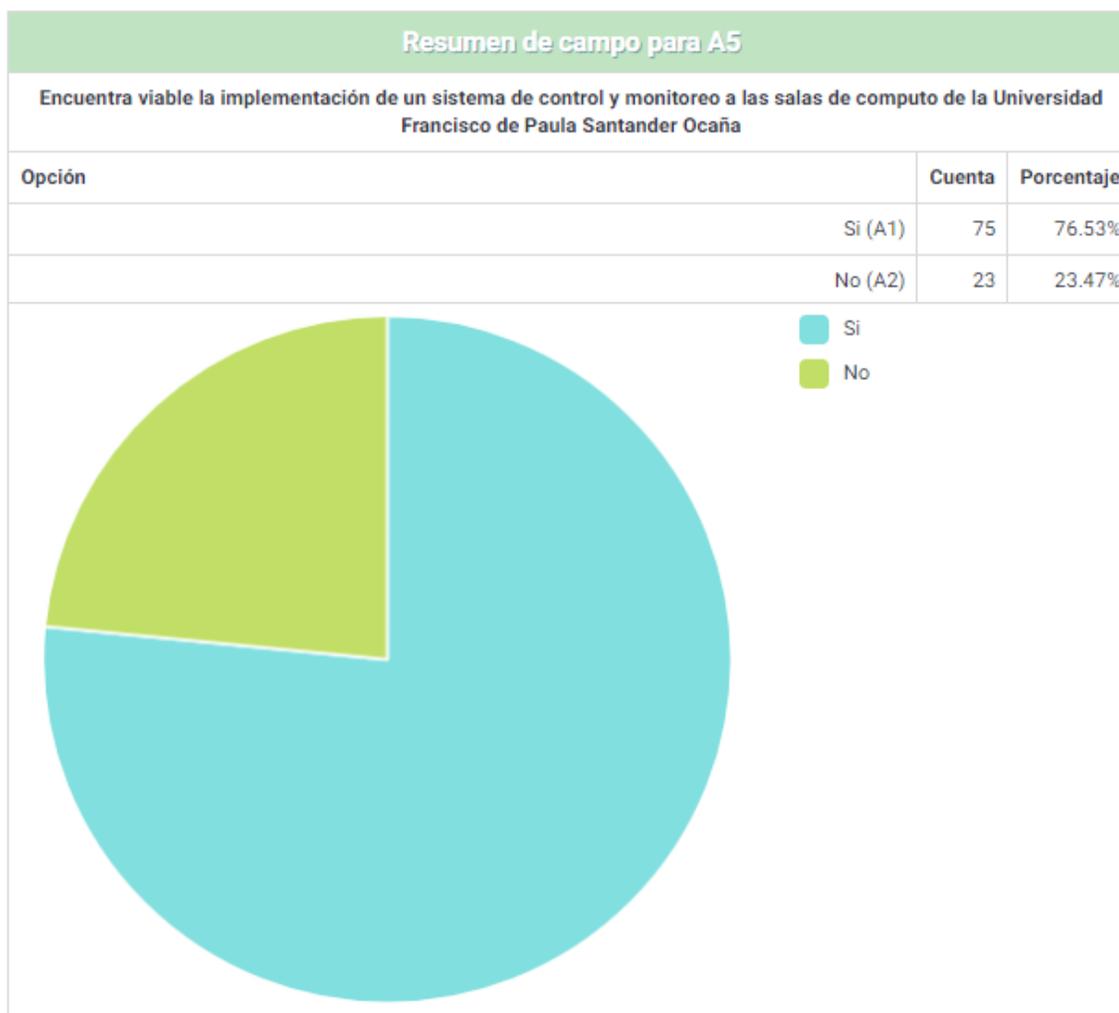
los sistemas de comprobación de asistencia, un 37.37% indica que la manera en cómo se toman estos datos es errónea y necesita un mejoramiento.



**Figura 21. Pregunta 4. Encuesta realizada mediante la plataforma encuesta.ufps.edu.co. Fuente autor**

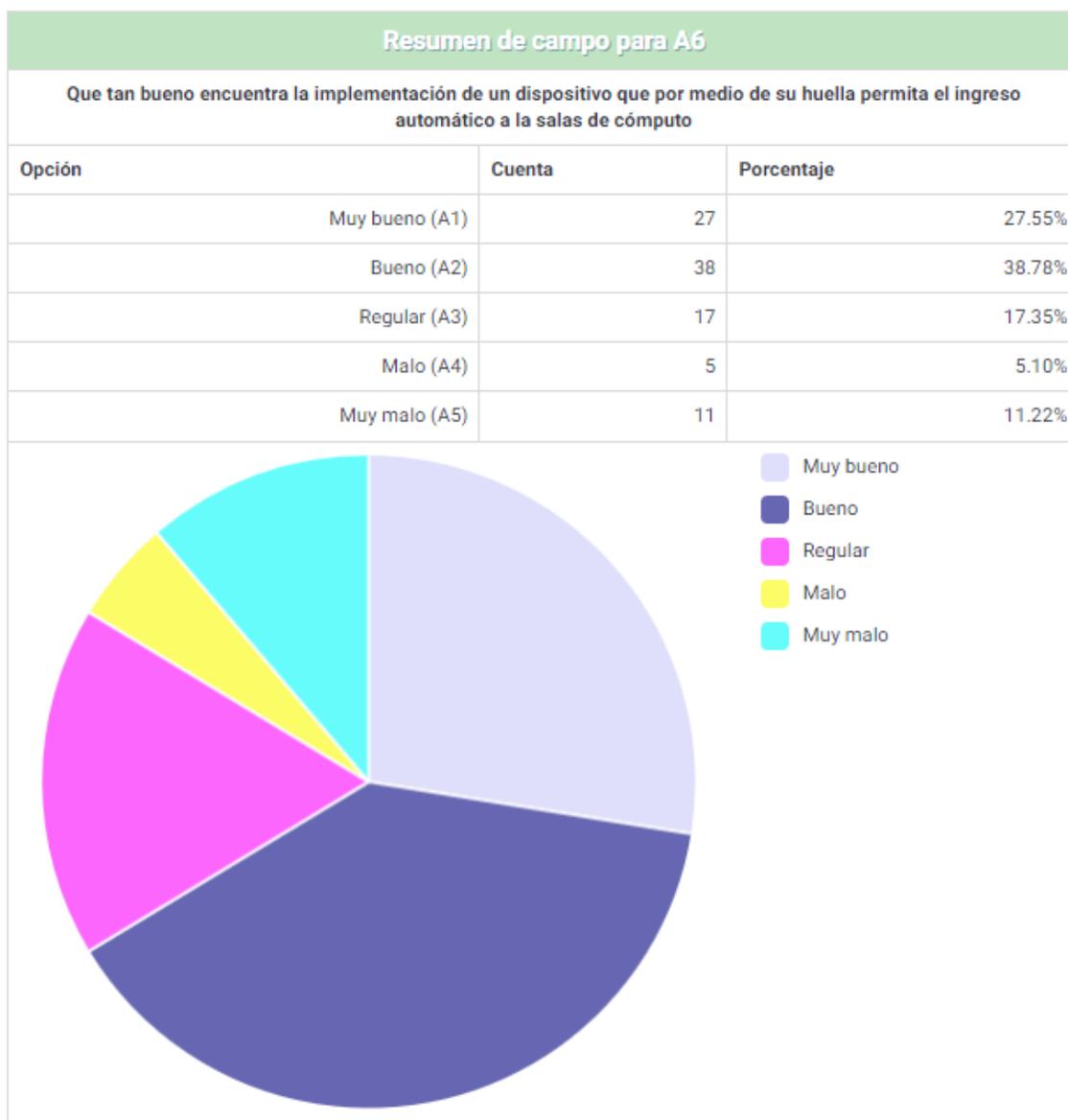
Luego de haber establecido la inconformidad de los docentes frente al tema de la comprobación de asistencias y puntualidad en las clases se muéstrala la posibilidad de almacenar automáticamente su hora de llegada.

Según el porcentaje de respuesta arrojado por la encuesta nos muestra que un 58.59% de los encuestados está de acuerdo mientras un 41% está en desacuerdo con este ítem.



**Figura 22. Pregunta 5. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor**

El propósito de esta pregunta es conocer que tan de acuerdo se encuentran los docentes frente al tema de control y monitoreo de las salas de computo donde un 76.53% de los encuestados están reconocen la viabilidad del proyecto.



**Figura 23. Pregunta 6. Encuesta realizada mediante la plataforma encuesta.ufpso.edu.co. Fuente autor**

Esta pregunta tiene como fin mostrar que tan acertada es la implementación de un sistema de monitoreo que use la autenticación biométrica (huella dactilar) como medio de comprobación.

## **CAPÍTULO 4: Administración Del Proyecto**

### **4.1 Recursos**

#### **4.1.1 Recursos humanos**

##### **Investigador y autor del proyecto.**

Alvaro Javier Moreno Rizo.

Estudiante Ingeniería De Sistemas de la Universidad Francisco de Paula Santander Ocaña.

##### **Director del proyecto.**

ING. Antón García Barreto.

##### **Empleados sala de servidores Universidad Francisco de Paula Santander Ocaña.**

##### **Profesional de apoyo.**

Numael Hernando Molina Angarita.

Leonardo Zambrano.

##### **Técnico en redes.**

Arley Santiago Q.

#### **4.1.2. Recursos Institucionales (Materiales)**

- Equipo de Computo

- Útiles de papelería
- Sujetadores aluminio.



**Figura 24. Sujetadores de aluminio reforzados. Fuente autor.**

- Lector Biométrico de huella dactilar con HID BioEntry W



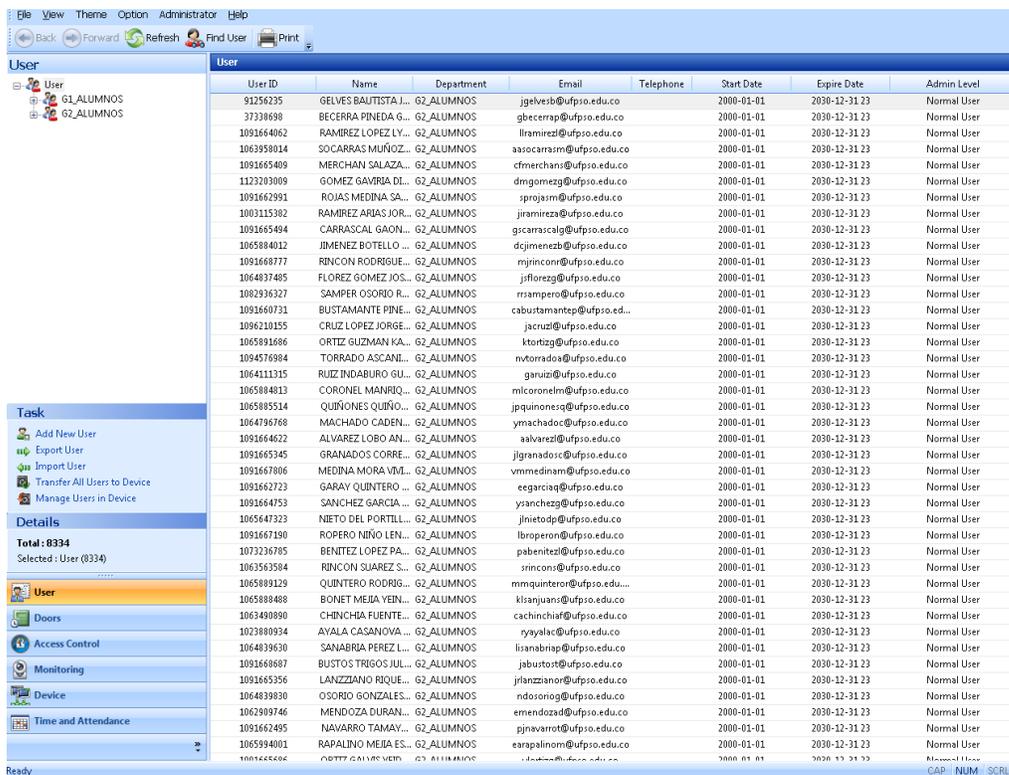
**Figura 25. Lector biométrico BioEntry W. Fuente autor.**

- Cable UTP categoría 6, con conector RJ45.



**Figura 26. Cable UTP CAT6 con topología conexión directa y conector RJ45. Fuente autor**

- Interfaz de usuario Biostar 1.0x



The screenshot displays the Biostar 1.0x user management interface. It features a menu bar at the top with options like 'File', 'View', 'Theme', 'Option', 'Administrator', and 'Help'. Below the menu is a toolbar with icons for 'Back', 'Forward', 'Refresh', 'Find User', and 'Print'. The main area is a table listing users, with columns for 'User ID', 'Name', 'Department', 'Email', 'Telephone', 'Start Date', 'Expire Date', and 'Admin Level'. A left-hand sidebar contains navigation options such as 'Task' (Add New User, Export User, Import User, Transfer All Users to Device, Manage Users in Device) and 'Details' (Total: 8334, Selected: User (8334)).

User ID	Name	Department	Email	Telephone	Start Date	Expire Date	Admin Level
91256235	GELVES BAUTISTA J...	G2_ALUMNOS	ggelvest@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
37338698	BECERRA PINEDA G...	G2_ALUMNOS	gbecerrap@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091644062	RAMIREZ LOPEZ LY...	G2_ALUMNOS	lramirezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063958014	SOCARRAS MUÑOZ...	G2_ALUMNOS	asocarrasm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091645409	MERCHAN SALAZA...	G2_ALUMNOS	cfmerchans@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1123203009	GOMEZ GAVIRA DL...	G2_ALUMNOS	dmgomezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091642991	ROJAS MEDINA SA...	G2_ALUMNOS	srojasrsm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1003115382	RAMIREZ APIAS JOR...	G2_ALUMNOS	jramireza@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091645494	CARRASCAL GAON...	G2_ALUMNOS	gcarrascalg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065984012	JIMENEZ BOTELLO ...	G2_ALUMNOS	djimenezb@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091648777	RINCON RODRIGUE...	G2_ALUMNOS	mjinconr@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064837485	FLOREZ GOMEZ JOS...	G2_ALUMNOS	jiflorezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1092936327	SAMPER OSORIO R...	G2_ALUMNOS	rsampero@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091640731	BUSTAMANTE PINE...	G2_ALUMNOS	cabustamantep@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1096210155	CRUZ LOPEZ JORGE...	G2_ALUMNOS	jacruzl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065931686	ORTIZ GUZMAN KA...	G2_ALUMNOS	ktorizg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1094576984	TORRADO ASCANIL...	G2_ALUMNOS	ntorradoa@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064111315	RUIZ INDIABURO GU...	G2_ALUMNOS	ruizigu@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065984013	CORONEL MANRIQU...	G2_ALUMNOS	mlcoronelm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065989514	QUIÑONES QUIÑO...	G2_ALUMNOS	jqquinonesq@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064786768	MACHADO CADEN...	G2_ALUMNOS	ymachadoc@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091644622	ALVAREZ LOBO AN...	G2_ALUMNOS	salvarezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091645345	GRANADOS CORRE...	G2_ALUMNOS	jgranadosc@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091647806	MEDINA MORA VMI...	G2_ALUMNOS	vmmedinam@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091642723	GARAY QUINTERO ...	G2_ALUMNOS	egarayq@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091644753	SANCHEZ GARCIA ...	G2_ALUMNOS	ysanchezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065647323	NIETO DEL PORTIL...	G2_ALUMNOS	jnietodp@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091647190	ROPERO NIÑO LEN...	G2_ALUMNOS	lroperon@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1073236785	BENITEZ LOPEZ PA...	G2_ALUMNOS	psbenitezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063563594	RINCON SUAREZ S...	G2_ALUMNOS	srincon@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065989129	QUINTERO RODRIG...	G2_ALUMNOS	mqquinteror@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065989488	BONET MEJA YEIN...	G2_ALUMNOS	kybonetj@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063498990	CHINCHA FUENTE...	G2_ALUMNOS	cachinchiaf@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1023989934	AYALA CASANOVA ...	G2_ALUMNOS	tyayalac@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064839630	SANABRIA PEREZ L...	G2_ALUMNOS	lsanabriap@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091648607	BUSTOS TRIGOS JUL...	G2_ALUMNOS	jbustosr@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091645356	LANZZANO RIQUE...	G2_ALUMNOS	jlanzzanor@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064839830	OSORIO GONZALEZ...	G2_ALUMNOS	ndosorio@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1062989746	MENDOZA DURAN...	G2_ALUMNOS	emendozad@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091642495	NAVARRO TAMAYO...	G2_ALUMNOS	pnavarrat@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065994001	RAPALINO MEJA ES...	G2_ALUMNOS	erapalino@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091645606	ORTIZ CALVO VED...	G2_ALUMNOS	vortizcalvo@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User

Figura 27. Interfaz Biostar. Fuente autor software Biostar.

- Canaleta adhesiva 2\*2

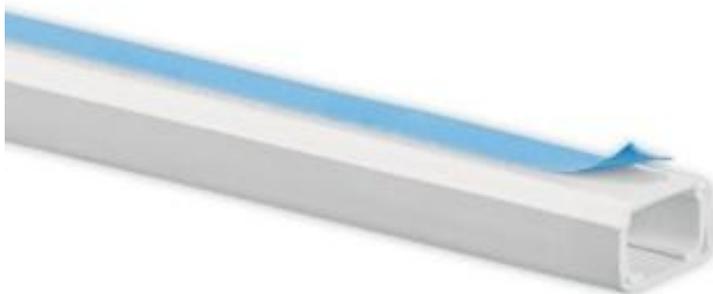


Figura 28. Canaleta 2x2. Fuente Telnet

- Botón press o botón del pánico



**Figura 29. Botón del pánico. Fuente autor**

- Batería en gel 12 voltios



**Figura 30. Batería en gel. Fuente autor**

- Cable UTP categoría 6



**Figura 31. Cable UTP categoría 6. Fuente autor**

- Conector corriente AC/AC



**Figura 32. Conector de corriente directa AC/AC. Fuente autor**

- SK-910RBQ (canal de conexión entre cerradura y Bioentry)



**Figura 33. SK-910RBQ canal de conexión. Fuente autor**

- ST-1206-1.5AQ (Fuente de alimentación / cargador)



**Figura 34. ST-1206-1.5AQ fuente de alimentación. Fuente autor**

- Equipo de oficina División de Sistemas UFPSO

### **4.1.3 Recursos Financieros**

#### **4.3. Recurso financiero**

El proyecto será financiado por la Universidad Francisco de Paula Santander Ocaña.

