UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"CONTROL DE REGISTRO DE ASISTENCIA PARA EL PERSONAL ADMINISTRATIVO Y DOCENTE UTILIZANDO RELOJES BIOMÉTRICOS Y RADIOENLACES EN LA UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN TACNA"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ROJAS BUSTAMANTE, JOSÉ MERCEDES

Villa El Salvador
2015

DEDICATORIA

Este proyecto está dedicado a mis padres por el apoyo incondicional en mi formación personal y al personal docente que en el transcurso vivencial ya sea colegio, centro preuniversitario y universidad fueron formándome profesionalmente

AGRADECIMIENTO

A Dios.

Por darnos la sabiduría.

A Mis Padres.

Por su comprensión y apoyo en todo momento

A mis Familiares.

Por los consejos aportados y bien recibidos que a larga hoy me encaminan hacia una meta trazada

INDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

En los últimos tiempos las nuevas tecnologías de información han transformado con su aplicación, casi todas las actividades que el ser humano realiza, hoy en día los avances científicos y tecnológicos le proporcionan al ser humano todas aquella herramientas y mecanismos que le permiten dar solución a los nuevos retos que se le presentan en la vida diaria.

La propuesta del presente proyecto es optimizar la administración en el control de asistencia del personal docente y administrativo del Centro Universitario Jorge Basadre Grohmann (UNJBG) de Tacna, basándose en un método de autentificación biométrica, en específico el método de huella digital.

En el Centro Universitario el control actual de asistencia no es de todo confiable ya que actualmente emplean dos métodos diferentes, para el personal docente se utiliza la firma de listados y para el personal administrativo se emplea el registro de tarjeta, ambos vulnerables a la manipulación del mismo personal puesto que no hay seguridad alguna a la hora de registro.

El sistema ayudara de tal forma que se permita eliminar el tiempo que actualmente se destina para crear los listados por día que se tienen que realizar para que el personal académico y la creación de tarjetas cada cierto tiempo para el personal administrativo situando todo en una base de datos sin la necesidad de gastar en papel y tinta en los listados, por otra parte, también se podrá asegurar que se

registre correctamente los horarios de entrada y salida reales del personal administrativo puesto que no se cuenta con alguna persona que en realidad verifique que el personal escribe la hora en que llego.

Además, cabe mencionar también que dicho sistema Biométrico será distribuido por puntos estratégicos por la cercanía a las facultades para que no se haga difícil el registro a tiempo, tal distribución implicaría un cableado a larga distancia para lo cual se va utilizar radioenlaces para evitar el mismo.

El punto de concentración será la Biblioteca, en la cual se encuentra ubicado el cuarto de comunicaciones del centro universitario.

La Universidad Nacional Jorge Basadre Grohmann, cuenta con 5 locales, la principal, el centro de postgrado, Imprex, Invitro y la escuela de Agronomía

Ilustración 1: Universidad Nacional Jorge Basadre Grohmann

Fuente: Pagina Web universidades (2014)

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

Actualmente en la Universidad Nacional Jorge Basadre Grohmann (UNJBG) de la ciudad de Tacna, se tiene la necesidad de automatizar el registro de control de ingreso de empleados administrativos y docentes. El mercado tecnológico ofrece diversas técnicas para ello y en la universidad se cuenta con recurso humano capaz para implementarlo.

No existe un adecuado seguimiento de las labores y control de ingreso del personal docente y administrativo, puesto que los mismos se registran de manera manual, es decir con la firma de un papel y tarjetas registran su ingreso, lo cual no garantiza un registro adecuado, ya que puede ser fácilmente vulnerado.

Como se menciona en el párrafo anterior el control de asistencia son tareas independientes, es decir para el personal docente su registro es mediante la firma de hojas, detallando la hora de su ingreso y lo mismo ocurre para los administrativos que se registrar en tarjetas y estas son colocadas en ficheros hasta la hora de su salida.

1.2. Justificación del Problema

La Biometría es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas, como es la huella digital, las empresas pasan por alto la implementación de sistemas sofisticados para controlar la asistencia de los empleados dejándolo en un segundo plano de poca importancia, por lo cual emplean listas de asistencias donde los empleados firman la hora de llegada y salida, este tipo de control de asistencia es vulnerable y manipulable de manera que el trabajador puede alterar la hora, así haya llegado tarde y no ingresaría la hora exacta. Con tales inasistencias o llegadas tardes tendrían amonestaciones y bajo rendimiento en la jornada laboral.

Debido a estos datos inexactos es importante contar con sistemas modernos para el control de asistencias en la Universidad Nacional Jorge Basadre Grohmann de modo que capturarían la hora exacta de entrada y salida de los docentes y administrativos de dicho centro universitario mejorando así el rendimiento en hora/hombre de trabajo. Creando motivación al empleado a ser puntual, esto generaría ganancias en el tiempo y mayor productividad en el trabajo.

1.3. Delimitación del Proyecto

Este proyecto se limita a solo el control de asistencia para el personal administrativo y docente, para lo cual se instalara relojes biométricos y antenas de radioenlaces, en el caso de los relojes biométricos estos están distribuidos a lo largo del campus universitario y se pudo observar que no cuentan con un sistema de vigilancia dichos equipos, puesto que pueden ser dañados.

1.4. Formulación del Problema

1.4.1. Problema Principal

Como controlar el registro de asistencia para el personal administrativo y docente utilizando Relojes Biométricos y Radioenlaces en la Universidad Nacional Jorge Basadre Grohmann de la cuidad de Tacna.

1.4.2. Problemas Específicos

Como controlar el ingreso y egreso del personal administrativo y docente al campus universitario

1.5. Objetivos

1.5.1. Objetivo General

Controlar el registro de asistencia para el personal administrativo y docente utilizando Relojes Biométricos y Radioenlaces en la universidad nacional Jorge Basadre Grohmann de la ciudad de Tacna

1.5.2. Objetivos Específicos

Controlar el ingreso y egreso del personal administrativo y docente al campus universitario

CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la Investigación

2.1.1. Ámbito Nacional

Luis Eduardo Balmelli Chuquisengo (2006), en la tesis: Verificación de Identidad de Personas mediante Sistemas Biométricos para el Control de Acceso a una Universidad, fue el resultado de la investigación realizada en la Pontificia Universidad Católica del Perú para la implementación de sistemas biométricos (lectores de huellas dactilares) como elementos de seguridad.

Dada su problemática en la universidad (robos, plagios, amontonamiento de personas para ingresar, etc.), al implementar sistemas biométricos se mejoró sustancialmente esta situación, aparte de tener un lugar más seguro y confiable.

En la investigación se abordó los temas relacionados a los sistemas de seguridad empleados actualmente tanto en lugares públicos como privados, y la descripción y evaluación (costos y beneficios) de los sistemas biométricos más usados en el mundo.

Habiéndose realizado el análisis de costos y beneficios, llegaron a la conclusión de que la implementación de sistemas biométricos basados en las huellas dactilares fue la opción óptima, tanto para mejorar la seguridad como para agilizar el ingreso al campus universitario.

Cernańdes Gómez Harry Alejandro, Zapata Ramírez Elmer Kristopher (2006), en la tesis: Identificación de Personas Mediante el Reconocimiento Dactilar y su Aplicación a la Seguridad Organizacional, La huella dactilar es un medio confiable de identificación de personas; es por ello que el reconocimiento de huellas dactilares por medios computacionales ha despertado un gran interés en el desarrollo de sistemas de información computacionales.

Las empresas necesitan cuidar sus activos por lo que buscan las formas de cómo lograrlo, así encuentran en la tecnología la manera automatizada de cuidar sus activos. Para ello, las empresas invierten en grandes sistemas de seguridad, la identificación biométrica ya no es más un concepto de investigación sino una realidad que se puede aplicar.

Hoy en día, existen sistemas computacionales de reconocimiento de huellas dactilares en grandes empresas que necesitan alta seguridad. Por otro lado, comenzaron a ver cada vez más su uso en un rango mucho más amplio de situaciones cotidianas.

La aplicación de este trabajo de tesis fue orientado a la seguridad organizacional, basado en la huella dactilar, específicamente tomaron como objeto de aplicación a la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos.

Gilber Rafaele Juárez (2011), el presente trabajo de investigación titulado: "software de control de asistencia del personal administrativo mediante el uso de la tecnología biométrica de huellas digitales, para la municipalidad provincial de grau-2011", tuvo como objetivo de aumentar el nivel de seguridad y disminuyendo el tiempo de registro del personal administrativo de la municipalidad provincial de Grau, en él se diseñó el algoritmo de comparación que hizo de este sistema una solución confiable y de bajo costo, la tecnología biométrica permite resolver problemas de control de acceso y seguridad informática sin la necesidad de olvidar objetos o recordar contraseñas. También se utilizó para permitir la conexión de hardware- software, para la adquisición de huellas digitales, se utilizaron un scanner de papel, para la simulación de prototipos se realizó con matlab.

Para realizar el algoritmo primero se realizó todo el proceso digital de imágenes con lo que la huella digital quedo lista para poder encontrar los dos tipos más comunes de puntos característicos que existen en las huellas que son los terminaciones y bifurcaciones de las crestas, sus posiciones son únicas en cada persona por lo que con ella es posible identificar una persona y determinar si el individuo es aceptado o no por el sistema.