**Tabla 1. Implementos utilizados**

<b>Elementos</b>	<b>Complementos</b>	<b>Valor</b>
Kit Electroimán de 600 lbs	-Cerradura Electroimán de 600 Lbs. -Control inalámbrico dos botones. -Canal receptor (Accesorio Electroimán) RF 315 MHz compatible con todos los SECO-LARM transmisores. 11-24VDC/VAC. REF.SK-910RBQ. Power Supply/Charger	1.071.000
Capta huella Multipropósito	lector de huella para PC con conexión USB Lector HID	870.000
Control de Acceso Biométrico	Tarjeta inteligente Tipo exterior anti vandálico	4.350.000
Cableado UPT categoría 6	_____	2.050.000
Software para el manejo del control de acceso	_____	5.000.000

## **CAPITULO 5: Resultados**

### **5.1. Identificar los requisitos funcionales y no funcionales que cumplan con los requisitos del proyecto.**

- **Requerimientos funcionales**

RF. 01: El sistema permitirá el acceso de manera remota para la manipulación de los datos y la administración de estos.

RF. 02: El sistema solo permitirá a dos administradores de sistema donde estos no podrán estar logueados simultáneamente.

RF. 03: El sistema permitirá la inclusión de nuevos usuarios con sus datos correspondientes por medio de su interfaz gráfica.

RF. 04: El sistema otorgara un identificador único por usuario el cual en este caso es el código asignado por la Universidad Francisco de Paula Santander Ocaña.

RF. 05: El sistema permitirá crear puertas lógicas las cuales serán asignadas a las salas de cómputo por nombre de sala.

RF. 06: El sistema permitirá asignar los lectores biométricos a las puertas con su interfaz gráfica.

RF. 07: El sistema permitirá almacenar los horarios y salas asignados a los docentes.

RF. 08: El sistema permitirá dar acceso a las salas por medio de grupos de acceso lógicos creados con la interfaz gráfica.

RF. 09: El sistema monitoreare el acceso solamente a usuarios autorizados.

RF. 10: Los usuarios deben ingresar al sistema por medio de su huella dactilar.

RF. 11: El usuario podrá tener acceso a las salas de cómputo por medio de su carnet institucional si no posee una huella dactilar legible.

RF. 12: El sistema almacenara la hora y fecha de llegada de los usuarios.

RF. 13. El sistema permitirá generar y emitir informes de asistencia.

RF. 14: El proceso de validación de usuario y almacenamiento de hora de llega se hará de manera inmediata.

RF. 15: El sistema controlara el ingreso a todas las salas de cómputo de manera simultánea y automatizada.

RF. 16: El sistema brindara acceso continuo a los monitores de salas de cómputo para que estos puedan acceder a la hora deseen y puedan dar acceso a estudiantes que requieran las salas.

RF. 17: Al momento de ingresar la huella el sistema comprobara si el usuario posee clases en la sala que desea acceder, si la respuesta da negativa el sistema NO permitirá el ingreso.

RF. 18: El sistema NO otorgara acceso a las salas a los estudiantes, para eso estarán disponibles los asistentes de salas.

- **Requerimientos no funcionales**

RNF. 01 Los lectores biométricos deben estar uno por puerta para el control independiente de las entradas por sala de cómputo.

RNF. 02 Los electroimanes que actúan como cerrojo de las puertas deben estar situado en la parte superior de las puertas.

RNF. 03: los lectores biométricos deben poseer una batería como respuesta alterna al fallo de corriente eléctrica.

RNF. 04: Los implementos de conexión como el suministro de carga y el controlador de canal de información deberán ser resguardados en una caga especializada donde no puedan ser manipulados por terceros.

RNF. 05: la conexión realizada con el cable UTP categoría 6 debe ser resguardada con una canaleta adhesiva 2x2.

RNF. 06: La conexión al servidor se debe hacer de manera remota utilizando su IP.

RNF. 07: La configuración de red en los lectores biométricos se realiza con IPV4.

RNF. 08: Si no se obtiene conexión con la base de datos el sistema almacenara en el dispositivo las horas de llegada de los usuarios y cuando se reanude la conexión enviara los datos para su almacenamiento.

RNF. 09: Todo intento de ingreso debe ser verificado en menos de 5 segundos.

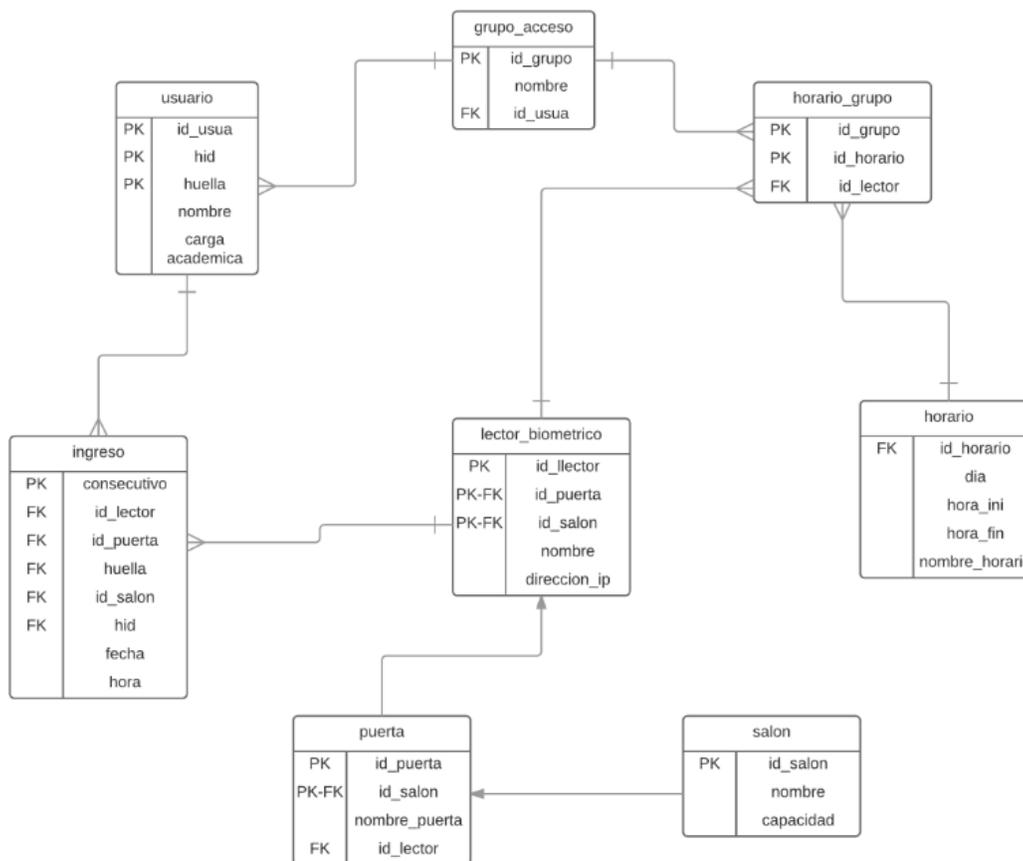
RNF. 10: Los permisos de acceso he ingreso solo pueden ser modificados por dos administrador de sistema.

RNF. 11: El Desarrollo deberá contar con cinco dispositivos para que cierren el circuito incluyendo la batería, los cuales son lector biométrico HID, suministro de carga Enforcer, controlador de canal de información, cerradura con electroimán.

RNF. 12: El sistema por medio del sonido y color en su led debe informar al usuario si su logueo al sistema fue exitoso o no donde el color azul es si y el rojo no.

RNF. 13: La configuración de las IP no será mostrada por seguridad y fiabilidad de la información.

**5.2. Definir un modelo de entidad relación para la base de datos que contenga la información necesaria para su uso lógico.**



**Figura 35. Modelo entidad relación (MER) sobre modelo de negocio. Fuente autor del proyecto.**

**5.3. Implantar una aplicación que permita interactuar con los datos.**

Al momento de buscar la manera en cómo manejar un volumen de información bastante alto, como lo es la información del personal de la Universidad Francisco de Paula Santander

Ocaña. Se toma como base que la información requerida está centralizada en una base de datos en ORACLE.

La aplicación implantada para este proceso es el sistema de administración BIOSTAR.

- **Como instalar**

- 1. Insertar cd de instalación del servidor Biostar**

- 2. Localizar el directorio de instalación(setup de instalación)**

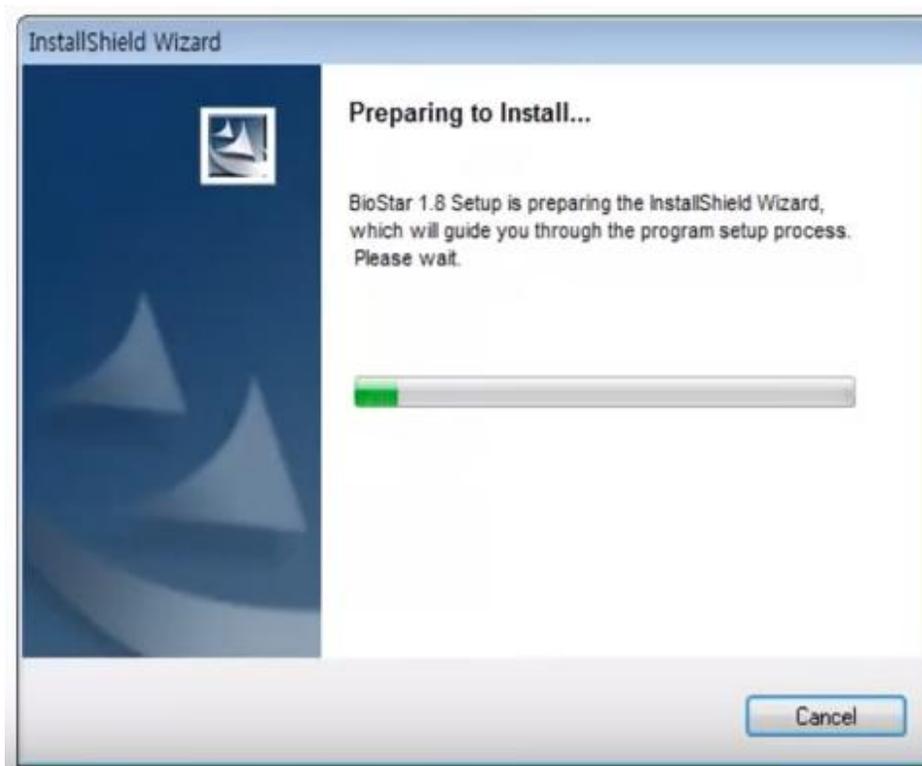
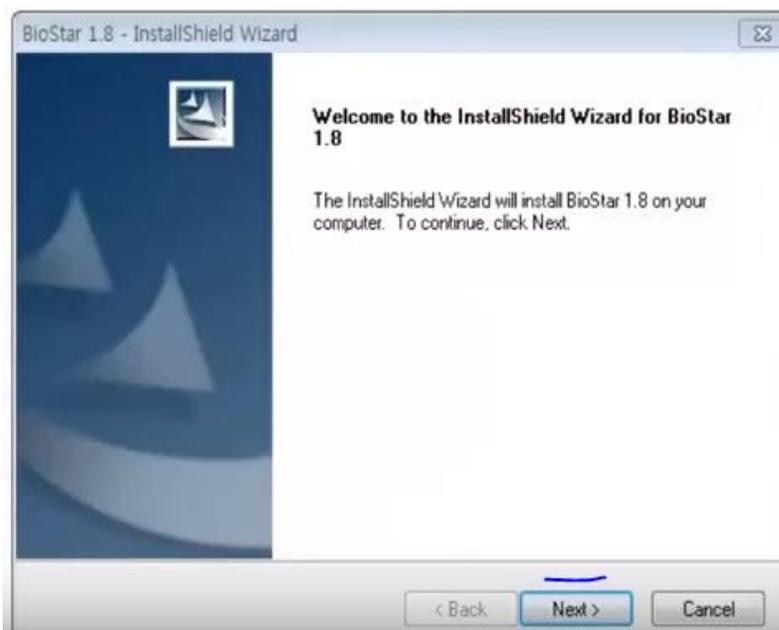
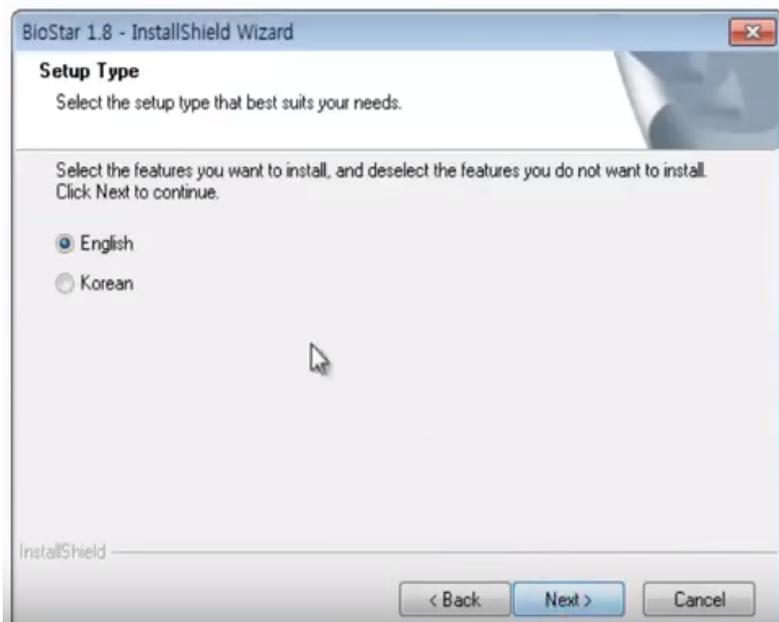


Figura 36. Instalación sistema Biostar, click a setup. Fuente autor software Biostar.

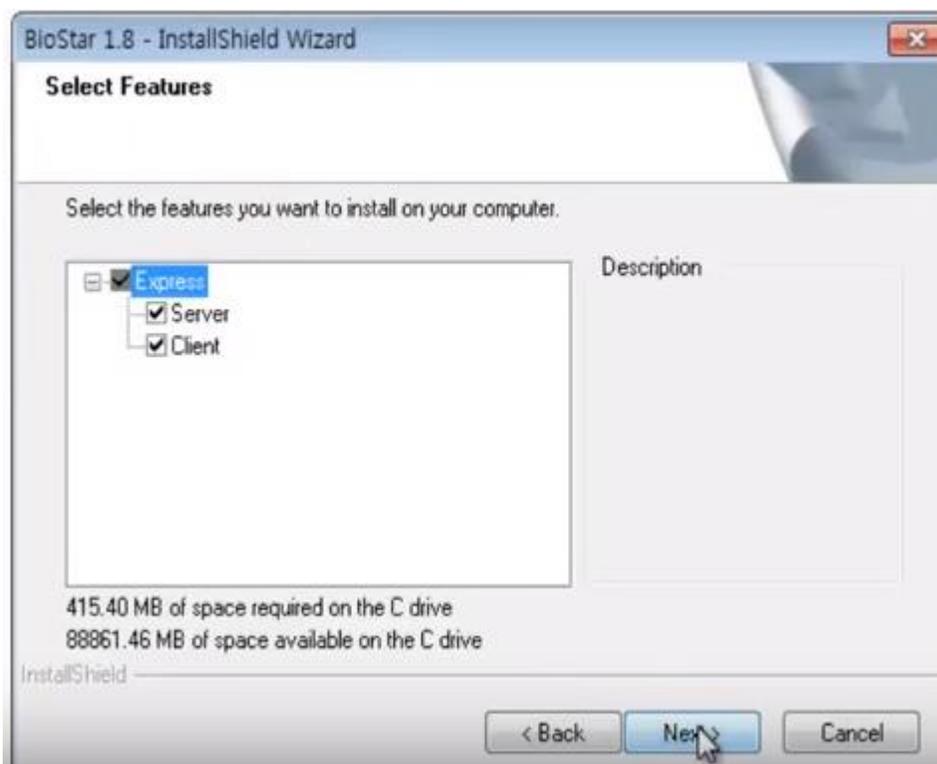
- 3. Seguir las instrucciones que aparecen en pantalla**



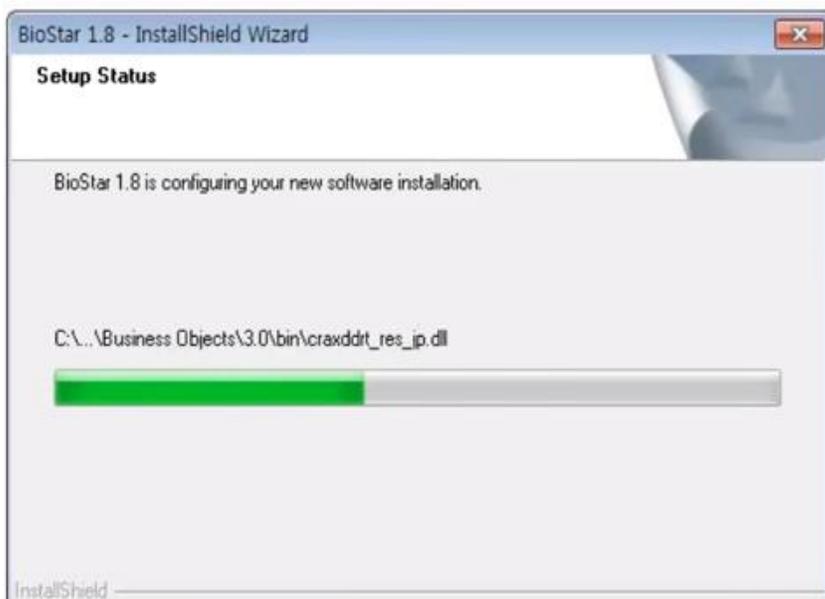
**Figura 37. Primera pantalla de instrucción. Fuente autor software Biostar.**



**Figura 38. Segunda pantalla de instrucción. Fuente autor software Biostar.**



**Figura 39. Tercera pantalla de instrucción. Fuente autor software Biostar.**



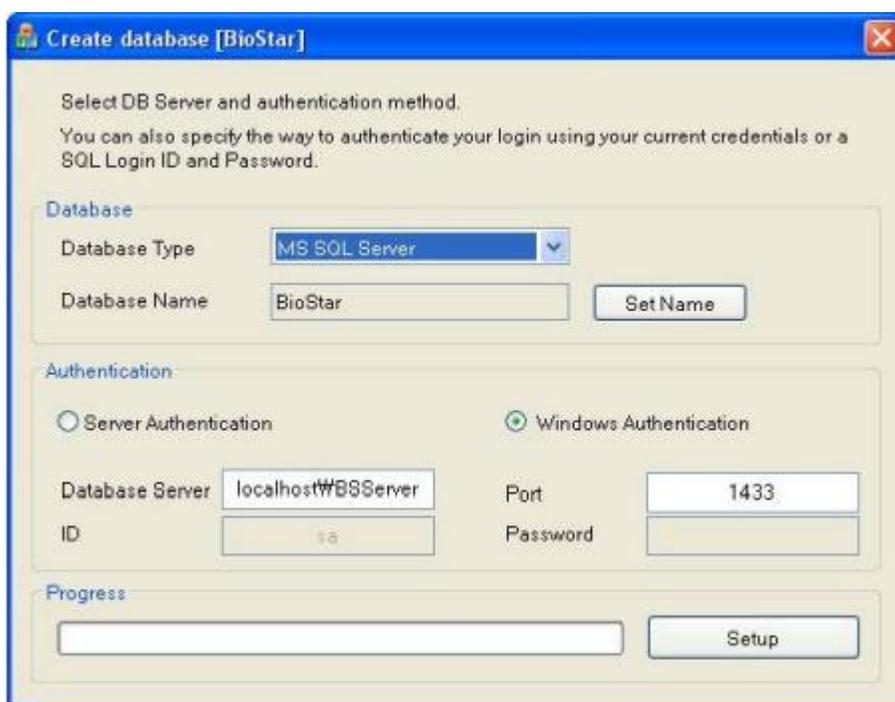
**Figura 40. Cuarta pantalla de instrucción. Fuente autor software Biostar.**

Al momento de dale siguiente (next) en la anterior pantalla se procede a instalar los

paquetes necesarios para la configuración de manera gráfica.

- **Como crear a base de datos**

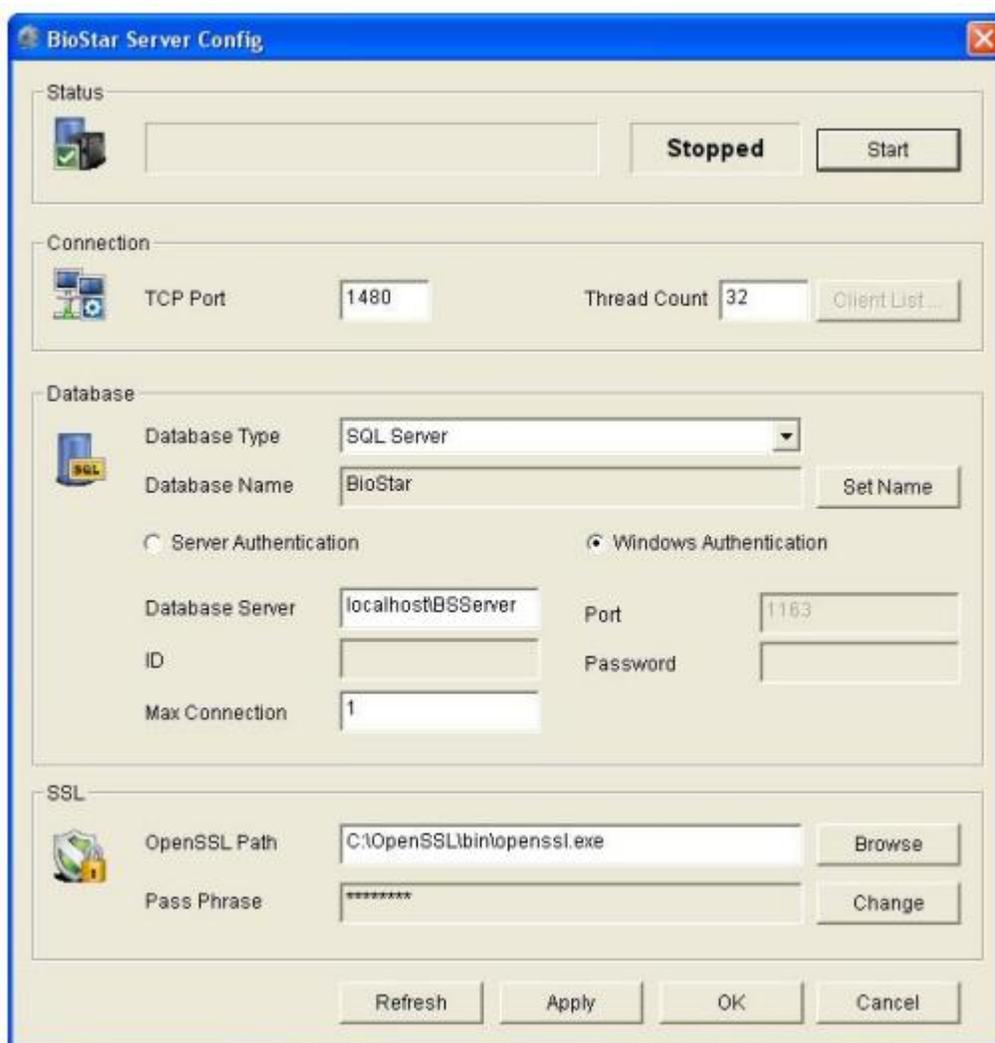
Por seguridad la configuración a continuación es un ejemplo de cómo se debe desarrollar, puesto que los datos involucrados son de alto valor y mostrarlo puede generar vulnerabilidad al sistema de información de donde se toman los datos de los docentes. Se hacen de esta manera por recomendación del director del proyecto.



**Figura 41. Creando base de datos sistema Biostar. Fuente autor, software Biostar.**

Al ejecutar el sistema ya instalado se nos muestra una pestaña como la figura 41. Donde podemos seleccionar el tipo de base de datos, el servidor de donde llamaremos los datos (database server) el puerto de comunicación y el nombre que se le dará. Como la universidad Francisco de Paula Santander Ocaña tiene una base de datos en Oracle el tipo de base de datos seleccionado será el mismo.

Si el tamaño máximo de los paquetes enviados a la base de datos es de 16MB, genera un error de cuello de botella donde la capacidad de la base de datos se ve afectada por ende se utiliza una pequeña línea de código para solucionar esto, en los archivos del servidor se busca: en Windows (ora.ini) y en Linux (ora.lnf) para ambos casos se modifica la línea: `max_allowed_packet=16MB`. Se guarda el archivo modificado y se reinicia el servidor para que tome los cambios.



**Figura 42. Configurando base de datos sistema BioStar. Fuente autor, software BioStar**

Al momento de crear la base de datos nos muestra una ventana donde podemos supervisar

y configurar lo siguiente:

- **Status:** se visualiza y modifica el estado actual del servidor Biostar (Stopped – Started) donde podemos observar que el servidor está detenido.
- **Connection:** visualiza y modifica los detalles de la conexión de los dispositivos con el servidor y el número máximo de subprocesos que este puede llevar a cabo, **si el número es más alto se requiere más recursos del sistema.**
- **Database:** se visualiza y modifica la configuración de la base de datos.
- **Max Connection:** esta es una de las partes más importantes dado que en esta se especifica el número de conexiones que puede existir entre el servidor y la base de datos.
- **SSL (Secure Sockets Layer):** visualiza el tipo de seguridad y configuración de la seguridad que posee la base de datos y el servidor incluyendo la contraseña que se maneje.

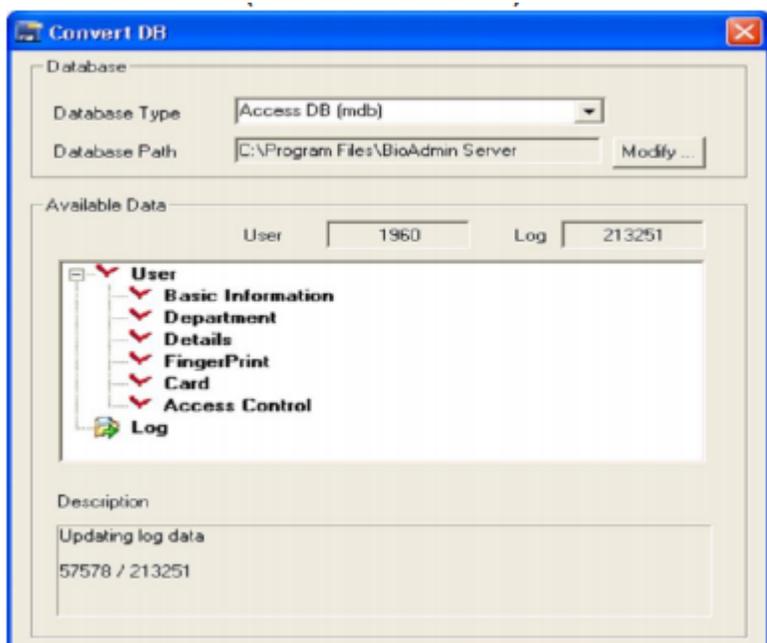


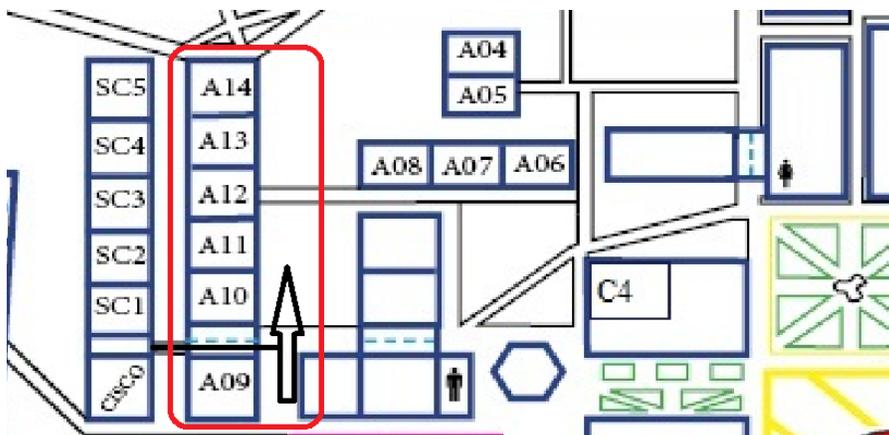
Figura 43. Migrar información a la base de datos. Fuente autor, sistema Biostar

.al tener la base de datos configurada se procede a migrar los datos de la base de datos en Oracle a el sistema Biostar (proceso desarrollado en la sala de servidores de la Universidad Francisco de Paula Santander Ocaña el cual no se muestra por cuestiones de seguridad). Al finalizar este proceso aparece la pestaña de la figura 43, donde podemos ver los datos migrados como, la información básica, el departamento o dependencia al cual está asociado, la huella dactilar entre otros.

#### **5.4. Realizar el análisis de recorrido y funciones que cumplen los asistentes de sala de cómputo.**

Partiendo del mapa ya mostrado el recorrido que toma los encarados de salas para el reporte y monitoreo es el siguiente:

- **Primer recorrido**



**Figura 44. Primer recorrido, Fuente Autor, mapa UFPSO 2016.**

Parte de control de salas bloque A, desde las salas A9 hasta A14. Donde debe verificar y anotar la hora de llegada del docente.

- **Segundo recorrido**

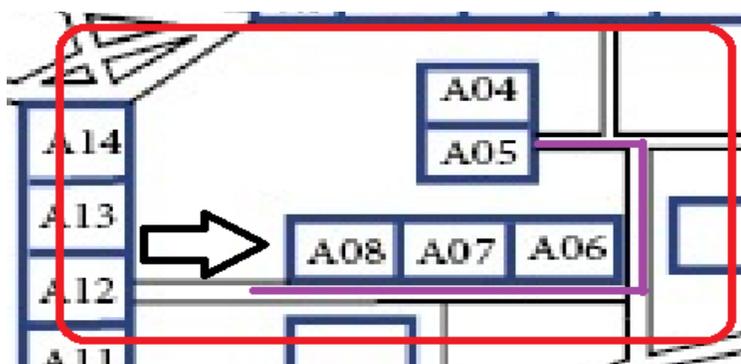


Figura 45. Segundo recorrido, Fuente Autor, mapa UFPSO 2016.

Después de revisar el bloque de aulas A9-A14, se dirigen hacia, A8-A7-A6-A5-A4.

- Tercer recorrido

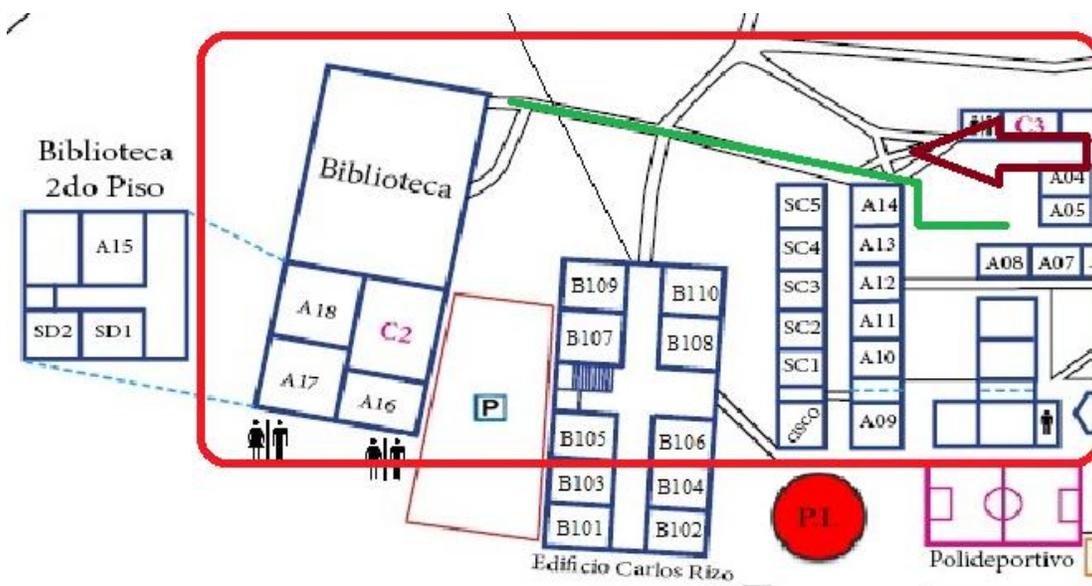
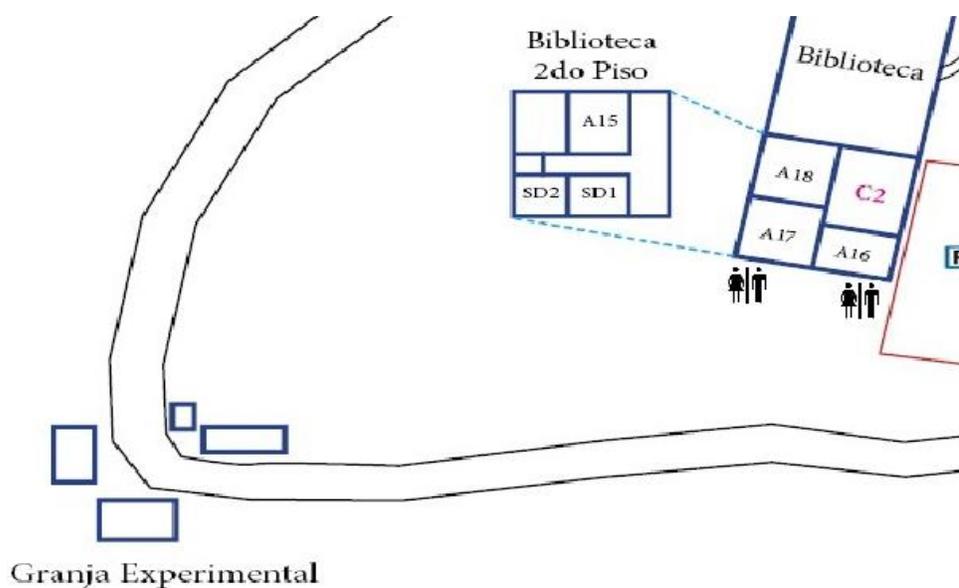


Figura 46. Tercer recorrido, Fuente Autor, mapa UFPSO 2016.

Luego de terminar por completo el bloque de aulas A parte para biblioteca y observan los salones cercanos a esta, de A15 hasta A18, las salas SD1 y SD2.

- **Cuarto recorrido**



**Figura 47. Cuarto recorrido, Fuente Autor, mapa UFPSO 2016.**

Al terminar el recorrido por los salones de biblioteca parten a la granja, luego regresan al edificio Carlos Rizo o bloque B.

Cabe recalcar que los encargados de las salas de computo se encargan del monitoreo y reporte oportuno del cumplimiento de horarios de los docentes y uso pertinente de las salas de computo.

**Recorrido de tiempo aproximado: 30 minutos.**

**Con la implementación del sistema Biostar para el manejo de información en conjunto con el sistema de autenticación biométrica el procedimiento se reduce en aproximadamente 25 minutos dando un estimado de efectividad de un 95%.**

**5.5. Almacenar en una base de datos los patrones biométricos de los docentes que imparten clases en las salas de cómputo de bloque A y edificio Carlos Rizo.**

En esta etapa de desarrollo tomamos la información disponibles en la base de datos de la Universidad Francisco de Paula Santander Ocaña y la ingresamos en los lectores biométricos la cual en este caso es la identificación biométrica de los docentes.