El procedimiento de cada huella tuvo un promedio de tiempo de 20 segundos y su verificación alrededor de 2 segundos.

2.1.2. Ámbito Internacional

Edgar Enrique Moreno Guerrero (2008), en esta tesis: Sistema de Registro y Control de Asistencia Utilizando Lectores Biométricos de Huella Digital, en este proyecto se toma en cuenta los avances que presenta la tecnología actualmente cada vez son mayores, y día a día se desarrollan un sinfín de nuevas tecnologías, una de ellas es la biometría, la cual se refiere al uso de características físicas, biológicas o de comportamiento que un individuo presenta para la identificación o verificación de su identidad.

La biometría trae consigo varias ventajas entre las que podemos resaltar la seguridad, la cual se vuelve muy eficiente pues es necesario que la persona a ser identificada este presente físicamente.

Tomando en cuenta estos factores, en el documento se desarrolló un sistema de registro y control de asistencias mediante el uso de lectores biométricos de huella digital, facilitando mediante esta experiencia la agilización del proceso de registro de asistencias y brindado una mayor seguridad a este mismo.

2.2. Bases Teóricas

2.2.1. Biometría

El concepto de «biometría» se deriva de las palabras griegas bios (de vida) y metron (de medida). Este concepto no se puso en práctica hasta finales del siglo XIX, si bien se sabe que al menos desde el siglo XIV los comerciantes chinos estampaban las impresiones y huellas de la palma de la mano de los niños en papel con tinta para distinguirles.

El concepto clásico de biometría denota la aplicación de técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Dentro del contexto tecnológico, la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características físicas o de comportamiento de las personas con el objetivo de establecer una identidad.

Durante la última década, investigadores del campo de la ciencia cognitiva han perseguido crear sistemas dotados de las habilidades humanas. Quizás la más admirada y estudiada de todas sea la visión, una tarea que resulta extremadamente fácil para nosotros. De hecho, se lleva a cabo de forma automática, y esconde un proceso realmente complejo, que aún hoy no se conoce por completo.

Un sistema biométrico es todo aquel que realiza labores de biometría de manera automática. En otras palabras, se trata de sistemas basados en medir y analizar

las características físicas y del comportamiento humano con propósito de autentificación.

En la actualidad, los métodos más aceptados de identificación se basan en la colección de rastros dactilares y, últimamente, en las muestras de ácido desoxirribonucleico (ADN), cuyos grados de confiabilidad resultan casi infalibles.

La mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. Aunque, se comienza a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial, la voz, la mano o la firma.

Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser, posiblemente, el mejor método de identificación humana.

Ilustración 2: Biometría

Fuente: Pagina Web Sistemas operativos (2014)

¿Por qué usar la Biometría?

Son claras las ventajas que se obtienen al utilizar sistemas biométricos.

Es fácil de usar. La utilización de sistemas biométricos libera al usuario del uso de elementos externos auxiliares. De forma resumida:

• El usuario no tiene nada que recordar,

• Nada que cambiar,

• Nada que perder.

Proporciona un nivel más alto de seguridad ya que los parámetros utilizados son unívoca “firma” de una característica humana que no puede ser fácilmente adivinada o descifrada.

La biométrica explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que las contraseñas.

a. Por razones de automatización. En el pasado el procesamiento de biométrico era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas nada que recordar.

Hoy en día, dispositivos tales como escáneres, videocámaras, y micrófonos pueden, electrónicamente, capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones.

Cada tecnología biométrica (huella dactilar, rostro, voz, etc.) tiene sus propias características, variedades y certezas.

Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con las contraseñas prestadas o robadas.

b. Importancia de la identificación personal. El problema de resolver la identidad de una persona se puede clasificar fundamentalmente en dos tipos distintos de planteamientos: reconocimiento (más popularmente conocido como identificación) y verificación.

El reconocimiento se centra en determinar la identidad del sujeto dentro de un conjunto ya conocido de identidades. La verificación se encamina a confirmar o denegar la identidad aducida por una persona. En muchas situaciones de nuestra vida cotidiana nos vemos requeridos a probar nuestra identidad, como por ejemplo cuando realizamos una compra con una tarjeta de crédito.

Una verificación certera de la identidad de una persona podría disuadir la delincuencia y el fraude, dinamizar las transacciones comerciales y salvaguardar los recursos críticos.

2.2.2. Dispositivos Biométricos

Un sistema biométrico en general consta de componentes tanto hardware como software necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

Reconocimiento de la huella dactilar.

Reconocimiento de la cara.

Reconocimiento de iris/retina.

Geometría de dedos/mano.

Autentificación de la voz.

Reconocimiento de la firma.

Los sistemas biométricos se han desarrollado como respuesta a la creciente demanda de seguridad existente en la actualidad y aunque algunos de ellos son altamente fiables, ningún sistema es efectivo al 100%, y estos sistemas también son susceptibles de ser engañados.

a. Modelo del proceso de identificación personal

Conocimiento: la persona tiene conocimiento (por ejemplo: un código),

Posesión: la persona posee un objeto (por ejemplo: una tarjeta), y

Característica: la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).

b. Características de un sistema biométrico para identificación personal

El desempeño, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

La aceptabilidad, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria.

La fiabilidad, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc.

c. ¿Cómo funcionan los sistemas Biométricos?

La mayoría de los sistemas biométricos funcionan con arreglo a un modelo general que consiste en dos pasos. El primer paso es el registro de la persona en

el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia.

De acuerdo con la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona.

En el caso de verificación, la persona le informa al sistema cuál es su identidad, ya sea presentando una tarjeta de identificación o introduciendo alguna clave especial. Se captura el rasgo biométrico y se compara con el modelo de referencia de la persona. Si ambos modelos parean, la verificación se realizó con éxito, si no es fallida.

En caso de que sea identificación, la persona no le informa al sistema biométrico cuál es su identidad. El sistema tan sólo captura el rasgo biométrico y lo compara con un conjunto de modelos de referencia para determinar la identidad de la persona.

2.2.3. Huellas Dactilares o Digitales

Las huellas dactilares o digitales son un ID único para cada ser humano, como las rayas del tigre, no hay dos tigres con las mismas rayas igual en el caso de las cebras, nunca coinciden dos huellas, ni en los gemelos idénticos. Página 16

Tiene muchos fines como proteger derechos de autor o en sistemas de seguridad de alta tecnología. También se llama DRM, sirven para proteger contenido digital por el "problema" de la copia pirata.

Son como marcas únicas en cada persona es como un comprobante perfecto de quien eres ya que no existe nadie más que tenga las mismas huellas, se utilizan para comprobar la identidad de las personas y además son importantes para el tacto por ejemplo para los cirujanos son muy necesarias al igual que para todo tipo de personas que en su trabajo necesite mucho usar las manos para sentir las cosas.

a. Propiedades de la huella dactilar

Está demostrado científicamente que los dibujos papilares, es decir, los dibujos que forman la impresión de la huella dactilar, son permanentes, inmutables y diversiformes.

Son **permanentes** porque, desde que se forman en el sexto mes de vida, permanecen invariables en número, situación, forma y dirección.

Son **inmutables** debido a que las crestas papilares no pueden modificarse fisiológicamente. De hecho, si hay un traumatismo poco profundo, se regeneran y, si llega a ser profundo, las crestas no reaparecen con forma distinta a la que

tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.

Por último, son **diversiformes**, pues aún no se ha dado el caso de encontrar dos impresiones idénticas producidas por dedos diferentes.

Dichas propiedades hacen de la huella dactilar un método de identificación muy seguro, en consecuencia, dicho método se presenta hoy en día como uno de los más reconocidos entre todas las técnicas biométricas existentes.

Ilustración 3: Huella Dactilar

Fuente: Pagina Web Sistemas operativos (2014)

b. ¿Por qué usar la huella dactilar?

La huella dactilar se usa en muchas aplicaciones en las que se quiere realizar la identificación de personas de forma segura y cómoda para el usuario. Su objetivo es evitar los riesgos de suplantación de identidad derivada del robo, copia o pérdida de tarjetas y códigos numéricos, de una forma muy práctica para el usuario, evitándole el tener que recordar códigos ni contraseñas.

Es un sistema rápido y seguro, pero, además, es el más extendido entre los sistemas de reconocimiento biométrico. Esto es así debido a que, si lo comparamos con otras técnicas presentes en el mercado, éstas presentan una serie de inconvenientes:

El iris da unos resultados muy óptimos, pero requiere que los ojos del usuario se aproximen mucho al dispositivo, lo que puede ser incómodo para éste; además, los dispositivos son costosos y aparatosos.

Por otra parte, el reconocimiento por voz está sujeto a diversos factores, como puede ser una enfermedad o ronquera en el caso de la voz, lo que impediría que el sistema reconociera al sujeto.

En cuanto al reconocimiento basado en la palma de la mano, los dispositivos tienden a ocupar mucho más espacio que los de la huella dactilar.