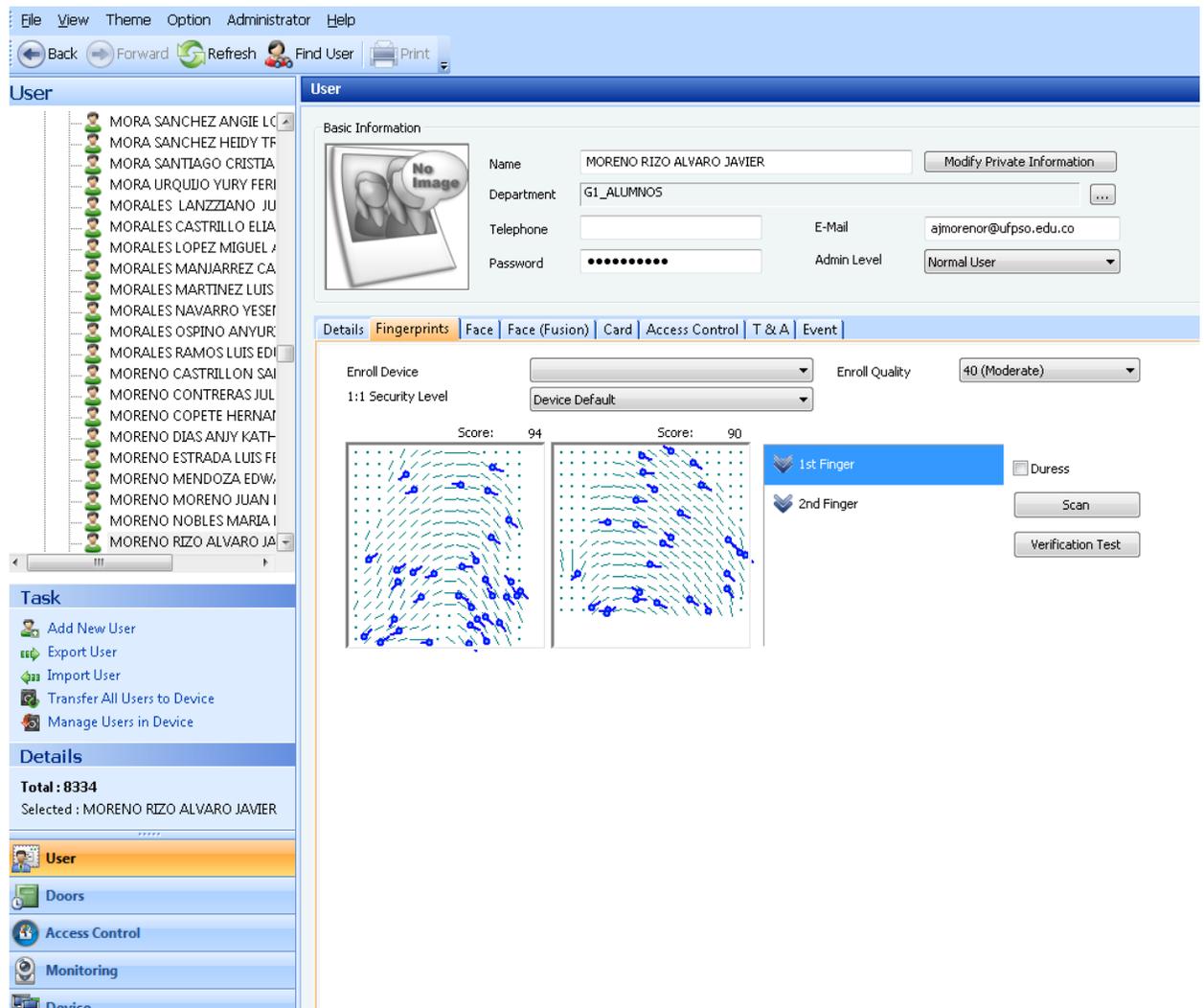


Figura 48. Modelo de almacenamiento de datos biométricos. Fuente autor, software Biostar 1.9

**5.6 Generar informes de cumplimiento de horario a docentes y utilización de las salas de cómputo en las horas establecidas.**

Date	Device ID	Device	Event	T&A Event	User ID	User	Status
2017-11-27 06:59:04	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-27 12:03:59	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-27 14:01:17	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-27 17:12:37	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-28 06:57:53	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-28 08:19:21	543611728	SERVIDO...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-28 12:04:57	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-28 13:58:42	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-28 17:12:54	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-29 07:01:07	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-29 07:53:16	543611728	SERVIDO...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-29 12:04:25	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-29 14:01:09	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-29 17:05:51	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-30 06:59:24	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-30 07:45:17	543611728	SERVIDO...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-30 12:05:57	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-30 13:59:13	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	
2017-11-30 17:13:34	543609541	DIVISIS[1...	Identify Success		63452456	RINCON CONTRERA...	

**Figura 49. Informe de llegada de los usuarios. Fuente Autor, software Biostar**

La figura anterior muestra la manera en como el sistema almacena la hora de llegada del usuario y muestra el reporte de las horas, el orden de la información está constituido por:

- Fecha y hora de llegada.
- Dispositivo el cual está asociado a una puerta con su respectivo nombre.
- El evento, que muestra si el usuario tiene permitido el ingreso a esa hora o no.
- ID de usuario, su identificador principal en la base de datos.
- Nombre de usuario.

Device		Device				
Device		Device ID	Name	Type	IP	Connect Type
BioStar Server		543609602	BLOQUEAULAS-3[172.20.165.9]	BioEntryW	172.20.165.9	Ethernet
ARCHIVO[172.20.165.3]		543609542	SALA_AUDIENCIAS[172.20.165.15]	BioEntryW	172.20.165.15	Ethernet
BELLAS_ARTES[172.20.165.5]		543611735	SC-CS[172.20.165.19]	BioEntryW	172.20.165.19	Ethernet
BIBLIOTECA[172.20.165.11]		543609541	DIVISIS[172.20.165.2]	BioEntryW	172.20.165.2	Ethernet
BIENESTAR[172.20.165.7]		543609601	SC-GNR1[172.20.165.20]	BioEntryW	172.20.165.20	Ethernet
BLOQUEAULAS-1 [172.20.165.8]		543609597	SC-INGCIVIL[172.20.165.21]	BioEntryW	172.20.165.21	Ethernet
BLOQUEAULAS-3[172.20.165.9]		539341204	DATA CENTER BA	BioEntryPlus	172.20.165.22	Ethernet
DATA CENTER BA		543609587	DIE-[172.20.165.5]	BioEntryW	172.20.165.5	Ethernet
DIE-[172.20.165.5]		543609114	ARCHIVO[172.20.165.3]	BioEntryW	172.20.165.3	Ethernet
DIVISIS[172.20.165.2]		543609586	POSTGRADOS[172.20.165.4]	BioEntryW	172.20.165.4	Ethernet
GRANJA[172.20.165.12]		543609532	PASANTIAS[172.20.165.6]	BioEntryW	172.20.165.6	Ethernet
LABORATORIO[172.20.165.10]		543609526	BELLAS_ARTES[172.20.165.14]	BioEntryW	172.20.165.14	Ethernet
LABORATORIO[172.20.165.10]		543609585	BIENESTAR[172.20.165.7]	BioEntryW	172.20.165.7	Ethernet
LABORATORIO[172.20.165.10]		543609589	LAB_FISICA[172.20.165.10]	BioEntryW	172.20.165.10	Ethernet
LABORATORIO[172.20.165.10]		543611728	SERVIDORES[172.20.165.18]	BioEntryW	172.20.165.18	Ethernet
LABORATORIO[172.20.165.10]		543609603	BIBLIOTECA[172.20.165.11]	BioEntryW	172.20.165.11	Ethernet
LABORATORIO[172.20.165.10]		543609540	BLOQUEAULAS-1 [172.20.165.8]	BioEntryW	172.20.165.8	Ethernet
LABORATORIO[172.20.165.10]		543609588	GRANJA[172.20.165.12]	BioEntryW	172.20.165.12	Ethernet
LABORATORIO[172.20.165.10]		543609594	SUB_ACADEMICA[172.20.165.13]	BioEntryW	172.20.165.13	Ethernet
LABORATORIO[172.20.165.10]		543609599	RESTAURANTE[172.20.165.17]	BioEntryW	172.20.165.17	Ethernet

Figura 50. Lectores biométricos asociados al sistema de monitoreo. Fuente Autor, software Biostar.

Door/Zone Monitoring		Realtime Monitoring		Log List			
Period	03/09/2018	<input type="checkbox"/> Event	Priority 0	<input type="button" value="Get Log"/>	<input type="button" value="Clear"/>		
~	28/09/2018	<input type="checkbox"/> User					
<input type="checkbox"/> Show Image		<input checked="" type="checkbox"/> Device ID	SERVIDORES[172.20.165]	<input type="checkbox"/> Network Log			
Date	Device ID	Device	Event	T&A Event	User ID	User	S.
2018-09-19 08:01:28	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 08:04:57	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 08:04:57	543611728	SERVIDORES[...]	Identify Success		63452456	RINCON CONT...	
2018-09-19 08:05:00	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 08:08:27	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 08:08:27	543611728	SERVIDORES[...]	Identify Success		13178446	SANTIAGO QUI...	
2018-09-19 08:08:31	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 08:09:12	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 08:09:12	543611728	SERVIDORES[...]	Identify Success		37182668	FORERO BLAN...	
2018-09-19 08:09:15	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 08:10:21	543611728	SERVIDORES[...]	Identify Fail				
2018-09-19 08:10:23	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 08:10:23	543611728	SERVIDORES[...]	Verify Success(Card ...		91523861	ZAMBRANO Z...	
2018-09-19 08:10:26	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 08:46:57	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 08:46:57	543611728	SERVIDORES[...]	Identify Success		13176447	MOLINA ANG...	
2018-09-19 08:47:00	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 10:24:58	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 10:24:58	543611728	SERVIDORES[...]	Identify Success		13177782	ALVERNIA ACE...	
2018-09-19 10:25:01	543611728	SERVIDORES[...]	Door Relay Off				
2018-09-19 10:25:42	543611728	SERVIDORES[...]	Door Relay On				
2018-09-19 10:25:42	543611728	SERVIDORES[...]	Identify Success		88280546	GARCIA BARRE...	
2018-09-19 10:25:45	543611728	SERVIDORES[...]	Door Relay Off				

**Figura 51. Asistencia sala de servidores, Fuente autor, software Biostar.**

Door/Zone Monitoring		Realtime Monitoring		Log List			
Period	10/07/2018	<input type="checkbox"/> Event	Priority 0	<input type="button" value="Get Log"/>	<input type="button" value="Clear"/>		
~	28/09/2018	<input type="checkbox"/> User					
<input type="checkbox"/> Show Image		<input checked="" type="checkbox"/> Device ID	SC-CS[172.20.165.19]	<input type="checkbox"/> Network Log			
Date	Device ID	Device	Event	T...	User ID	User	St...
2018-07-26 16:37:49	543611735	SC-CS[172.20....	Time Change				
2018-07-26 16:40:45	543611735	SC-CS[172.20....	Door Relay On				
2018-07-26 16:40:45	543611735	SC-CS[172.20....	Identify Success		13178446	SANTIAGO QUINTERO ARLEY	
2018-07-26 16:40:48	543611735	SC-CS[172.20....	Door Relay Off				
2018-07-26 16:40:53	543611735	SC-CS[172.20....	Door Relay On				
2018-07-26 16:40:53	543611735	SC-CS[172.20....	Identify Success		13178446	SANTIAGO QUINTERO ARLEY	
2018-07-26 16:40:56	543611735	SC-CS[172.20....	Door Relay Off				
2018-07-26 16:41:05	543611735	SC-CS[172.20....	Door Relay On				
2018-07-26 16:41:05	543611735	SC-CS[172.20....	Identify Success		13178446	SANTIAGO QUINTERO ARLEY	
2018-07-26 16:41:08	543611735	SC-CS[172.20....	Door Relay Off				
2018-07-26 16:41:24	543611735	SC-CS[172.20....	Door Relay On				
2018-07-26 16:41:24	543611735	SC-CS[172.20....	Identify Success		13178446	SANTIAGO QUINTERO ARLEY	
2018-07-26 16:41:27	543611735	SC-CS[172.20....	Door Relay Off				
2018-07-26 16:41:50	543611735	SC-CS[172.20....	Door Relay On				
2018-07-26 16:41:50	543611735	SC-CS[172.20....	Identify Success		13178446	SANTIAGO QUINTERO ARLEY	
2018-07-26 16:41:53	543611735	SC-CS[172.20....	Door Relay Off				
2018-07-26 16:42:22	543611735	SC-CS[172.20....	Identify Fail				
2018-07-27 00:25:29	543611735	SC-CS[172.20....	Server Socket Disco...				
2018-07-27 00:25:30	543611735	SC-CS[172.20....	IP Initializing				
2018-07-27 00:25:34	543611735	SC-CS[172.20....	Server Socket Conn...				
2018-07-27 01:59:06	543611735	SC-CS[172.20....	Server Socket Conn...				
2018-07-27 07:04:34	543611735	SC-CS[172.20....	Identify Fail				
2018-07-27 08:37:42	543611735	SC-CS[172.20....	Identify Fail				

**Figura 52. Prueba de funcionamiento asistencia sala de cómputo comunicación social. Fuente autor, software Biostar.**

### 5.6.1. Emparejar patrones biométricos con horarios y otorgar permisos a los docentes

Ver apéndice B.

### **5.7. Instalar el sistema de control en la sala de servidores y comunicación social de la Universidad Francisco de Paula Santander Ocaña.**

En esta fase de desarrollo se implementó el lector biométrico con sus respectivos complementos para su funcionamiento, este proceso de implementación dio como muestra el comportamiento de este dispositivo a la hora de permitir el acceso al área de sala de servidores y comunicación social.



**Figura 53. Sensor en estado pendiente, sala de servidores. Fuente autor.**



**Figura 54. Sensor apagado, sala comunicación social. Fuente**

El sensor advierte si el usuario ha sido identificado, no ha sido identificado o está en espera por medio de su led en la parte superior.

**Tabla 2 Funciones por color del lector biométrico Bioentry W.**

COLOR DEL LED	DESCRIPCIÓN DE FUNCIONAMIENTO DEL COLOR
Led azul	Estado en espera.
Led purpura	Leyendo identificación Biométrica o HID.
Led rojo	Usuario no permitido o usuario no identificado.
Led verde	Usuario identificado o control de acceso concedido.

**Nota:** La tabla indica los cuatro estados posibles que el usuario podrá observar en el uso de este dispositivo.



**Figura 55. Usuario no identificado o acceso no permitido, sala de servidores. Fuente autor.**

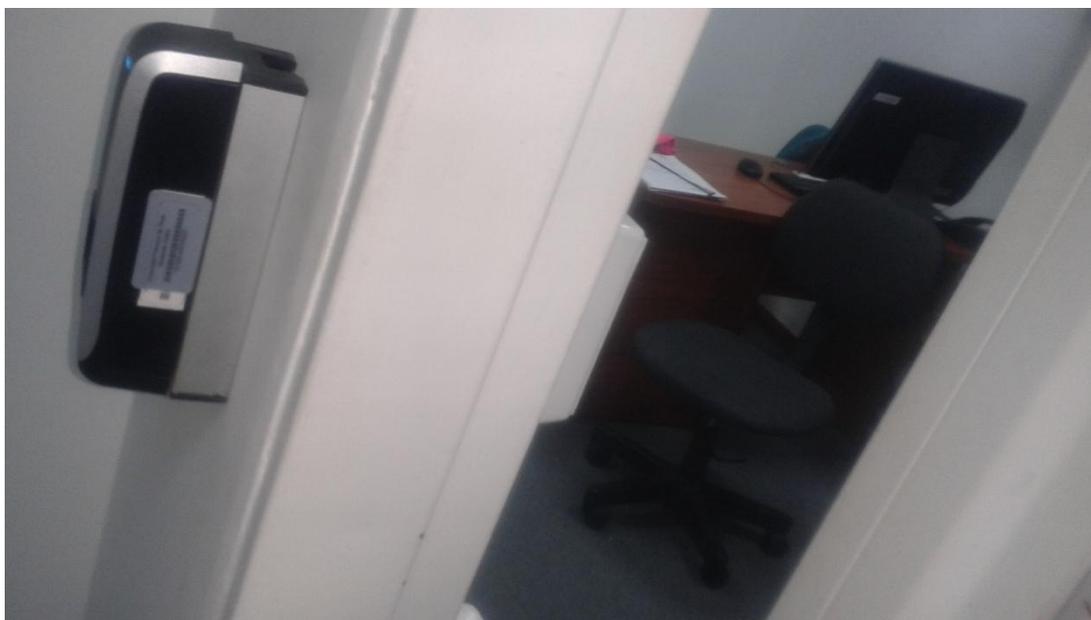


**Figura 56. Sensor escaneando huella, sala de servidores. Fuente autor.**



**Figura 57. Usuario autenticado o acceso permitido, sala de servidores. Fuente autor.**

En el momento donde la huella fue ingresada, escaneada y verificada el sistema otorga el acceso a la sala enviando una señal a la cerradura con electroimán instalado en la puerta y concede el acceso.



**Figura 58. Acceso entrada permitido. Fuente Autor.**

Para poder dar la salida de la sala se instaló un botón press de pánico.



**Figura 59. Botón del pánico, sala de servidores. Fuente autor.**



**Figura 60.** Botón del pánico, sala de comunicación social. Fuente autor.



**Figura 61.** Botón de pánico y funcionamiento. Fuente autor.

Al momento de instalar y comprobar el funcionamiento óptimo de los dispositivos en conjunto se desarrolla una descripción de la manera en cómo se deben conectar estos aparatos

electrónicos para su funcionamiento, desde la conexión a un switch hasta la configuración electrónica de sus componentes. **Ver apéndice C**

## **CAPÍTULO 6: Conclusiones**

La automatización de procesos y la filosofía Smart campus mediante el desarrollo e implementación de un sistema de control y monitoreo de asistencia a las salas de cómputo de la Universidad Francisco de Paula Santander Ocaña permitió concluir que:

Teniendo como base los requisitos funcionales sobre el uso de los lectores biométricos BIOENTRY W se logró definir un modelo entidad relación que permite el entendimiento del funcionamiento interno en la base de datos sin generar redundancia de información con el software de administración de dispositivos BIOSTAR.

Al definir el modelo entidad relación permitimos aumentar la congruencia de la información dado que al tener todos los datos que se almacenaran establecidos permite aplicar una normalización de la base de datos reduciendo así la redundancia de la información y mejorando la integridad de los datos.

Con la implantación de un sistema que permite interactuar con los datos y dada la cantidad de información suministrada por la base de datos con el sistema BIOSTAR y los lectores biométricos ubicados en la sala de servidores y sala de comunicación social se permite demostrar que los tiempos en la toma de información referente a los tiempo de llegada de los docentes se reducen, al solo tener que observar estos datos en el sistema y por ende la apertura de estas salas que se hace de manera automática.

Este trabajo está encaminado a la optimización de procesos en este caso la toma de datos de los docentes mediante informes de asistencia y apertura de salas, dado que la Universidad Francisco de Paula Santander Ocaña está aumentando de personal y de recurso material, como lo es el edificio de ingeniería, se busca poner en practica la automatización de procesos por medio del Smart campus.

Al momento de instalar los lectores biométricos se revela un importante comportamiento de la corriente dependiendo de la distancia que se encuentre la fuente de poder del dispositivo con la puerta si la distancia es mayor la potencia varía dependiendo de qué cableado se está utilizando, mientras que si la distancia es menor la potencia con la que llega la energía es constante.

Al implementar el proyecto con una metodología descriptiva y tomando como referencia los resultados de las encuestas, se sitúa la relación con la gestión de ingreso y monitoreo a las aulas de cómputo, no como un hecho aislado o de poco interés, si como como un inconveniente a la que se le debe proporcionar el debido trato dado el crecimiento de los procesos he infraestructura de la Universidad Francisco de Paula Santander Ocaña.

Los sistemas de automatización de procesos y la ideología Smart campus aún no están completamente implementadas en las universidades pero si se toma a la tarea de aplicar esta filosofía se puede mejorar en gran medida la eficiencia y eficacia de los procesos dentro de los entes, en este caso la universidad Francisco de Paula Santander Ocaña.