Por último, el reconocimiento de cara depende de la iluminación, el ángulo, la expresión y la edad del sujeto, lo que hace que este método no esté muy aceptado en entornos en los que se requiera un alto nivel de seguridad.

c. ¿Cómo reconocen los sensores la huella dactilar?

La huella dactilar presenta unas particularidades como son las convergencias, desviaciones, uniones, interrupciones, fragmentos, etc. que forman las crestas que la componen.

¿Qué buscamos en una huella dactilar? ¿Cuáles son sus puntos de interés? En una huella tenemos una serie de crestas y valles que crean el dibujo en el cual podemos reconocer ciertos puntos de interés, comúnmente llamados “minutiae” o minucia. De todos estos puntos, lo que realmente nos interesa para la identificación son principalmente las terminaciones o bifurcaciones de las crestas. Además, existen también otros puntos de interés como: el núcleo (centro del patrón de la huella), las islas, los deltas y las discontinuidades.

El motivo por el cual nos interesan tanto estos puntos es que, entre ambos, suman casi el 80% de los puntos de la huella dactilar.

A una minucia se le atribuyen dos características: la posición, la cual señalaremos con dos coordenadas (x,y); Y la orientación, la cual cuantificaremos como el ángulo comprendido entre la horizontal hacia la derecha (las tres en un reloj) y la prolongación de la línea con sentido positivo en contra de las agujas del reloj.

Para que un sistema de identificación de huellas dactilares sea eficiente, es absolutamente necesario el uso de un procesado electrónico de la huella dactilar. Para realizar dicho procesado, el algoritmo encargado de comparar la huella debe recibir como parámetros las características de las minucias presentes en la muestra. Pero obtener dicha información no es un problema trivial.

Este procedimiento recibe el nombre de filtrado, pues se encarga de eliminar la información no necesaria para quedarse sólo con lo interesante: las minucias y su par posición y dirección.

d. ¿Cómo funcionan los productos de reconocimiento de huella dactilar?

Para que un dispositivo basado en la identificación por huella dactilar garantice el acceso a un servicio únicamente a los usuarios deseados, existe un proceso previo a la identificación, llamado enrolado. El enrolado consiste en la inserción, dentro del sistema, de la huella dactilar de un usuario para que este la pueda reconocer en operaciones futuras, así como los permisos ligados a dicha huella. El usuario puede enrolarse colocando su dedo en un aparato de reconocimiento de huella dactilar, tal como un dispositivo de escritorio o el mismo aparato de control de acceso. El sensor digitaliza el dedo del usuario y captura la imagen de la huella dactilar.

El algoritmo específico extrae puntos particulares de la imagen tal como se ha comentado en la sección anterior, y convierte la información en un único modelo matemático, comparable a una contraseña con 60 dígitos. Este modelo único se encripta y se archiva para representar al usuario. No se guarda ninguna imagen concreta de la huella dactilar, por lo que no puede ser utilizada para la reconstrucción física de ésta.

Una vez incluido el usuario en el sistema, éste ya puede ser reconocido. De qué manera se haga este reconocimiento dependerá de la modalidad de funcionamiento del aparato: verificación o identificación.

En la verificación, se confirma la autenticidad de un usuario previamente enrolado. El usuario proporciona su huella dactilar (posicionando el dedo en el sensor) junto con su información de identidad como, por ejemplo, su número de ID. El sistema de comprobación de huella dactilar recupera la plantilla de la huella según el número de ID y la compara con la huella dactilar del usuario adquirida en tiempo real. Si ambas coinciden (muestra previamente registrada y muestra actual), el usuario es verificado positivamente. En cambio, en caso de identificación, se establece la identidad de un individuo comparando su huella dactilar capturada en vivo contra una base de datos de individuos conocidos. Sin el conocimiento previo de la identidad de la persona, el sistema de identificación de huella dactilar intenta comparar su huella con aquellas que están en la base de datos. Si encuentra una huella similar, el sujeto es identificado con éxito.

2.2.4. Control de Asistencia en una Organización

Existen diversas formas para controlar la asistencia del personal, desde el reloj checador tradicional hasta equipos electrónicos con sofisticados lectores de huella digital, de banda magnética y de código de barras. Si bien es cierto que los dispositivos electrónicos son más costosos, también proporcionan un mayor número de ventajas en cuanto a la simplificación de procesos para el departamento de recursos humanos.

Además, el control de asistencia sirve como herramienta para tener los reportes de incidencias siempre actualizados. Así, cuando éstos se necesiten en alguna controversia laboral, el patrón podrá desvirtuar los hechos en su contra y ahorrarse el desgaste que conllevan los laudos laborales.

a. Beneficio del control de asistencia.

Seguimiento del horario de trabajo de los trabajadores.

Mejor control sobre ellos y hacer las correcciones del caso.

Se adapta a los medios externos como (tarjetas, huella digital, comando de voz, etc.).

Flexible a configuraciones de horario (cuando se cuenta con diferentes tipos de horarios).

Permite justificar tardanzas e inasistencias.

b. Las empresas obtendrán:

Permite hacer el seguimiento horas – hombres.

Mejor control y pago de horas extra.

Permite tener un orden para temas de control de auditoria

2.2.5. Métodos de Reconocimiento de Huellas Dactilares

Los métodos existentes para almacenar y posteriormente comparar las plantillas de las huellas dactilares almacenadas en un repositorio de datos contra la capturada in-situ de la persona a identificar, son: el método basado en patrones y el método basado en minucias.

a. Método basado en Patrones

Un dispositivo lector toma una imagen gráfica de la huella dactilar. La imagen gráfica recién obtenida del lector es conocida como una lectura en vivo (livescan) para distinguirla de una plantilla o huella almacenada en una base de datos. Un software de procesamiento examina la imagen de la huella digital y ubica el centro de la imagen, el cual podría ser distinto al centro de la huella digital. Luego se recorta la imagen a una distancia definida alrededor de ese centro de la imagen. El rectángulo de la Ilustración 3 muestra esta región recortada. La región recortada se comprime, se almacena y es clasificada para posteriores comparaciones.

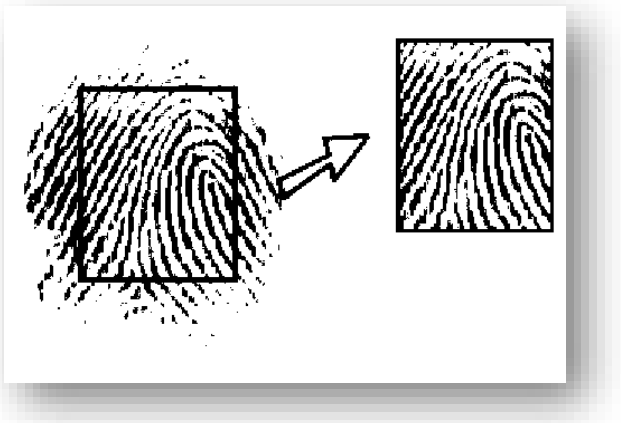

Ilustración 4: Método Basado en Patrones

Fuente: Almudena Lindoso Muñoz, Tesis Doctoral (2009)

Este proceso consiste en ubicar una huella dentro de los varios tipos existentes, los cuales son clasificados de acuerdo al número y dirección de crestas presentes en: Anillo de crestas, Lado derecho, Lado izquierdo, Arco, Arco de capa.

Las comparaciones de huellas digitales con plantillas basadas en patrones implican realizar una comparación gráfica de las dos plantillas y determinar una medición de la diferencia. Mientras más grande es la diferencia, menos concuerdan las huellas, es decir, consiste en ubicar una huella dentro de las varias plantillas existentes.

b. Método basado en Minucias

Tal como en el método basado en patrones, en el método basado en minucias un dispositivo lector toma una imagen gráfica de la huella dactilar (lectura en vivo). Un software especial analiza la imagen para determinar si realmente contiene la imagen de una huella dactilar, luego determina la ubicación del centro de la huella, el tipo de patrón (por ejemplo, de arco a la izquierda, de remolino u otro), estima la calidad de las crestas y finalmente extrae las minucias.

Vistas desde una perspectiva sencilla, las minucias indican dónde ocurre una variación relevante en la huella. Estas variaciones se muestran en la Ilustración 4.

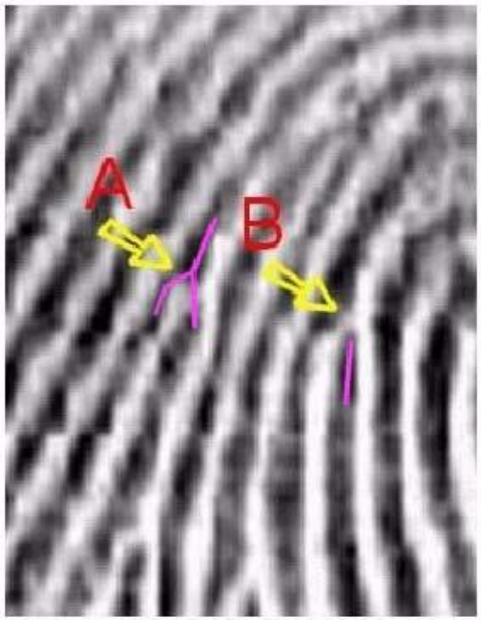

Ilustración 5: Método Basado en Minucias
Fuente: Almudena Lindoso Muñoz, Tesis Doctoral (2009)

Entendiéndose que las líneas oscuras de la imagen representan las crestas y las líneas claras representan los surcos, la flecha A muestra una región donde una cresta se divide en dos crestas (conocida como una bifurcación) y la flecha B muestra dónde termina una cresta.

Luego de reconocer estas variaciones en la huella digital, el software de extracción de minucias determina una orientación de estas variaciones (usando la flecha B como ejemplo, la orientación comienza al final de la cresta y se mueve hacia abajo).

Las minucias resultantes, en su forma más sencilla, son una colección de todas las bifurcaciones y finales de crestas, teniendo en cuenta su ubicación y su orientación.

La Ilustración 6 muestra un conjunto de minucias.

Ilustración 6: Conjunto de Minucias

Fuente: Almudena Lindoso Muñoz, Tesis Doctoral (2009)

Adicionalmente, el software de extracción de minucias coloca un eje de coordenadas sobre la huella, posicionándolo de tal forma que el centro del eje esté sobre el núcleo de la huella y que se alinee con la orientación de la huella.

Para que dos plantillas basadas en minucias concuerden no es necesario que concuerden todas las minucias que se han extraído de las huellas. De por sí se pueden obtener resultados muy precisos con que tan solo concuerde un tercio del total de minucias.

2.2.6. Tecnologías Biométricas

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma

de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor. Partiendo de estas características se han desarrollado dispositivos que han tenido mayor o menor éxito en el mercado.

Nos basaremos en el sistema lector de impresión digital.

a. Lector de impresión digital. Esta tecnología se basa en identificar al individuo por medio de su huella dactilar. Aunque puede utilizarse cualquier dedo de la mano, por una cuestión de dimensión y comodidad, los dedos más utilizados son el índice y el corazón. Su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos reducir dicha imagen a una representación matemática de la huella (“plantilla”) y compa. Esta plantilla patrón se acumula en la memoria interna del equipo (junto con un número de identificación o PIN si se trata de un verificador, a fin de tener asociada la huella al individuo).

Luego, cada vez que la persona necesite identificarse, ya sea para registrar su horario de ingreso o regreso al trabajo o activar una puerta o barrera, debe digitar su PIN (en el caso que sea un verificador) y a continuación colocar su dedo (el mismo que registró originalmente) en el lector.

Ilustración 7: Lector de Impresión Digital

Fuente: Mg Juan Carlos Gonzales, Tecnologías biométricas aplicadas a la seguridad, UNMSM (2010)

b. Escáner híbrido sin contacto para huellas y venas de los dedos. Este sistema escáner sin contacto HS100-10 ContactlessHybridFinger Scanner emplea la autenticación de la huella digital y también de las venas de los dedos, pero no requiere ningún contacto físico para obtener los datos que se necesitan para autentificar la identidad de un individuo mediante ambas modalidades biométricas.

Ilustración 8: Escáner Híbrido sin Contacto para Huellas y Venas de los Dedos

Fuente: Mg Juan Carlos Gonzales, Tecnologías biométricas aplicadas a la seguridad, UNMSM (2010)

2.3. Marco Conceptual

2.3.1. Lector USB de huella dactilar ZK 4500

El ZK4500 es un dispositivo de huella dactilar que captura a la huella y la carga al sistema mediante USB. ZK4500 soporta la mayoría de los sistemas operativos Windows y dispone de SDK para desarrollar.

Con el SDK se puede integrar el ZK4500 en otros sistemas tales como: seguridad social, seguridad pública, control de presencia, cifrado de huellas digitales, sistemas embebidos y otros campos de aplicación.

Ilustración 9: Lector ZK 4500

Fuente: Ficha técnica ZK 4500, Empresa SEGO, Lima-Perú

ESPECIFICACIONES TECNICAS	
Sensor	ZK (óptico)
Resolución	500 DPI / 256 gray
Área del sensor	15x18 mm
Tamaño de imagen	280x360 pixel
Color	negro
Interface	USB
Dimensiones	65.5x49x79.8 mm
Peso	0,20kg
Temperatura	0°C – 55°C
Humedad	20% - 80%

Tabla 1: Especificaciones Técnicas ZK4500

Fuente: Ficha técnica ZK 4500, Empresa SEGO, Lima-Perú

2.3.2. Lectora Biométrica ICLOCK 700

IClock 700 ID es una innovadora solución para control de personal y accesos, con cámara de foto integrada. Trabaja con la versión de algoritmo de huella digital más avanzada, que le da confiabilidad y precisión al momento de la registración. Su velocidad de verificación es menor a 2 segundos y permite registrar los accesos mediante tres opciones: huella digital, tarjetas de aproximación y contraseña de manera independiente o combinada. Cuenta con una pantalla TFT de 3,5 pulgadas, pudiendo así mostrar de manera óptima la información del dispositivo, incluyendo la foto del usuario, la calidad de imagen de la huella digital y el resultado de la verificación. Sus 8 teclas de función parametrizables permiten identificar el estado de la asistencia, el trabajo o verificar los mensajes de texto públicos y privados. Su comunicación estándar es a través del puerto TCP/IP, logrando un monitoreo en tiempo real de las registraciones del personal.

Ilustración 10: Lectora ICLOCK700

Fuente: Ficha técnica ICLOCK 700, Empresa SEGO, Lima-Perú

ESPECIFICACIONES TECNICAS	
Capacidad de Huellas	8000
Capacidad de Tarjetas	10000
Capacidad de Transacción	200000
Sensor	ZK Sensor óptico antirralladuras
Versión de Algoritmo	Zk v9.0 y v10.0
Lector RFID	EM Marin 125 khz, Mifare opcional
Batería de Respaldo	Si, con duración de hasta 4 horas
Velocidad de Verificación	1:N 1 a 1
Pantalla	Color TFT 3,5”
Fuente de Alimentación	12V, 1,5A
Temperatura Tolerable	0°C – 45°C
Humedad Tolerable	20% - 80%
Dimensiones	225mm x 165.5mm x 50mm
Comunicación	RS232/485, USB Host/Cliente, TCP/IP

Tabla 2: Especificaciones técnicas ICLOCK 700

Fuente: Ficha técnica ICLOCK 700, Empresa SEGO, Lima-Perú

2.3.3. Antena WipAir 8000

De WaveIP WipAir 8000 es la última palabra en punto a punto y soluciones inalámbricas punto a multipunto de banda ancha.

Con sin precedentes de rendimiento neto asimétrico dinámico de 310 Mbps y latencia ultra baja de 1 ms, este puente inalámbrico avanzado OFDM 2X2 MIMO es la solución óptima para aplicaciones de alta capacidad, como IP y backhauls celulares, video vigilancia y redes privadas. Mediante la implementación de la tecnología MIMO, WipAir 8000 ofrece el doble de rendimiento, alcance y fiabilidad, así como una mayor disponibilidad.

Altamente entorno interferido enfrentará innovadoras soluciones de rechazo de interferencia de WaveIP: tecnología única sensibilidad automática Interferencia (AIS), el funcionamiento y la estabilidad sin error la única hitless adaptativa Codificación y Modulación (ACM) en el mercado y la petición de retransmisión más rápida automática (ARQ), garantizando en la latencia y el rendimiento.
Gama fenomenal de más de 130 Km, de mayor capacidad, menor latencia y el rechazo de interferencia RF excepcional coloca WipAir 8000 en la cima de su categoría.

ESPECIFICACIONES TECNICAS
Mayor rendimiento neto - **310 Mbps**
Más eficiente la capacidad asimétrica dinámica
Interfaz de 2x10/100/1000 Base –T Gigabit Ethernet
Mejor latencia de 1ms
Rango de longitud – más de 130 km
Ancho de banda de canal Configurable - 3.5 / 5/7/10/14/20/28/40/50 MHz
Diseño resistente a la intemperie Resistente y fiable
Consumo de energía 7Watt
Licencia de frecuencia 4.8 Ghz – 6.0 Ghz

Tabla 3: Especificaciones Técnicas Antena WIPAIR 8000

Fuente: Ficha técnica Antena WIPAIR 8000

Ilustración 11: PTP-PMP/Antena WipAir 8000

Fuente: Ficha técnica Antena WIPAIR 8000

2.3.4. Antena Omnidireccional 5Ghz-12Dbi MIMO

ESPECIFICACIONES TECNICAS	
Rango de Frecuencia	4950-5850 MHZ
Ganancia	12 dBi
Temperatura	-55°C a 70°C
Polarización	Vertical y horizontal
Ancho de haz	360 °
Potencia Max.	50w
Impedancia	50Ω
Dimensiones	65x450mm
Peso	2Kg
Humedad	< 95%

Tabla 4: Especificaciones Técnicas Antena Omnidireccional
Fuente: Ficha técnica Antena WIPAIR 8000

Ilustración 12: Antena Omnidireccional 5Ghz
Fuente: Ficha técnica Antena WIPAIR 8000

2.3.5. Switch HP 08 puertos POE

Los HP 1410 series switches son switches Gigabit Ethernet y Fast Ethernet no gestionados, diseñados para la busca de soluciones de red de gama baja y de bajo coste con una garantía de por vida completa. Los HP 1410 switch series consta de siete modelos con opciones de montaje flexibles que permiten a los clientes elegir el mejor switch que se ajuste a sus necesidades de conmutación de red. Todos los modelos son compatibles con las funciones de QoS y de control de flujo IEEE 802.3x para garantizar la máxima eficiencia de datos. El funcionamiento simplificado plug and play se habilita con funciones como MDIX automática y la negociación de velocidad automática. HP ha innovado y combinado los últimos avances en tecnología de silicio para proporcionar los switches más eficientes energéticamente: los modelos Fast Ethernet de 16 y 24 puertos son los primeros conmutadores Fast Ethernet no gestionados del sector compatibles con IEEE 802.3az. Las funciones ecológicas disponibles junto con la garantía de por vida de HP convierten a los HP 1410 switch series en productos ideales para los clientes que buscan soluciones de red fiables y de bajo coste.