## Referencias Bibliográficas

- Aguilar, L. J. (2016). *Big Data, Análisis de grandes volúmenes de datos en organizaciones*. Alfaomega Grupo Editor.
- Almenara, J. C. (1998). *Impacto de las nuevas tecnologías de la información y la comunicación en las organizaciones educativas*. Grupo Editorial Universitaria.
- AMETIC, (2013). Foro TIC para la sostenibilidad. Recuperado de:  
[http://dg6223fhel5c2.cloudfront.net/PD/wp-content/uploads/2014/06/Informe\\_Smart\\_Cities.pdf](http://dg6223fhel5c2.cloudfront.net/PD/wp-content/uploads/2014/06/Informe_Smart_Cities.pdf)
- Arrieta, A., Marín, J., Sánchez, L. G., Romero, L., Sánchez, L. A., & Batista, V. *Gestión y Reconocimiento Óptico de los Puntos Característicos de Imágenes de Huellas Dactilares*. Universidad de Salamanca.
- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15), 2787-2805.
- Borja, C. T., & Bueno, Á. G. *Sistemas Biométricos*. Disponible en internet: [http://www.dsi.uclm.es/asignaturas/42635/web\\_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf](http://www.dsi.uclm.es/asignaturas/42635/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf).
- Coll, C. (Ed.). (2008). *Psicología de la educación virtual: aprender y enseñar con las tecnologías de la información y la comunicación*. Ediciones Morata.
- Congreso de la república. (2008). *Ley estatutaria 1266*. Recuperado de [http://www.secretariassenado.gov.co/senado/basedoc/ley\\_1266\\_2008.html](http://www.secretariassenado.gov.co/senado/basedoc/ley_1266_2008.html)
- Duró, V. E. (2001). *Evaluación de sistemas de reconocimiento biométrico*. Departamento de Electrónica y Automática. Escuela Universitaria Politécnica de Mataró.
- Enerlis, F. S. Ernst & Young & Madrid Network.(2012). *Libro Blanco, Smart Cities*. recuperado de: [http://www.innopro.es/pdfs/libro\\_blanco\\_smart\\_cities.pdf](http://www.innopro.es/pdfs/libro_blanco_smart_cities.pdf)
- Etchart, G., Luna, L., Leal, C., Benedetto, M. G., & Alvez, C. E. (2011). *Sistemas de reconocimiento biométricos, importancia del uso de estándares en entes estatales*. In XIII Workshop de Investigadores en Ciencias de la Computación.
- Galton, F. (1904). *Eugenics: Its definition, scope, and aims*. *American Journal of Sociology*,

- 10(1), 1-25.
- Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. (2007). Smart cities. Ranking of European medium-sized cities, Final Report, Centre of Regional Science, Vienna UT.
- Harrison, C., & Donnelly, I. A. (2011, September). A theory of smart cities. In Proceedings of the 55th Annual Meeting of the ISSS-2011, Hull, UK.
- Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. Proceedings of the IEEE, 85(9), 1365-1388.
- Laudon, F., & Laudon, J. (1996). Sistemas de Información. Editorial Diana, México.
- Liñan A., Vives A., Zennaro M. (2015). Internet de las cosas. Recuperado de: <http://wireless.ictp.it/Papers/InternetdelasCosas.pdf>
- Maza Figueroa, N. P., Orozco Acevedo, M. A., & Ospino Pinedo, M. E. D. (2017). Modelo de gestión estratégica para el desarrollo de un campus inteligente basado en conceptos de Smart City en la Universidad de Cartagena-Campus Piedra de Bolívar (Doctoral dissertation, Universidad de Cartagena).
- Meneses, A. J., & García, C. G. (2016). Diseño e Implementación de un Prototipo para el Control de Acceso en la Sede de Ingeniería de la Universidad Distrital Francisco José de Caldas Mediante el Uso de Torniquetes Controlados por Carnet con Tecnología NFC y Lector Biométrico de Huella Dactilar.
- Miller, B. (1994). Vital signs of identity [biometrics]. IEEE spectrum, 31(2), 22-30.
- Ministerio de educación nacional. (2009). Ley 1286. Recuperado de <http://www.mineducacion.gov.co/1759/w3-article-186955.html>
- Ministerio de tecnologías de la información y las comunicaciones de Colombia. (2009). Ley 1341. Recuperado de <http://www.mintic.gov.co/portal/604/w3-article-3707.html>
- ORACLE, (2016). An Enterprise Architect's Guide to Big Data. Recuperado de: <http://www.oracle.com/technetwork/topics/entarch/articles/oea-big-data-guide-1522052.pdf>
- Sáenz Leguizamón, J. A. Implementación de un sistema de seguridad para las comunicaciones en medidores inteligentes de baja tensión en Smart Grids (Doctoral dissertation, Universidad Nacional de Colombia-Bogotá)

- Serratosa, F. (2008). La biometría para la identificación de las personas. Universitat Oberta de Catalunya, 8-20.
- Shoup, D. (2006). Parking on a smart campus. California Policy Options.
- Supo, J. (2012). Seminarios de investigación científica. Tipos de investigación.
- Telefónica, F. (2011). Smart Cities: un primer paso hacia la Internet de las Cosas (Vol. 16). Fundación Telefónica.
- The Broadband Internet Technical Advisory Group, BITAG. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Recuperado de:  
[https://www.bitag.org/documents/BITAG\\_Report\\_-\\_Internet\\_of\\_Things\\_\(IoT\)\\_Security\\_and\\_Privacy\\_Recommendations.pdf](https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf)
- Universidad de Alicante. (2015). UA Smart University. Recuperado de:  
<https://web.ua.es/es/smart/smart-university-hacia-una-universidad-mas-abierta-universidad-de-alicante.html>.
- Van Dalen, D. B., & Meyer, W. J. (2006). Síntesis de" Estrategia de la investigación descriptiva. Manual de técnica de la investigación educacional.
- VARGAS, A. M., & DE LA SEGURIDAD, E. E. A. Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida.
- Zorita, D. S., & García, J. O. (2003). Reconocimiento automático mediante patrones biométricos de huella dactilar. D. Simón Zorita

## Apéndice

### Apéndice A: Encuesta realizada a los docentes de la Universidad Francisco de Paula Santander Ocaña utilizando la plataforma encuesta.ufpso.edu.co.



**Encuestas**

UFPSO  
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER  
OCAÑA

Universidad  
Francisco de Paula Santander  
Ocaña

Aviso: La ejecución de JavaScript está deshabilitada en su navegador. Es posible que no pueda responder todas las preguntas de la encuesta. Por favor, verifique la configuración de su navegador.

**Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO**

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

Por favor responder de la manera más honesta posible.

Hay 6 preguntas en esta encuesta.

Cargar encuesta sin terminar      Siguiente      Click me to open modal

Figura 62. Portada encuesta docente UFPSO. Fuente autor del proyecto.



**Encuestas**

UFPSO  
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER  
OCAÑA

Universidad  
Francisco de Paula Santander  
Ocaña

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

0%

Encuesta de fiabilidad en la implementación

**Con que frecuencia realiza clases en las salas de cómputo**

Marque las opciones que correspondan

1 - 2 veces a la semana

3 - 4 veces a la semana

4 - 6 veces a la semana

Más de 8 veces

Nunca

Continuar después      Siguiente      Click me to open modal

Figura 63. Pregunta uno, encuesta UFPSO. Fuente autor del proyecto.

**Encuestas**

**Universidad Francisco de Paula Santander Ocaña**

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

16%

Encuesta de fiabilidad en la implementación

**Aproximadamente cuantos minutos espera para que los encargados de las salas le de ingreso**

Marque las opciones que correspondan

- 2 - 5 minutos
- 5 - 10 minutos
- Más de 10 minutos

Continuar después      Siguiente ▶      Click me to open modal

**Figura 64. Pregunta dos, encuesta UFPSO. Fuente autor del proyecto.**

**Encuestas**

**Universidad Francisco de Paula Santander Ocaña**

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

33%

Encuesta de fiabilidad en la implementación

**Cómo calificaría los medios de comprobación de asistencia a las clases existentes en la Universidad Francisco de Paula Santander Ocaña**

Seleccione una de las siguientes opciones

- Muy bueno
- Bueno
- Regular
- Malo
- Muy malo

Continuar después      Siguiente ▶      Click me to open modal

**Figura 65. Pregunta tres, encuesta UFPSO. Fuente autor del proyecto.**



**Encuestas**

**UFPSO**  
AVEL PORO DE VOUS  
OCAÑA

**Universidad**  
Francisco de Paula Santander  
OCAÑA

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

50%

Encuesta de fiabilidad en la implementación

**Encuentra factible que al momento de ingresar a la sala se almacene su hora de llegada a estas**

Seleccione una de las siguientes opciones

Si

No

Por favor, escriba la justificación de su respuesta aquí:

Continuar después      Siguiente ▶      Click me to open modal

**Figura 66. Pregunta cuatro, encuesta UFPSO. Fuente autor del proyecto.**



**Encuestas**

**UFPSO**  
AVEL PORO DE VOUS  
OCAÑA

**Universidad**  
Francisco de Paula Santander  
OCAÑA

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

66%

Encuesta de fiabilidad en la implementación

**Encuentra viable la implementación de un sistema de control y monitoreo a las salas de computo de la Universidad Francisco de Paula Santander Ocaña**

Seleccione una de las siguientes opciones

Si

No

Por favor, escriba la justificación de su respuesta aquí:

Continuar después      Siguiente ▶      Click me to open modal

**Figura 67. Pregunta cinco, encuesta UFPSO. Fuente autor del proyecto.**



**Encuestas**

**UFPSO**  
AVILA RUIRO DE TOSOS,  
OCAÑA

**Universidad**  
Francisco de Paula Santander  
OCAÑA

Encuesta realizada para mostrar la importancia de la implementación del control de acceso a las salas de cómputo en la UFPSO

DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL Y MONITOREO DE ASISTENCIA A LAS SALAS DE CÓMPUTO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

83%

Encuesta de fiabilidad en la implementación

**Que tan bueno encuentra la implementación de un dispositivo que por medio de su huella permita el ingreso automático a la salas de cómputo**

Seleccione una de las siguientes opciones

- Muy bueno
- Bueno
- Regular
- Malo
- Muy malo

Continuar después      Enviar      Click me to open modal

**Figura 68. Pregunta seis, encuesta UFPSO. Fuente autor del proyecto.**

## Apéndice B: Guía de uso

Esta guía de configuración se centrará en el manejo de la plataforma Biostar para el control y monitoreo de las salas de computo. Esta muestra la manera en cómo se deben configurar las puertas lógicas que son las que permiten el manejo independiente de las salas de computo, la asignación de lectores biométricos como la creación y asignación de los horarios en los grupos de accesos los cuales son los que permiten el ingreso o logueo a las salas de computo.

- **Paso uno: entrada al sistema de información Biostar**

El equipo que desee ingresar debe tener los permisos que son asignados por los encargados de sala de servidores también debe estar en la misma red lógica que se encuentre el servidor del sistema Biostar. Para el ingreso debe utilizar la IP asignada al servidor como se muestra en la imagen.

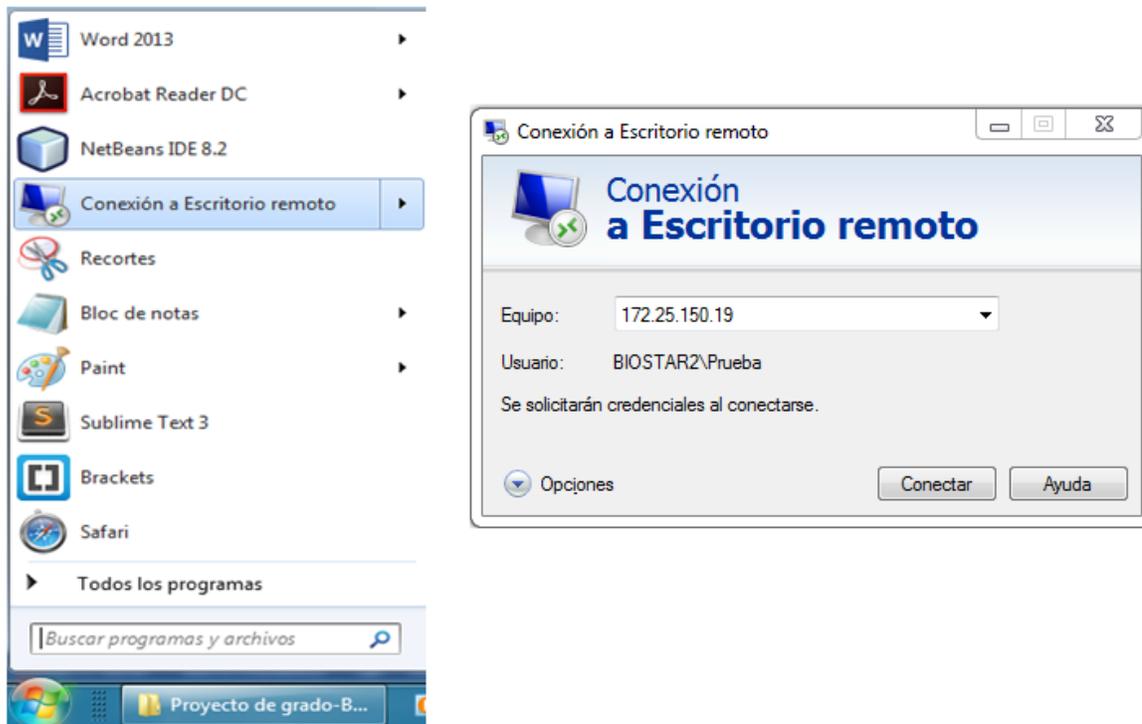
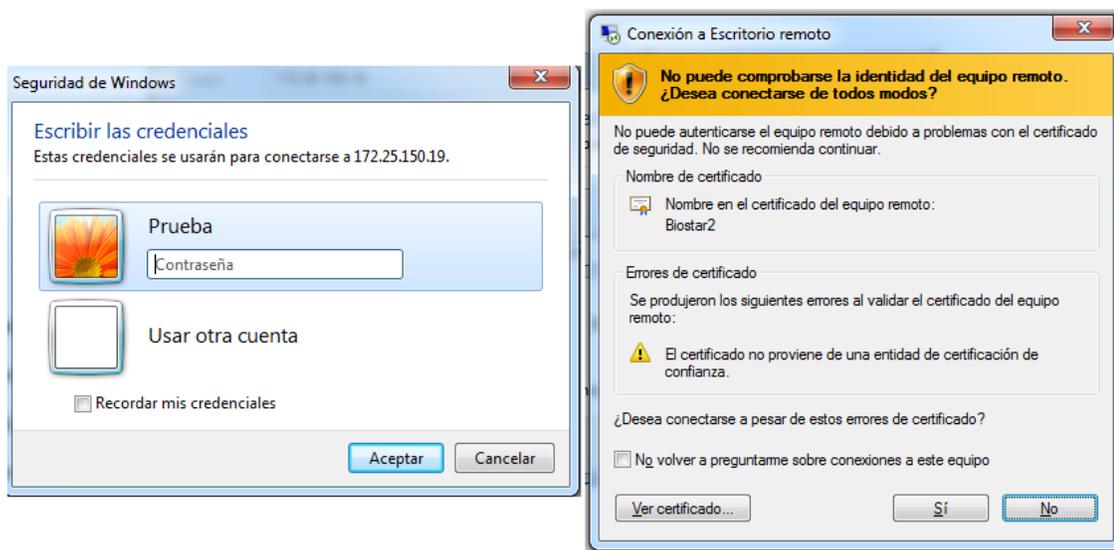


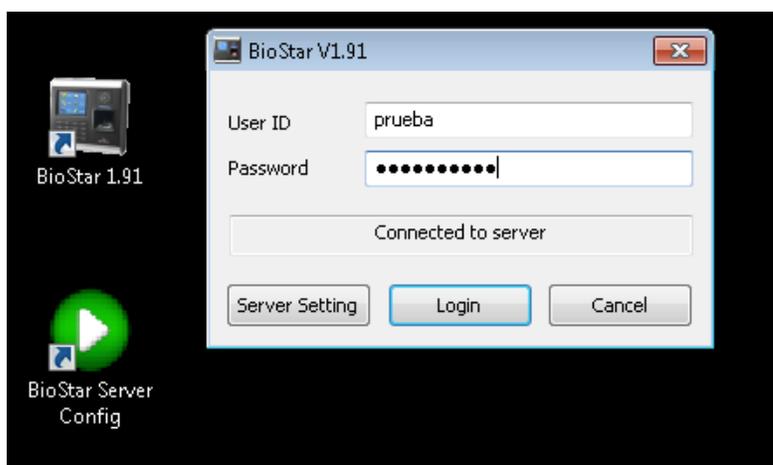
Figura 69. Conexión a escritorio remoto. Fuente autor del proyecto

Al momento de ingresar la IP asignada al servidor se mostrara una ventada que solicitara la contraseña de ingreso, al digitarla y desear entrar el sistema muestra una ventana emergente que contiene una pregunta sobre el certificado de seguridad la cual se debe seleccionar la respuesta sí.



**Figura 70. Ventada de contraseña y certificado de seguridad. Fuente autor del proyecto.**

Al momento de seleccionar la opción si se abre una ventada donde aparecerá el programa Biostar, dando doble clic abrimos el programa y este nos muestra una ventana de logueo que es la que nos permite estar en la interfaz de usuario del sistema



**Figura 71. Ventana de logueo interfaz Biostar. Fuente autor del proyecto.**

Al ingresar a la plataforma BioEntry muestra la siguiente interfaz, donde están los usuarios que posee en la base de datos y los diferentes menús de interacción.

User ID	Name	Department	Email	Telephone	Start Date	Expire Date	Admin Level
91256235	GELVES BAUTISTA J...	G2_ALUMNOS	jgelvesb@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
37336988	BECERRA PINEDA G...	G2_ALUMNOS	gbecerrap@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091664062	RAMIREZ LOPEZ LY...	G2_ALUMNOS	llramirezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063958014	SOCARRAS MUÑOZ...	G2_ALUMNOS	aasocarrasm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091665409	MERCHAN SALAZA...	G2_ALUMNOS	cmERCHANTS@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1123203009	GOMEZ GAVIRIA DL...	G2_ALUMNOS	dmgomezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091662991	ROJAS MEDINA SA...	G2_ALUMNOS	sprojasrm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1003115382	RAMIREZ ARIAS JOR...	G2_ALUMNOS	jiramireza@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091665494	CARRASCAL GAON...	G2_ALUMNOS	gscarrascalg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065884012	JIMENEZ BOTELLO ...	G2_ALUMNOS	djimenezb@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091668777	RINCON RODRIGUE...	G2_ALUMNOS	mjinconr@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064837485	FLOREZ GOMEZ JOS...	G2_ALUMNOS	jfflorezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1082936327	SAMPER OSORIO R...	G2_ALUMNOS	rrsamper@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091660731	BUSTAMANTE PINE...	G2_ALUMNOS	cabustamante@ufpso.edu...		2000-01-01	2030-12-31 23	Normal User
1096210155	CRUZ LOPEZ JORGE...	G2_ALUMNOS	jacruzl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065891686	ORTIZ GUZMAN KA...	G2_ALUMNOS	ktortizg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1094576984	TORRADO ASCANIL...	G2_ALUMNOS	mtorradoda@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064111315	RUIZ INDAURO GU...	G2_ALUMNOS	garuizl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065884813	CORONEL MANRIQ...	G2_ALUMNOS	mlcoronelm@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065885514	QUIÑONES QUIÑO...	G2_ALUMNOS	jpquionesq@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064796768	MACHADO CADEN...	G2_ALUMNOS	ymachadoc@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091664622	ALVAREZ LOBO AN...	G2_ALUMNOS	aalvarezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091665345	GRANADOS CORRE...	G2_ALUMNOS	jlganadosc@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091667806	MEDINA MORA VML...	G2_ALUMNOS	vmmedinam@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091662723	GARAY QUINTERO ...	G2_ALUMNOS	eegarciaq@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091664753	SANCHEZ GARCIA ...	G2_ALUMNOS	ysanchezg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065647323	NIETO DEL PORTIL...	G2_ALUMNOS	jlnietodp@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091667190	ROPERO NIÑO LEN...	G2_ALUMNOS	lbroperon@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1073236785	BENITEZ LOPEZ PA...	G2_ALUMNOS	pabenitezl@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063563584	RINCON SUAREZ S...	G2_ALUMNOS	srincon@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065889129	QUINTERO RODRIG...	G2_ALUMNOS	mmquinteror@ufpso.edu....		2000-01-01	2030-12-31 23	Normal User
1065888488	BONET MEJIA YEIN...	G2_ALUMNOS	klsanjuaans@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1063490890	CHINCHIA FUENTE...	G2_ALUMNOS	cachinchiaf@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1023880934	AYALA CASANOVA ...	G2_ALUMNOS	ryayalac@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064839630	SANABRIA PEREZ L...	G2_ALUMNOS	lisanabriap@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091668687	BUSTOS TRIGOS JUL...	G2_ALUMNOS	jabustot@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091665356	LANZZIANO RIQUE...	G2_ALUMNOS	jrlanzzianor@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1064839830	OSORIO GONZALES...	G2_ALUMNOS	ndosoriog@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1062909746	MENDOZA DURAN...	G2_ALUMNOS	ermendozad@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1091662495	NAVARRO TAMAY...	G2_ALUMNOS	pjnavarrot@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1065948001	RAPALINO MEJIA ES...	G2_ALUMNOS	earapalinom@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User
1001655696	ORTIZ GAVIRIA VEI...	G2_ALUMNOS	ortizg@ufpso.edu.co		2000-01-01	2030-12-31 23	Normal User

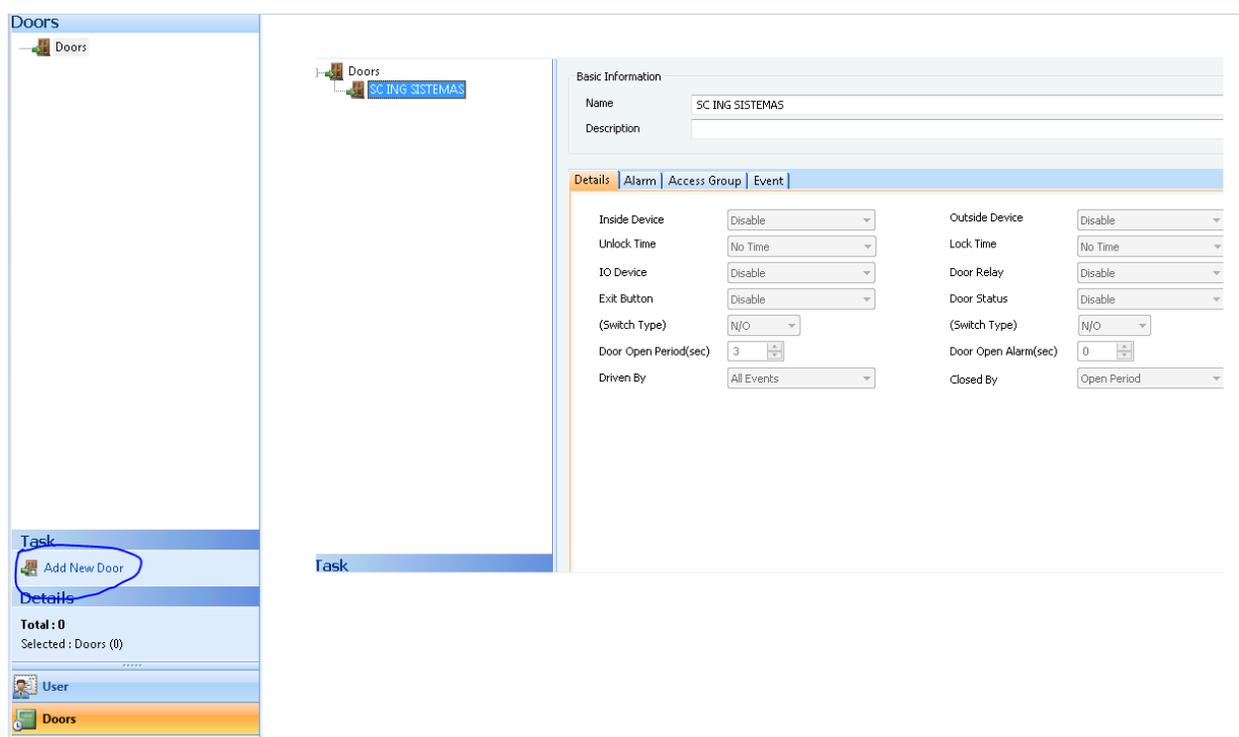
Figura 72. Interfaz de usuario inicial Biostar. Fuente autor del proyecto.

- **Pasó dos: Crear puertas lógicas y asignar los lectores biométricos.**

Como la información necesaria de los usuarios ya la posee la base de datos de la universidad, lo que viene a continuación es crear las puertas, horarios y grupos de acceso.

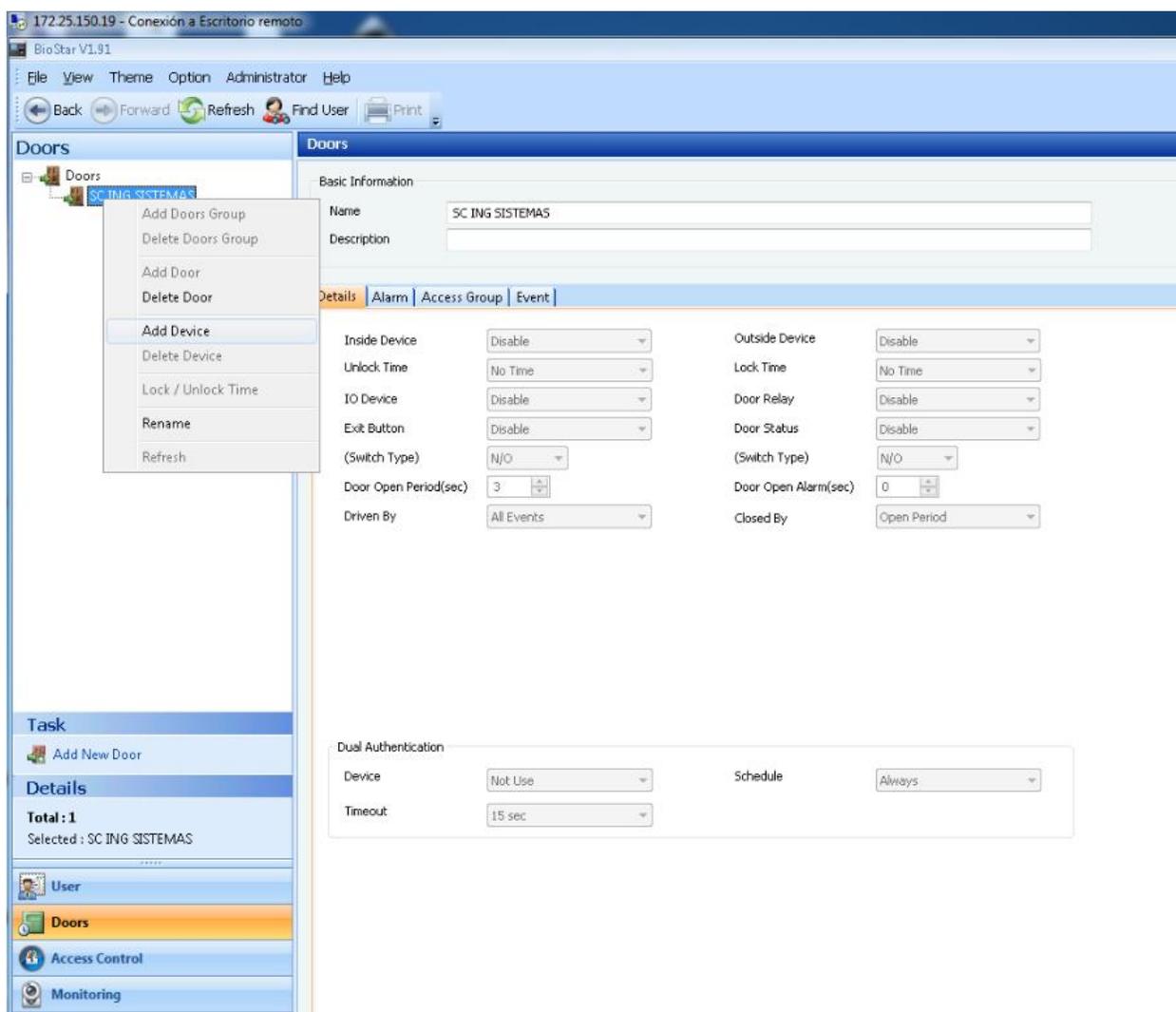
Para la creación de puertas lógicas en el menú de acciones (TASK) seleccionamos la pestaña Doors.

Esta nos muestra el menú de puertas donde podemos asignarle un nombre y agregar el dispositivo correspondiente a esta.



**Figura 73. Menú de creación y configuración de puertas. Fuente autor del proyecto.**

Después de crear la puerta lógica procedemos a asignar el lector biométrico correspondiente a la sala, utilizando el clic derecho se muestran distintas opciones a escoger donde seleccionamos Add Device.



**Figura 74. Asignando dispositivo a puerta lógica. Fuente autor del proyecto.**

Al seleccionar Add Device se muestra un árbol de dispositivos donde seleccionamos el dispositivo correspondiente a la puerta,

Para asignar el dispositivo a la puerta y que este tome la configuración que se le haga a la puerta en la pestaña IO device asignamos el dispositivo.

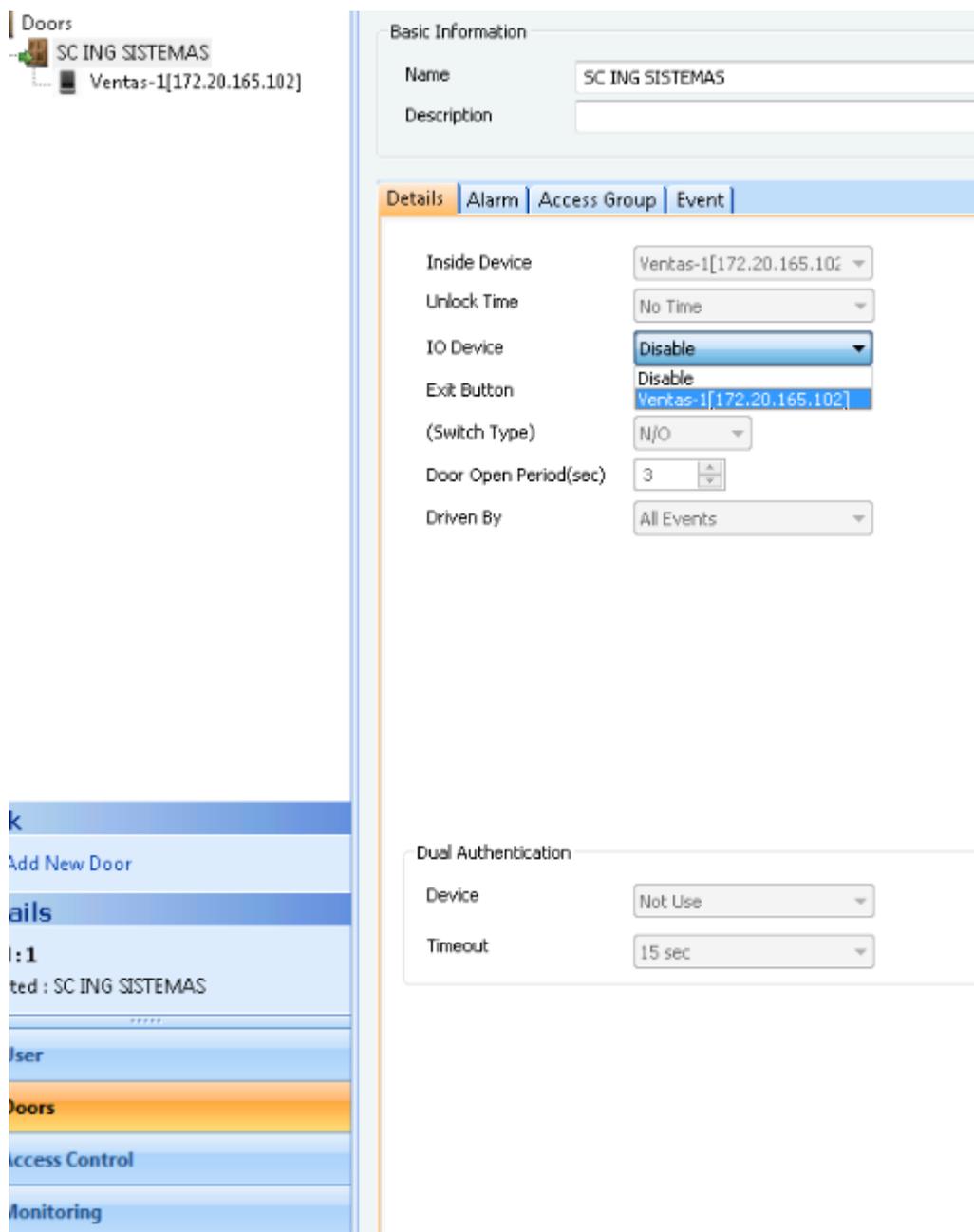
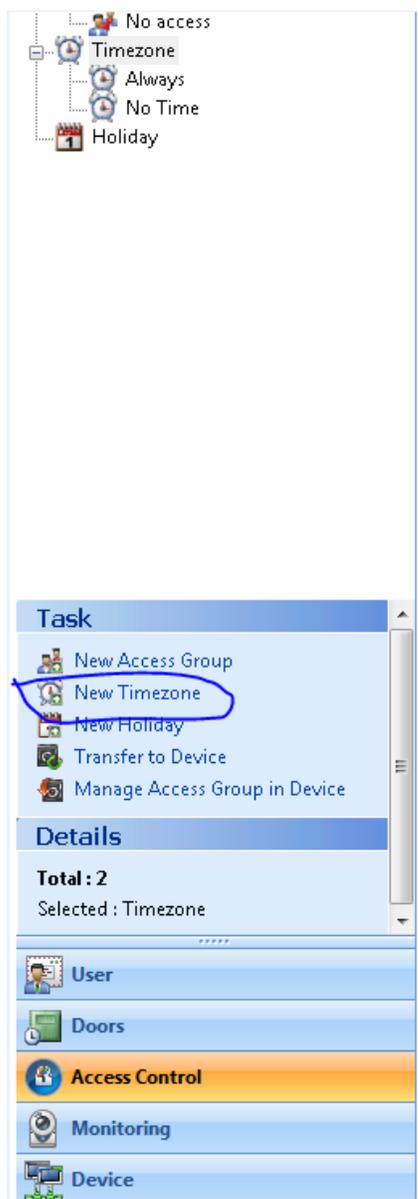


Figura 75. Asignación de dispositivo a puerta lógica. Fuente autor del proyecto.

- **Pasó tres: Crear Timezone (horarios).**

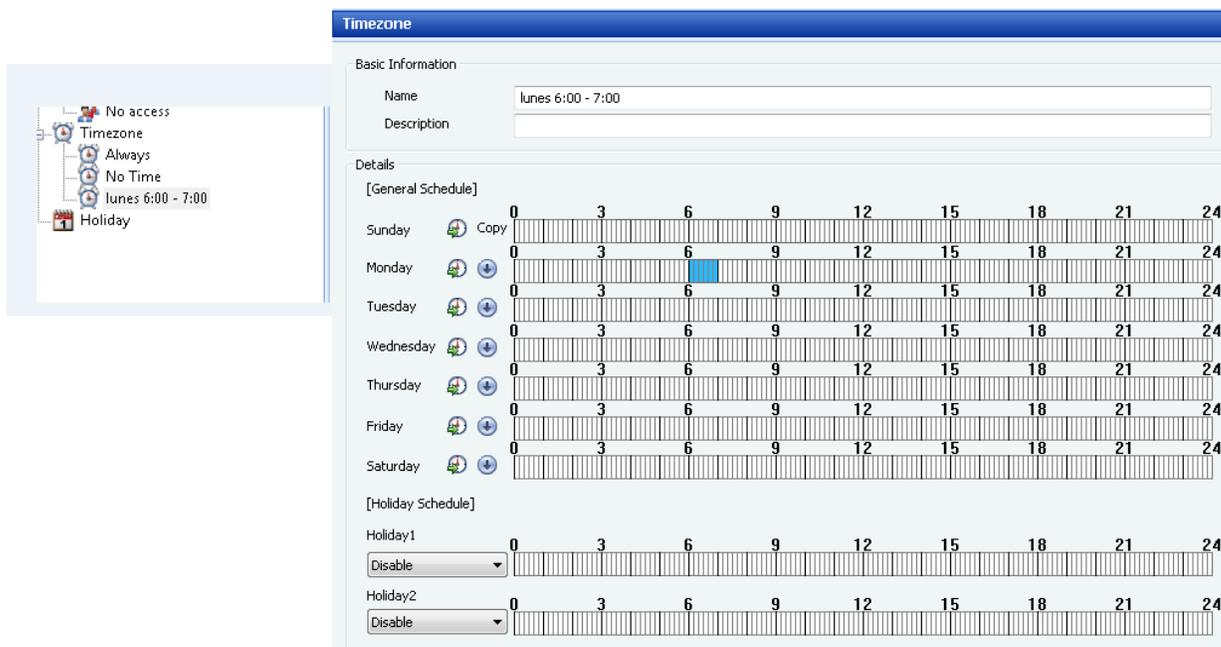
Para la asignación de los horarios se crean los Timezone que son los que contienen los diferentes tipos de horarios. Para crear un Timezone se va a la pestaña Monitoring.