Características:

Calidad de servicio (QoS)

- Asignación de prioridades IEEE 802.1p: envía los datos a los dispositivos en función de la prioridad y el tipo de tráfico
- Compatibilidad con el Punto de código de DiffServ (DSCP): permite la priorización del tráfico en tiempo real basado en parámetros TOS/DSCP de 3 capas

Conectividad

- MDIX automático: se ajusta automáticamente para cables normales o cruzados en todos los puertos 10/100 y 10/100/1000

Rendimiento

- Compatible con Green Ethernet (solo J9662A y J9663A): compatible con nuevo estándar IEEE 802.3az; permite un menor consumo de energía al trabajar con dispositivos de cliente compatibles con IEEE solo en modo de 100 Mb/s.
- Capacidad de negociación automática semidúplex/dúplex en todos los puertos: duplica la velocidad de todos los puertos
- Compatibilidad con tramas gigantes (solo modelos Gigabit Ethernet): permite tramas de hasta 9216 bytes para estar siempre conectado a través de la red.

- Compatibilidad con tramas jumbo mini (solo J9662A y J9663A): permite que las tramas de hasta 2.048 bytes se conmuten a través de la red, que admite grandes transferencias de datos

Tabla 5: Especificaciones técnicas Switch

ESPECIFICACIONES TECNICAS	
Cantidad puertos RJ45	8
Tecnología de cableado ethernet	100 Base-TX, 10Base-T
Peso	340g
Consumo energético	3,6W
Corriente	0,3A
Voltaje	100 – 240V
Disipación de calor	13 BTU/h
Frecuencia	50/60HZ
Temperatura	0 - 40°C
Humedad	15 - 95%

Fuente: Ficha técnica Switch HP 1410 / POE

Ilustración 13: SWITCH POE/8 PUERTOS/HP

Fuente: Ficha técnica Switch HP 1410 / POE

2.3.6. Servidor R620 Intel/Xeon

ESPECIFICACIONES TECNICAS	
Marca	Dell
Serie	R620
Peso	21Kg
Dimensiones	90,5 x 61,4 x 29 cm
Velocidad del procesador	2 GHZ
Toma del procesador	Socket R (LGA 2011)
Numero de procesadores	12
Capacidad de la memoria RAM	8 GB
Capacidad del disco duro	10 TB
Numero de puertos de ethernet	4
Potencia eléctrica	750 vatios
Memoria máxima compatible	768 GB
Sistema Operativo	No, Red Hat Enterprise Linux, SUSE Linux, Windows Server 2008 R2 SP1, x64,Windows Small Business Server 2011

Tabla 6: Especificaciones Técnicas Servidor R620

Fuente: Ficha técnica Servidor R620-INTEL/Xeon

Ilustración 14: Servidor R620-Intel

Fuente: Ficha técnica Servidor R620-INTEL/Xeon

2.3.7. Cable UTP cat 6

El Cable de categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para evitar la diafonía (o crosstalk) y el ruido. El estándar de cable se utiliza para 10BASE-T, 100BASE-TX y 1000BASE-TX (*Gigabit Ethernet*). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1 Gbps. La conexión de los pines para el conector RJ45 que en principio tiene mejor inmunidad a interferencia arriba de 100Mbps es el T568A.

El cable contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores. Aunque la categoría 6 está a veces hecha con cable 23 AWG, esto no es obligatorio; la especificación **ANSI/TIA-568-B.2-1** aclara

que el cable puede estar hecho entre 22 y 24 AWG, mientras que el cable cumpla todos los estándares de control indicados. Cuando es usado como cable patch, Cat-6 acaba normalmente en conectores RJ-45, a pesar de que algunos cables Cat-6 son incómodos para terminar de tal manera sin piezas modulares especiales y esta práctica no cumple con el estándar.

Si los componentes de los varios estándares de cables son mezclados entre sí, el rendimiento de la señal quedará limitado a la categoría que todas las partes cumplan. Como todos los cables definidos por TIA/EIA-568-B, el máximo de un cable Cat-6 horizontal es de 90 metros. Un canal completo (cable horizontal más cada final) se permite que llegue a los 100 metros en extensión.

Los cables utp Cat-6 comerciales para redes LAN, se construyen eléctricamente para exceder la recomendación del grupo de tareas de la IEEE, que está trabajando desde antes de 1997.

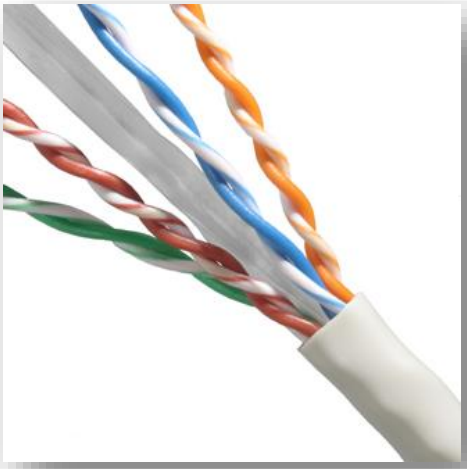

Ilustración 15: Cable UTP Cat 6

Fuente: Pagina web wikipedia, cable cat. 6

2.3.8. Cámara IP SONY SNC-CH160

- Capacidad de alimentación por Ethernet.
- Ángulo visión horizontal de 85.4 a 31.2 grados.
- Resolución HD 720 p
- Función día/noche óptica.
- Calefactor integrado.
- Relación de zoom Óptico de 2,9 aumentos

Ilustración 16: Cámara IP-SONY

Fuente: Ficha técnica Cámara IP SONY SNC-CH160

CAPITULO III: DISEÑO DEL SISTEMA

3.1. Análisis del Sistema

3.1.1. Análisis actual

Se pudo observar que en el Centro Universitario UNJBG de Tacna, existen procesos que aún se llevan a cabo de forma manual, tal es el caso de toma de asistencia del personal docente de esta Institución, deben firmar en una hoja de papel y el personal administrativo se registra en una tarjeta, lo que implica que:

- Personas ajenas a las diferentes tarjetas puedan registrar por otras.
- Los docentes puedan firmar las hojas de asistencia después del horario de entrada.
- La manipulación de las hojas de asistencia es muy primitiva lo que provoca desperdicio de papel además de inversión de tiempo.
- Todos los días se deben actualizar las hojas de asistencia para los académicos.
- Las tarjetas de chequeo deben imprimirse cada mes.

Con este proyecto se podrá controlar el registro de asistencia almacenando los datos tanto del personal docente y administrativo del centro universitario en un servidor, los cuales serán administrados y así poder llevar un mejor control.

3.1.2. Herramientas

ZK4500

El ZK4500 es un dispositivo de huella dactilar que captura a la huella y la carga al sistema mediante USB. ZK4500 soporta la mayoría de los sistemas operativos Windows y dispone de SDK para desarrollar.

Ilustración 17: Modo de registro usando ZK4500

Fuente: Ficha técnica ZK 4500, Empresa SEGO, Lima-Perú

ICLOCK700

Es un lector Biométrico, en el cual el personal docente y administrativo se registrara mediante sus huellas dactilares, después podrá verificar que haya sido registrado. La información puede descargarse a través del software de gestión de asistencia en la PC.

Ilustración 18: Partes del biométrico ICLOCK700

Fuente: Ficha técnica ICLOCK 700, Empresa SEGO, Lima-Perú

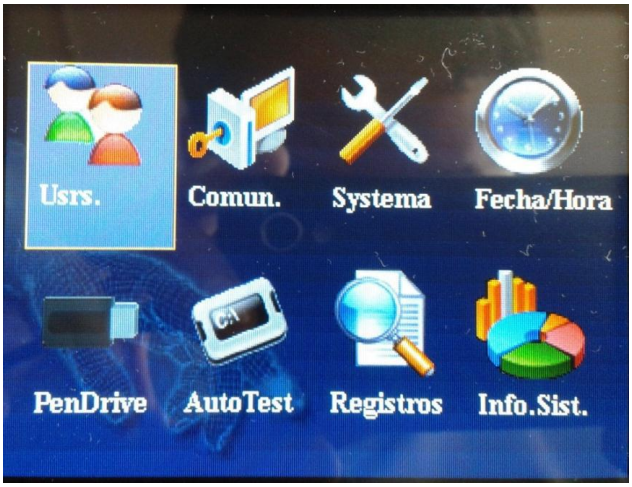

Ilustración 19: Opciones internas ICLOCK700

Fuente: Ficha técnica ICLOCK 700, Empresa SEGO, Lima-Perú

ZKTIME ENTERPRISE

ZKTime Enterprise es una aplicación de control de presencia que incorpora nuevas utilidades al sistema de control de presencia, facilitando su manejo y atendiendo una mayor cantidad de casos específicos.