**Figura 76. Menú administración de horarios. Fuente autor.**

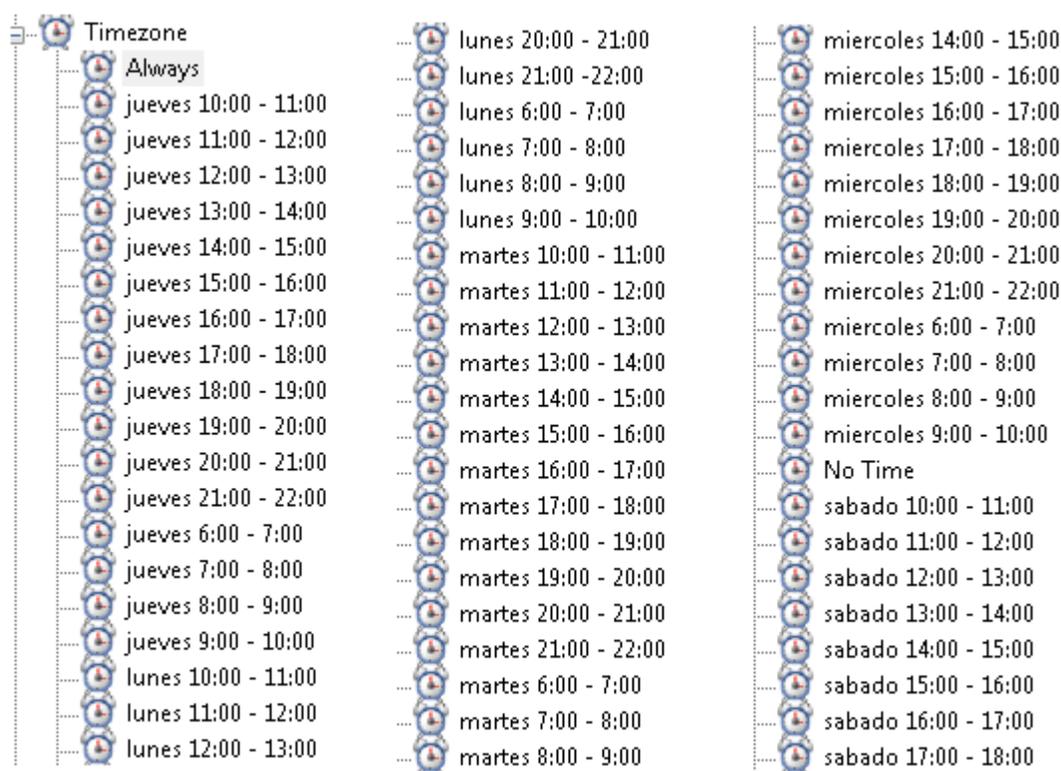
Para modificar los horarios este nos muestra una línea de tiempo donde podemos escoger que hora va a ser asignada o que grupo de horas son las que se necesitan según la labor.

Al momento de seleccionar New timezone podemos asignarle un nombre, una descripción y escoger en la línea de tiempo que horario va a cubrir.



**Figura 77. Horario con su respectiva línea de tiempo. Fuente autor del proyecto.**

Como el sistema de información del Bioentry solo permite crear 126 tipos de horario o timezone se crean los diferentes horarios por lapsos de una hora para que en total a la semana sean 112 horarios.

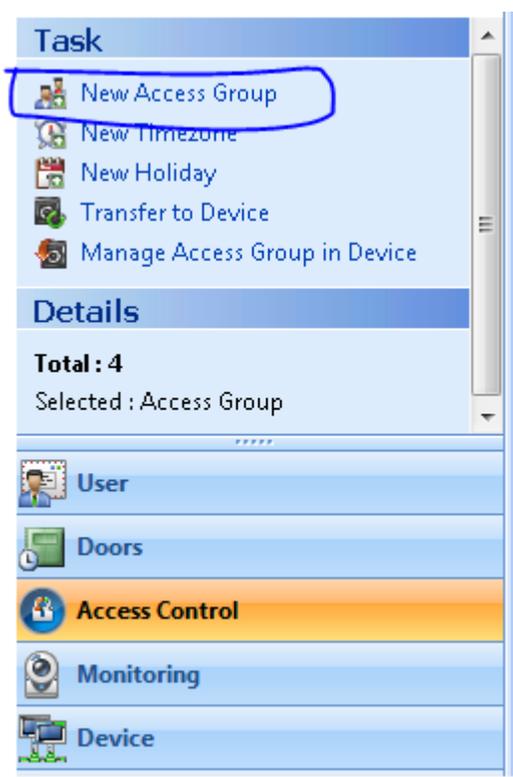


**Figura 78. Timezone creados por lapso de una hora. Fuente autor del proyecto.**

- **Pasó cuatro: Crear Access group (grupos de acceso).**

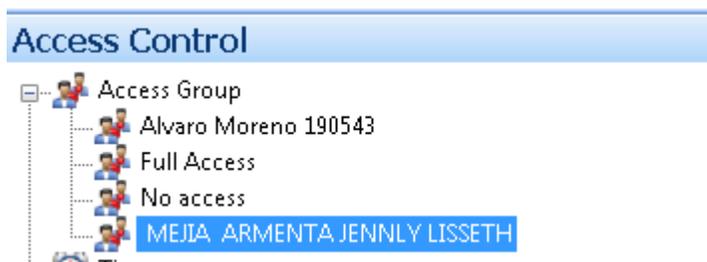
Para la asignación de los turnos o permisos de acceso a las salas se crean los grupos de acceso (access group) que son los que contienen la configuración necesaria para permitir a los usuarios el acceso en sus respectivas horas.

En la pestaña TASK ingresamos a Access control luego seleccionamos new Access group.



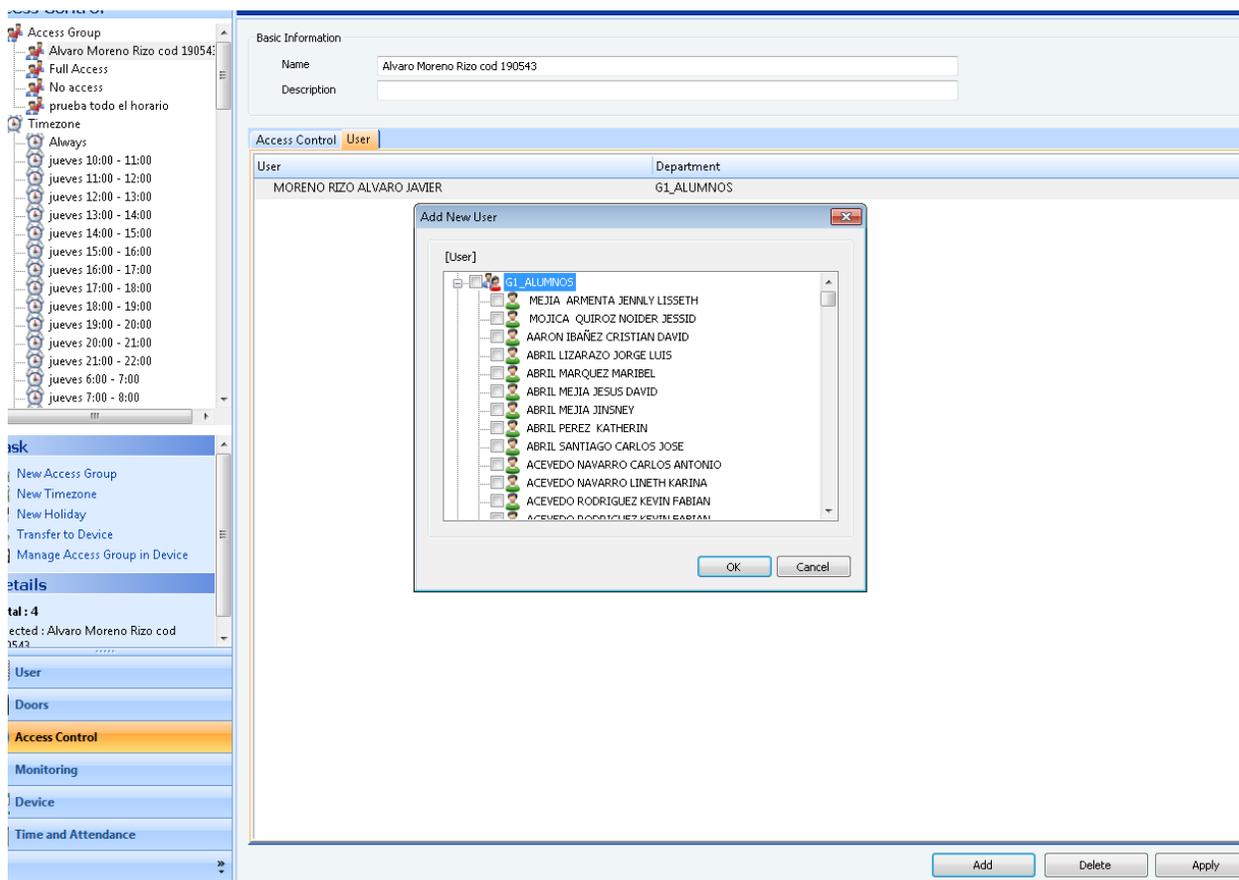
**Figura 79. Crear Access group. Fuente autor del proyecto.**

Al momento de crear el access group le asignamos un nombre. En este caso cada access group será un docente. En el desarrollo del proyecto se encontró que no se puede diferenciar en un solo Access group cual docente puede entrar a una hora determinada y cual no, de esta manera asignamos a un solo Access group un usuario que contenga sus diferentes horarios en las salas respectivas.



**Figura 80. Access group con nombre de usuario. Fuente autor del proyecto.**

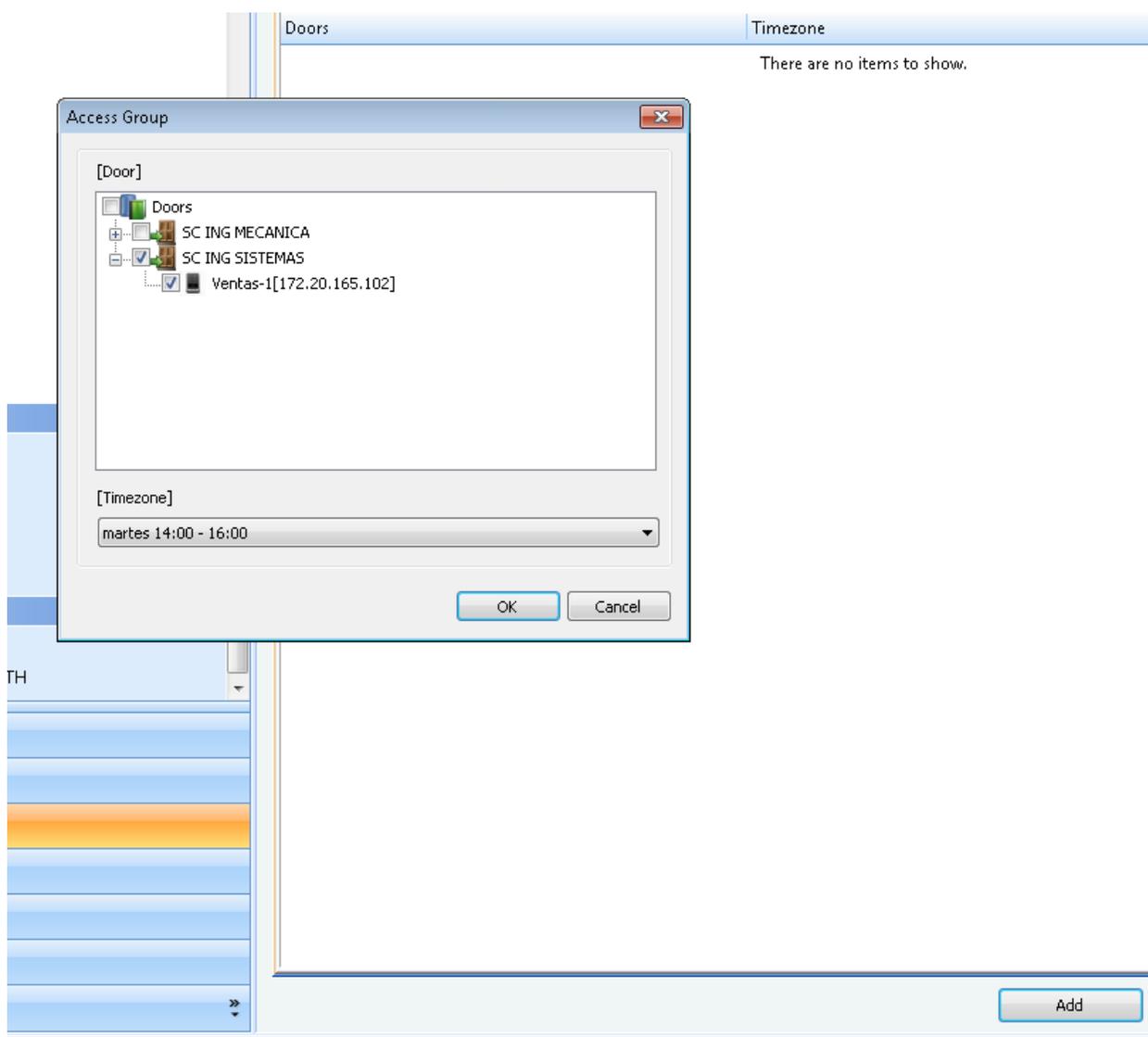
Para asignar un usuario al access group ya creado se selecciona el grupo de acceso y en la pestaña user se selecciona la opción add que muestra un árbol de los usuarios disponibles en la base de datos.



**Figura 81. Agregando usuario al grupo de acceso. Fuente autor del proyecto.**

Situado en el access group creado y ya asignado el usuario procedemos a darle los permisos de entrada por hora, el cual se hace seleccionando la pestaña access control, en esta seleccionamos add donde nos muestra un árbol con el listado de puertas disponibles seleccionamos la puerta donde el usuario tenga la clase y en la pestaña de abajo del árbol seleccionamos la hora en la que puede entrar.

**nota:** este proceso se repite puesto que las horas están divididas de una en una y la universidad posee bloques de horas de clase de hasta 3 horas consecutivas o más.



**Figura 82. Proceso de asignación de hora de entrada. Fuente autor del proyecto.**

Para almacenar la información en los dispositivos se debe transferir la información a estos,

esto se logra en el menú TASK en la opción Transfer to device.

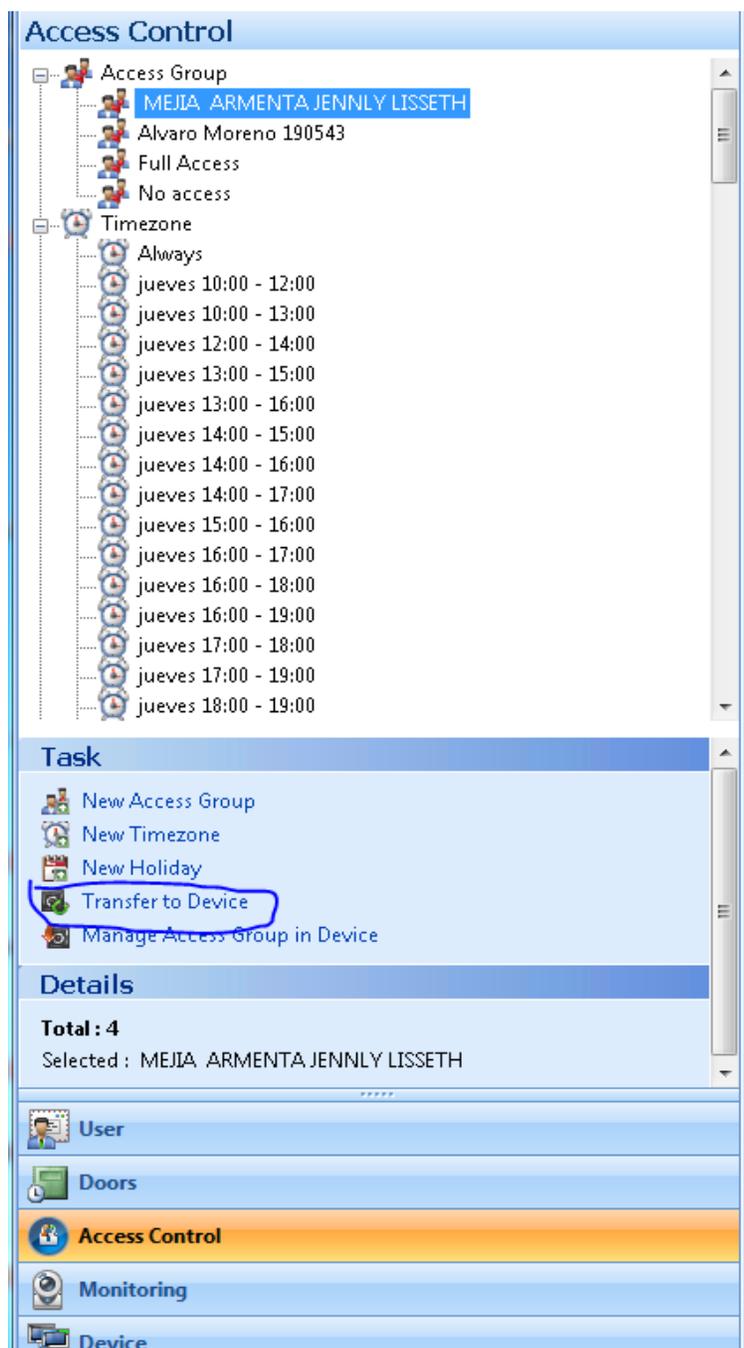


Figura 83. Manera en cómo se almacenan los cambios en el dispositivo. Fuente autor

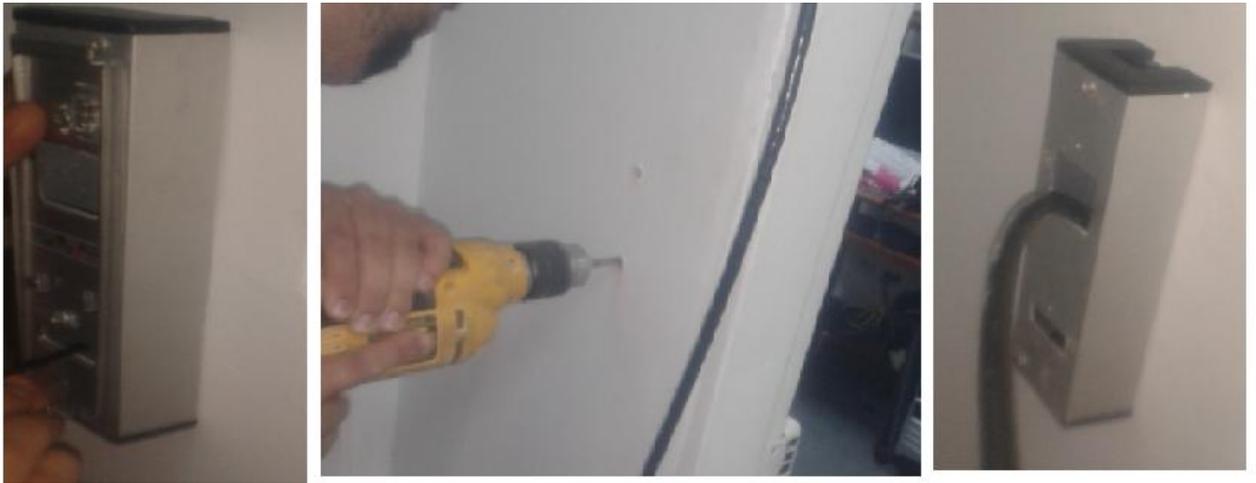
### Apéndice C: Conexión de componentes.