Requisitos mínimos y datos de acceso

- Procesadora 800Mhz con sistema operativo Windows XP, 2000 o superior.
- 100Mb de disco duro disponibles y resolución mínima de 1024x768
- Tener instalados los prerrequisitos (FrameWork.NET 3.5 o superior)
- Trabaja con MySQL y SQL Server.
- Permite multiempresa y multiusuario

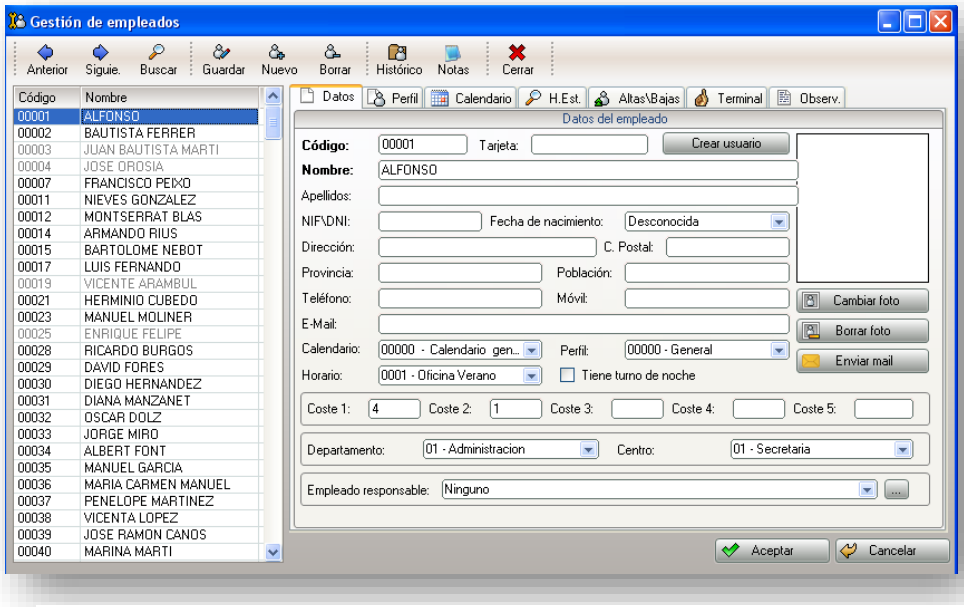

Ilustración 20: Plataforma del programa ZKTIME ENTERPRISE

Fuente: Manual de Usuario ZKTIME ENTERPRISE

3.2. Construcción del Sistema

3.2.1. Topología de Relojes Biométricos y Antenas de radioenlace

A continuación se detalla la ubicación de los relojes biométricos que serán distribuidos a lo largo del campus principal y sedes respectivas.

Estos serán enlazados mediante antenas de radioenlace, para evitar un largo cableado.

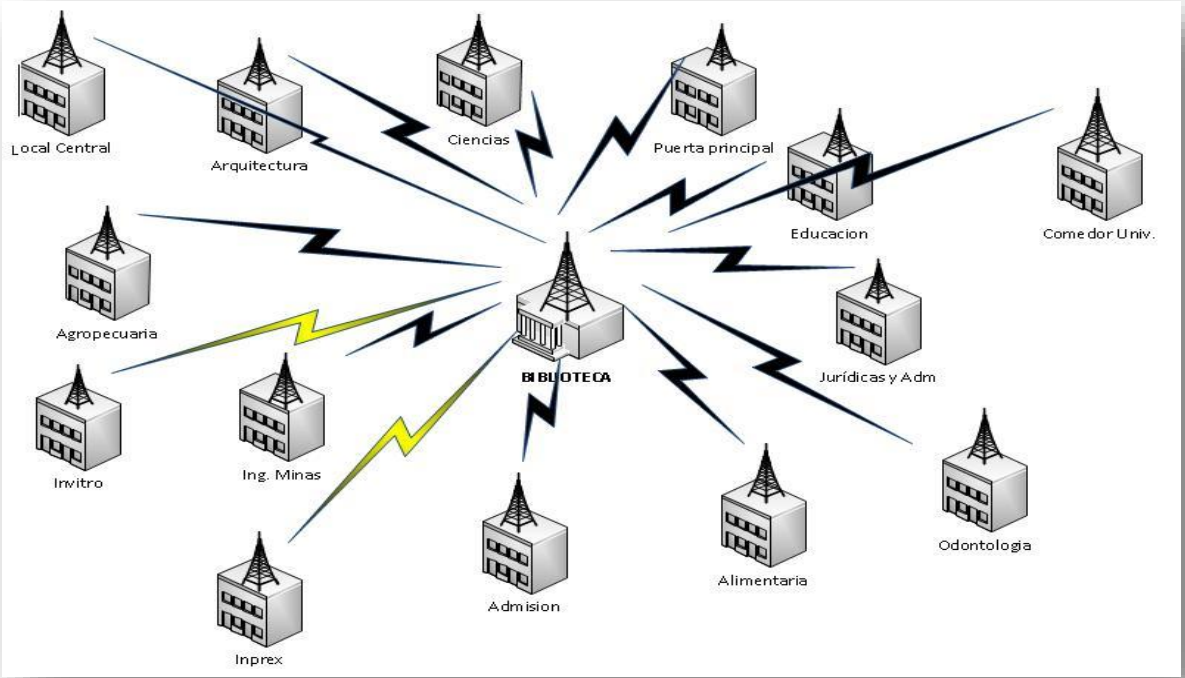

Ilustración 21: Ubicación de los biométricos y radioenlaces

Fuente: Autoría propia

Como se observa todos los puntos de enlace van hacia la biblioteca del campus principal, en dicho lugar en el primer piso se encuentra el cuarto de comunicaciones que albergara el Switch POE y Servidor para administrar y controlar los equipos.

3.2.2. Ubicación de los Relojes Biométricos

a. Sede principal

En la sede principal se ubicaran los siguientes Relojes Biométricos:

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio Comedor
Biométrico	1	Edificio Jurídicas
Biométrico	1	Edificio ciencias de Salud
Biométrico	1	Edificio Biblioteca
Biométrico	2	Puerta principal
Biométrico	1	Edificio Educación
Biométrico	1	Edificio Admisión
Biométrico	1	Edificio Alimentarias
Biométrico	1	Edificio Minas
Biométrico	1	Edificio Arquitectura
Biométrico	1	Edificio Ciencias