En esta sección se muestra la imagen referente al circuito guía creado para la instalación de

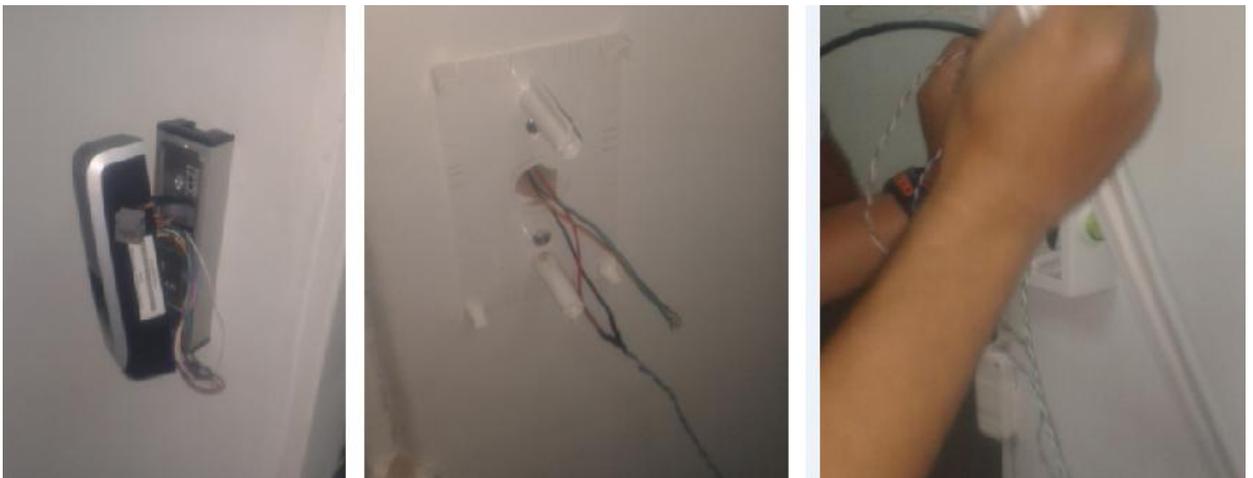
estos dispositivos con su imagen de respaldo del mundo real, resaltando la configuración de los dispositivos que se implementaron en este proyecto cabe recalcar el uso de IPV4 para la comunicación con el servidor. Como los lectores biométricos y los switch son topologías diferentes se usa un cable de conexión directa ya que si se implementa un cable cruzado no se genera ningún tipo de comunicación entre el servidor y el dispositivo.



**Figura 84. Cable UTP directo y switch. Fuente autor del proyecto.**



**Figura 85. Instalación caja de suspensión lector Bioentry W. Fuente autor del proyecto.**



**Figura 86. Instalación lector Bioentry W. Fuente autor del proyecto.**



**Figura 87. Instalación Electroimán. Fuente autor del proyecto.**



**Figura 88. Instalación soporte en puerta para barra metálica. Fuente autor del proyecto.**



Figura 89. Caja protectora de implementos. Fuente autor del proyecto.

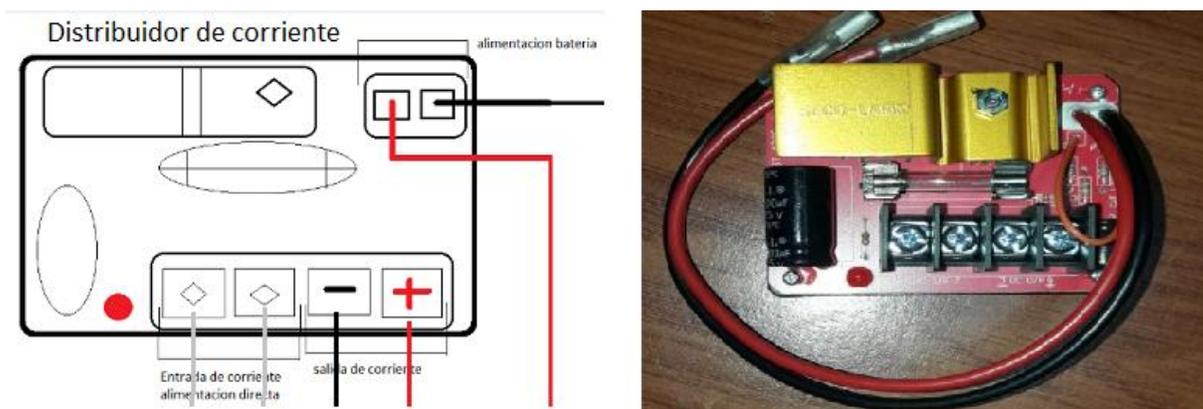


Figura 90. Distribuidor de corriente. Fuente autor del proyecto.

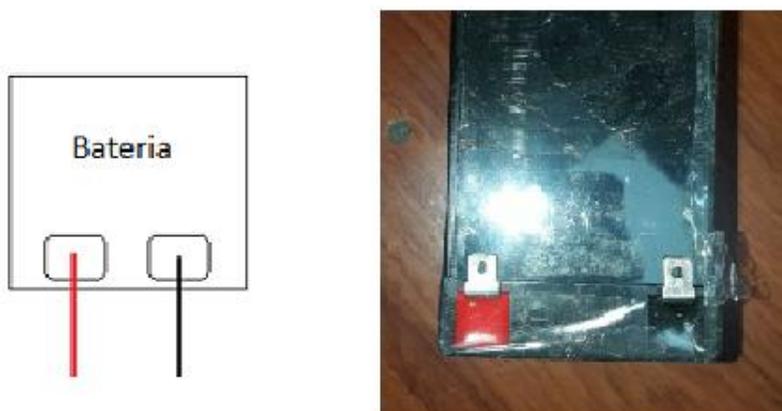


Figura 91. Batería. Fuente autor del proyecto.

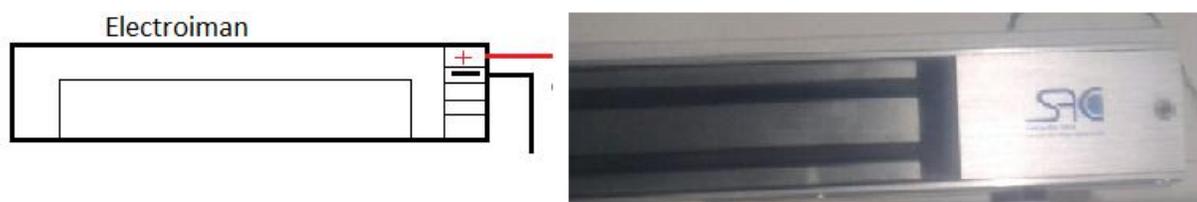


Figura 92. Electroimán. Fuente autor del proyecto.

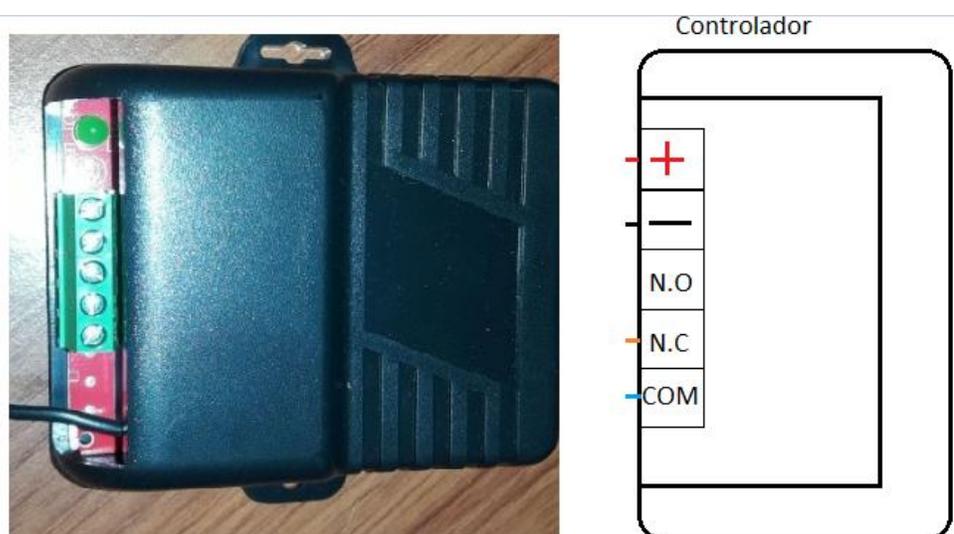
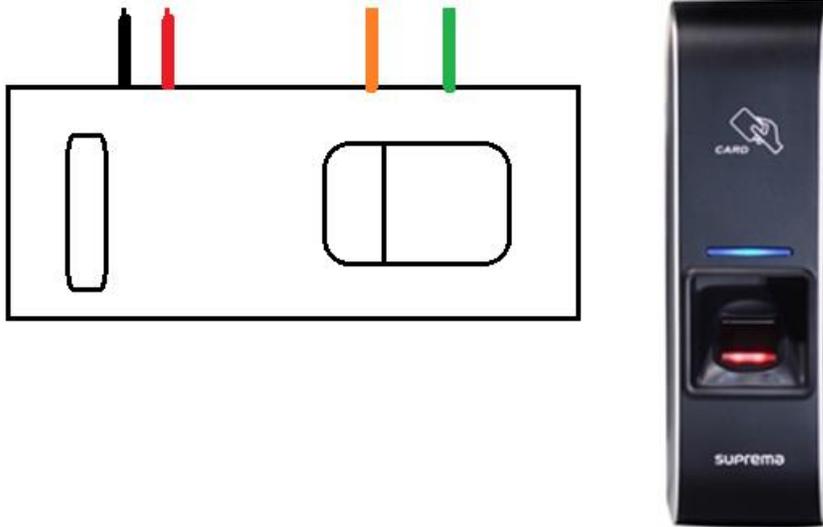


Figura 93. Controlador. Fuente autor del proyecto.



**Figura 94. Bioentry W. Fuente autor del proyecto.**

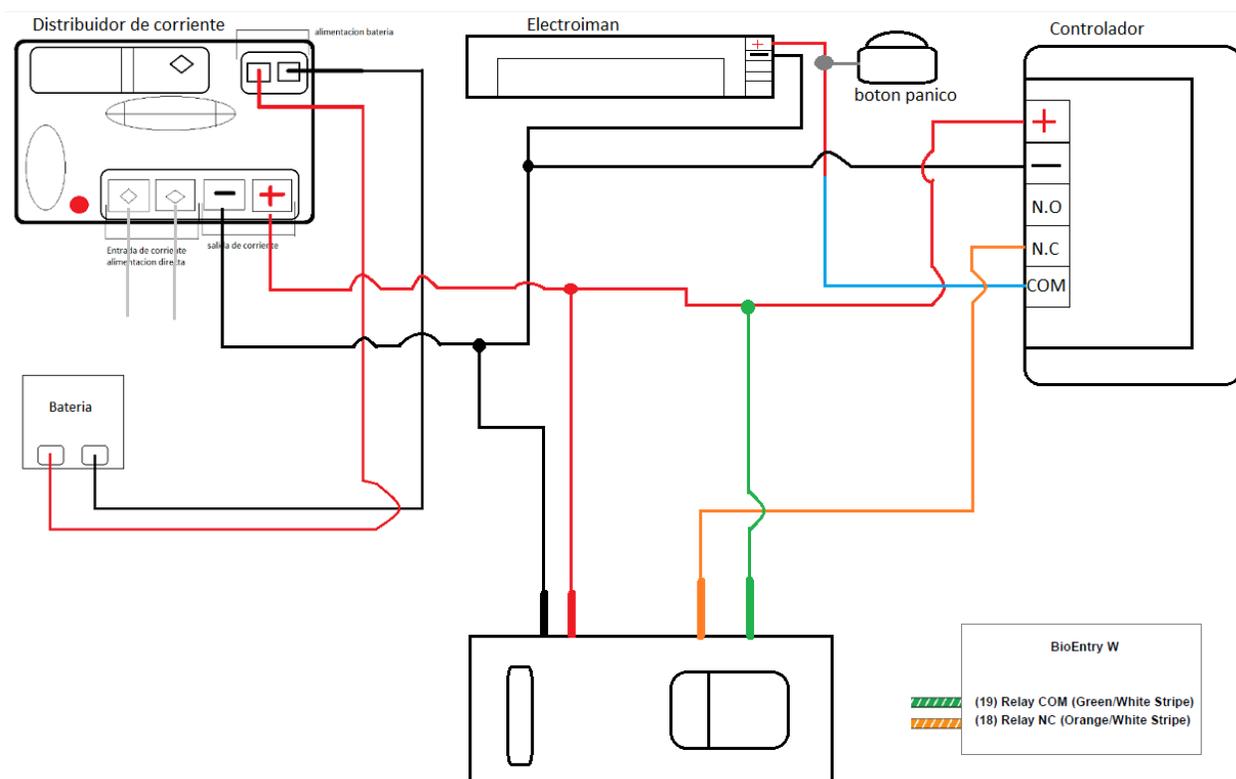


Figura 95. Circuito de instalación de implementos. Fuente autor del proyecto.

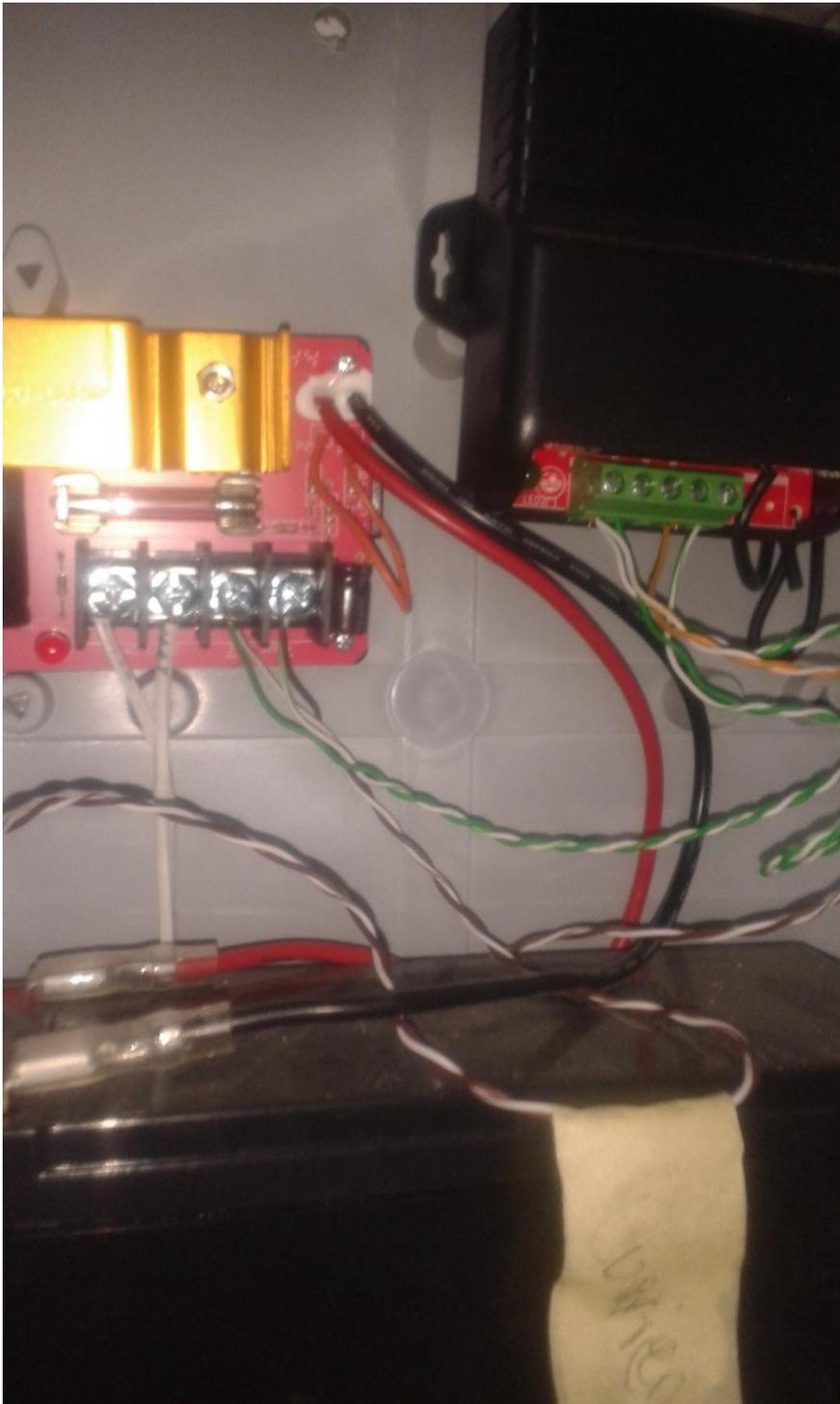


Figura 96. Circuito de control. Fuente autor del proyecto.