Tabla 7: Ubicación de Biométrico en la sede principal

Fuente: Autoría propia

Edificio comedor

Ilustración 22: Ubicación del Biométrico en el comedor

Fuente: Autoría propia

Edificio Jurídico

Ilustración 23: Ubicación del Biométrico en el edificio Jurídico

Fuente: Autoría propia

Edificio Salud

Ilustración 24: Ubicación del Biométrico en el edificio Salud

Fuente: Autoría propia

Biblioteca

Ilustración 25: Ubicación del Biométrico en la Biblioteca

Fuente: Autoría propia

Puerta Principal

Ilustración 26: Ubicación del Biométrico en la Puerta Principal

Fuente: Autoría propia

Edificio Educación

Ilustración 27: Ubicación del Biométrico en el edificio Educación

Fuente: Autoría propia

Edificio Admisión

Ilustración 28: Ubicación del Biométrico en el edificio Admisión

Fuente: Autoría propia

Edificio Alimentarias

Ilustración 29: Ubicación del Biométrico en el edificio Alimentarias

Fuente: Autoría propia

Edificio Minas

Ilustración 30: Ubicación del Biométrico en el edificio Minas

Fuente: Autoría propia

Edificio Arquitectura

2

Ilustración 31: Ubicación del Biométrico en el edificio Arquitectura

Fuente: Autoría propia

Edificio de Ciencias

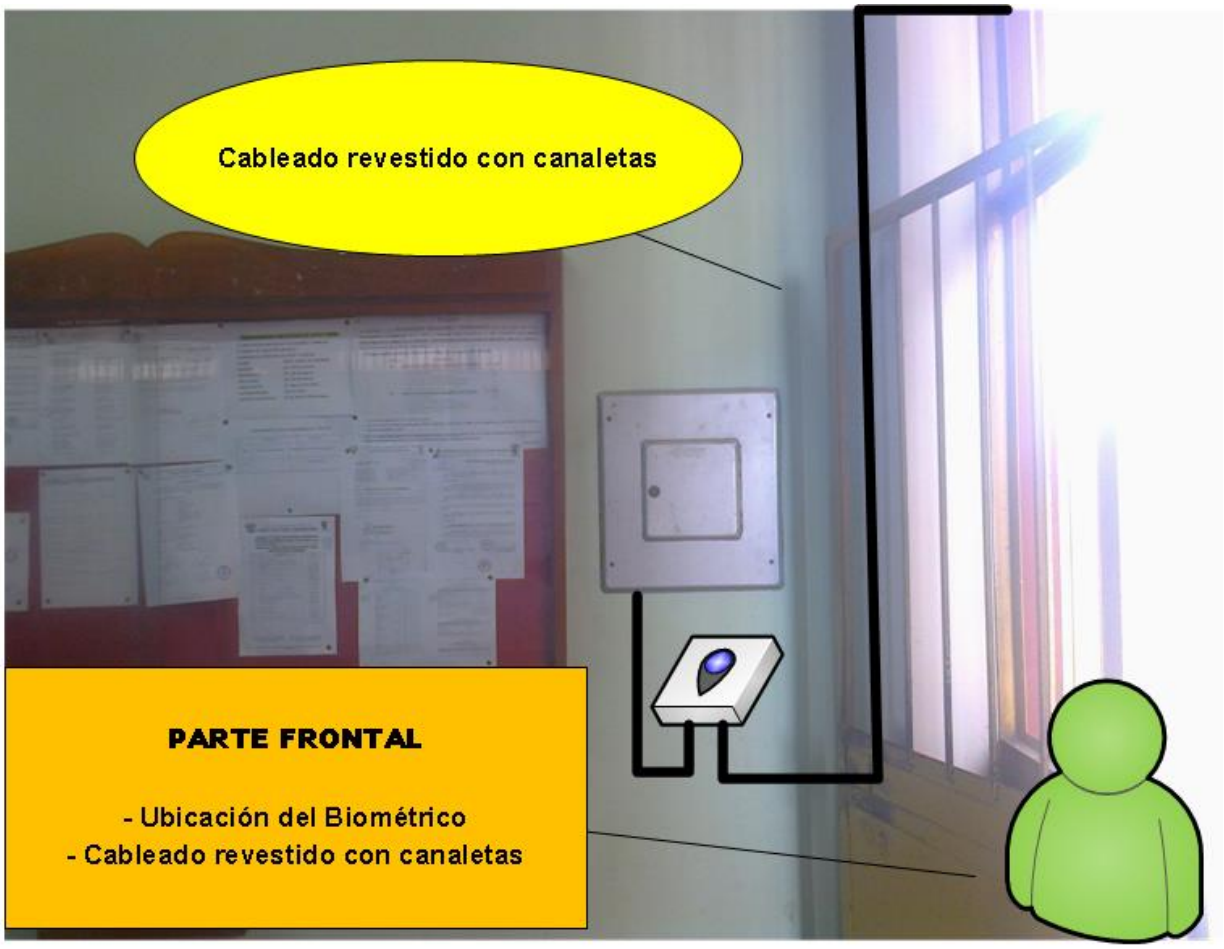

Ilustración 32: Ubicación del Biométrico en el edificio Ciencias

Fuente: Autoría propia

b. Local central

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio postgrado

Tabla 8: Ubicación de Biométrico en la sede Local Central

Fuente: Autoría propia

Ilustración 33: Ubicación del Biométrico en el local central

Fuente: Autoría propia

c. Inprex

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio

Tabla 9: Ubicación de Biométrico en la sede Inprex

Fuente: Autoría propia

Ilustración 34: Ubicación del Biométrico en Inprex

Fuente: Autoría propia

d. Escuela de Agronomía

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio

Tabla 10: Ubicación de Biométrico en la escuela de Agronomía

Fuente: Autoría propia

Ilustración 35: Ubicación del Biométrico en la escuela Agronomía

Fuente: Autoría propia

3.2.3. Ubicación de las antenas de radioenlace

a. Sede principal

En la sede principal se ubicaran las siguientes antenas:

TIPO	ENLACE	CANTIDAD	UBICACION
Omnidireccional	Radio	1	Torre de telecomunicaciones
Omnidireccional	Radio	1	Torre de telecomunicaciones
Omnidireccional	Radio	1	Torre de telecomunicaciones
Panel	Radio	1	Mástil en la azotea del Comedor
Panel	Radio	1	Mástil en la azotea de Jurídicas
Panel	Radio	1	Mástil en la azotea de ciencias de Salud
Panel	Radio	1	Mástil en la azotea Puerta principal
Panel	Radio	1	Mástil en la azotea Educación
Panel	Radio	1	Mástil en la azotea Admisión
Panel	Radio	1	Mástil en la azotea Alimentarias
Panel	Radio	1	Mástil en la azotea Minas
Panel	Radio	1	Mástil en la azotea puerta av. Cuzco
Panel	Radio	1	Mástil en la azotea puerta salida autos
Panel	Radio	1	Mástil en la azotea Arquitectura
Panel	Radio	1	Mástil en la azotea Ciencias
Panel	Radio	1	Torre de

			telecomunicaciones

Tabla 11: Ubicación de Antenas en la sede principal

Edificio comedor **Fuente:** Autoría propia

Ilustración 36: Ubicación de Antena en el comedor

Fuente: Autoría propia

Edificio Jurídico

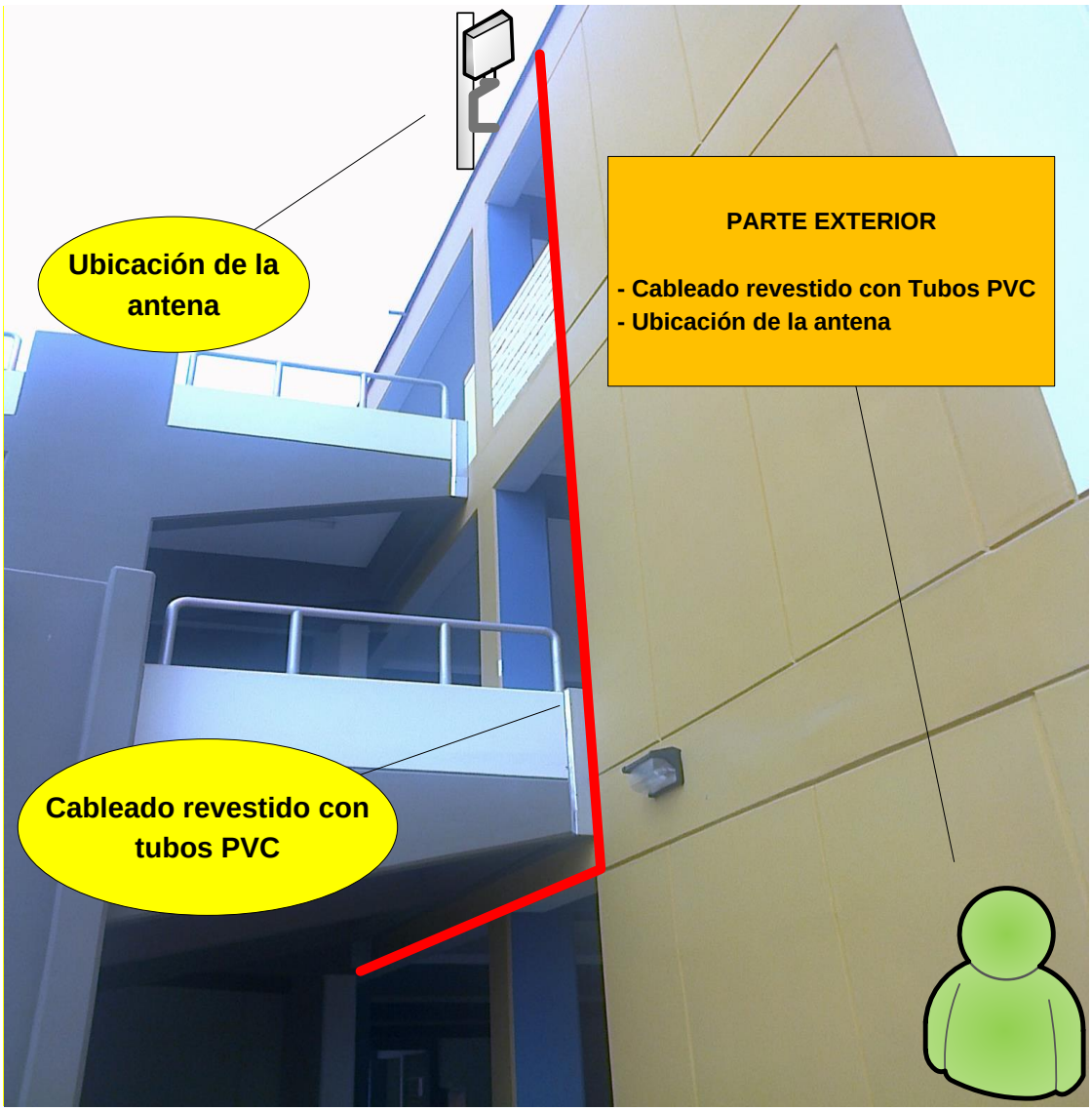

Ilustración 37: Ubicación de Antena en el edificio Jurídico

Fuente: Autoría propia

Edificio Salud

Ilustración 38: Ubicación de Antena en el edificio Salud

Fuente: Autoría propia

Biblioteca

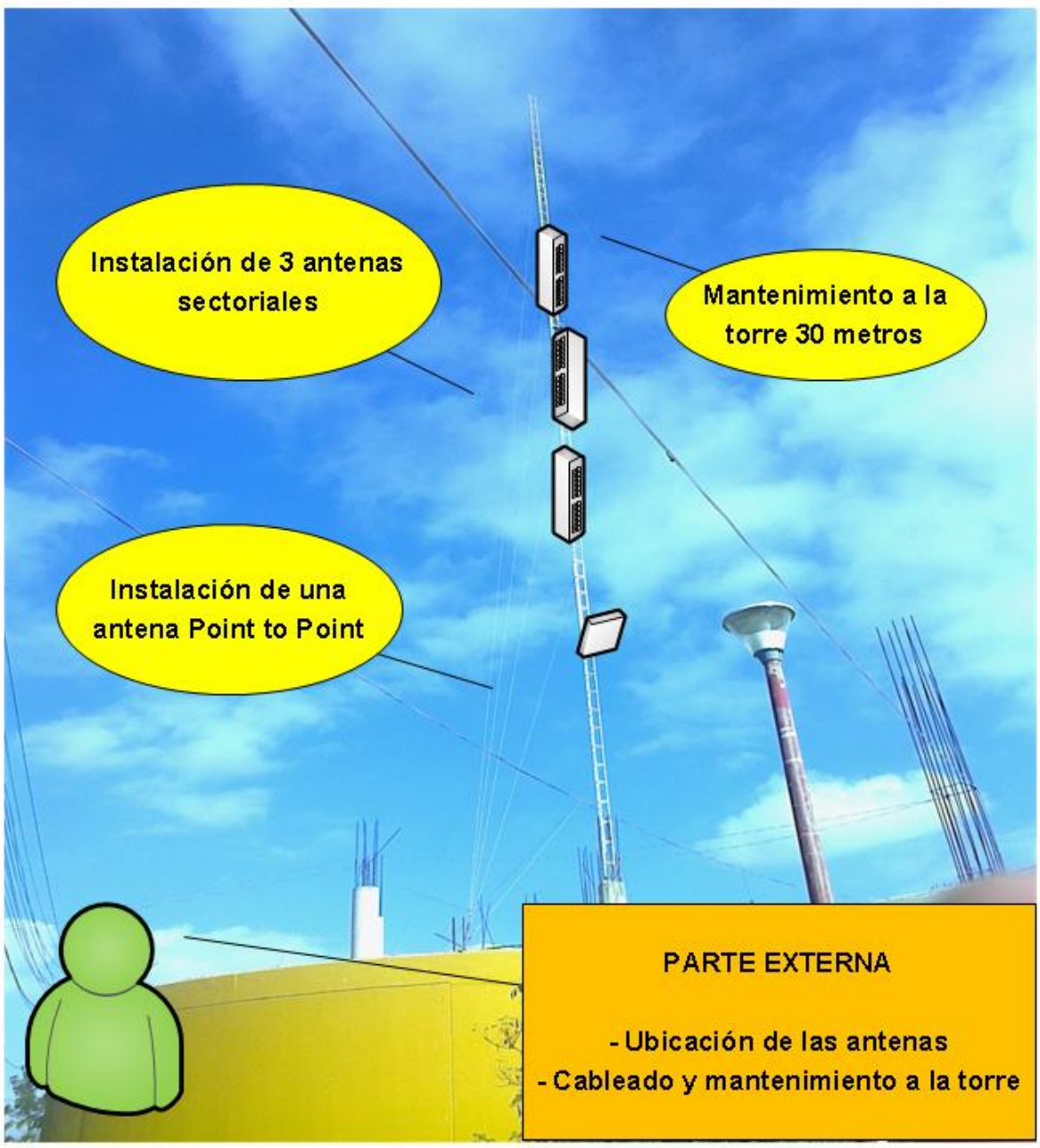

Ilustración 39: Ubicación de Antena en la Biblioteca

Fuente: Autoría propia

Puerta Principal

Ilustración 40: Ubicación de Antena y Cámara en la puerta principal

Fuente: Autoría propia

Edificio Educación

Ilustración 41: Ubicación de Antena en el edificio Educación

Fuente: Autoría propia

Edificio Admisión

Ilustración 42: Ubicación de Antena en el edificio Admisión

Fuente: Autoría propia

Edificio Alimentarias

Ilustración 43: Ubicación de Antena en el edificio Alimentarias

Fuente: Autoría propia

Edificio Minas

Ilustración 44: Ubicación de Antena en el edificio Minas

Fuente: Autoría propia

Edificio Arquitectura

Ilustración 45: Ubicación de Antena en el edificio Arquitectura

Fuente: Autoría propia

Edificio de Ciencias

Ilustración 46: Ubicación de Antena en el edificio Ciencias

Fuente: Autoría propia

b. Local central

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio postgrado

Tabla 12: Ubicación de Antenas en la sede Local Central

Fuente: Autoría propia

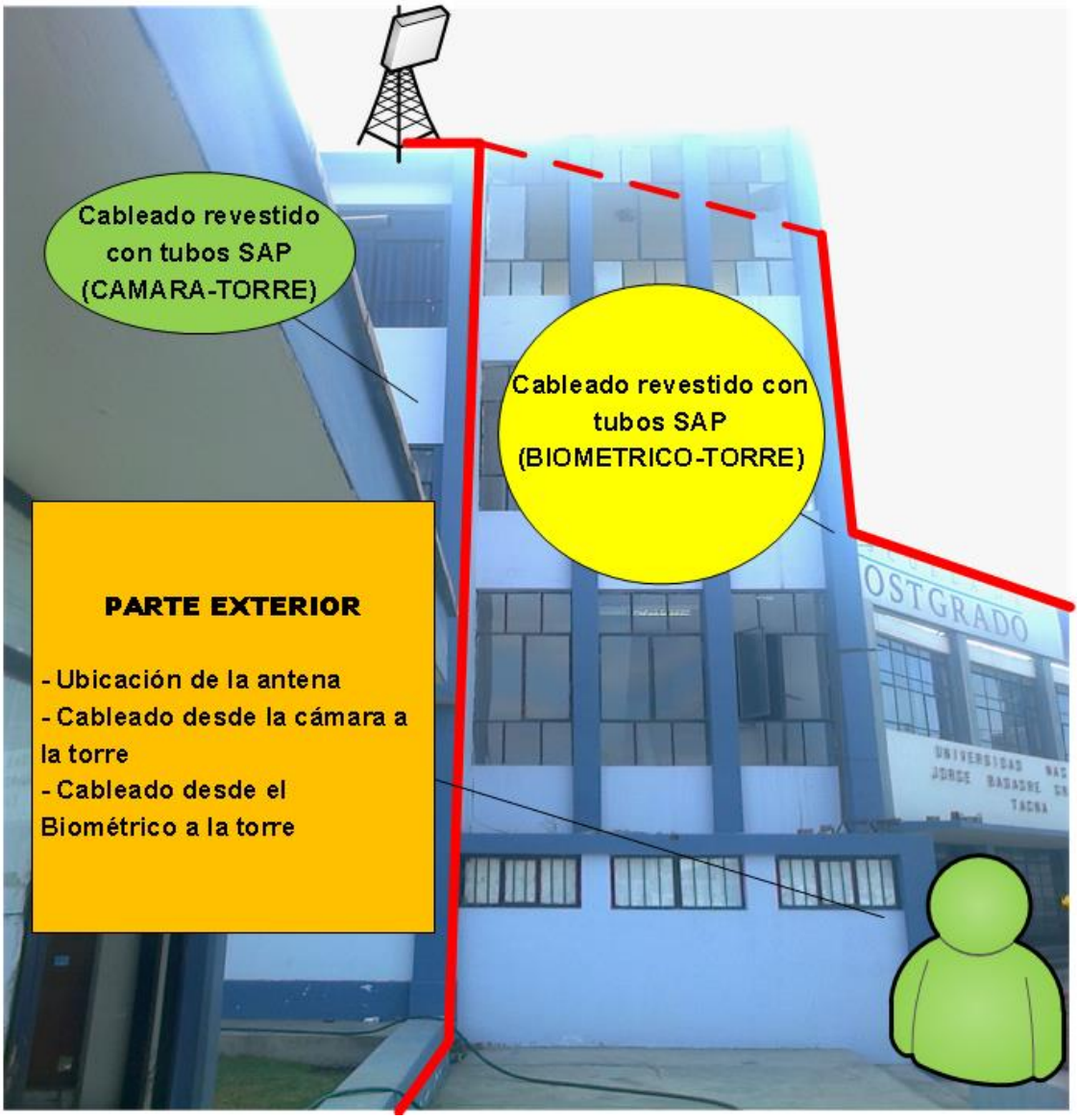

Ilustración 47: Ubicación de Antena y Cámara en el Local Central

Fuente: Autoría propia

c. Inprex

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio

Tabla 13: Ubicación de Antenas en la sede Inprex

Fuente: Autoría propia

Ilustración 48: Ubicación de Antena y Cámara en Inprex

Fuente: Autoría propia

d. Escuela de Agronomía

EQUIPO	CANTIDAD	UBICACION
Biométrico	1	Edificio

Tabla 14: Ubicación de Antena en la escuela de Agronomía

Fuente: Autoría propia

Ilustración 49: Ubicación de Antena en la escuela Agronomía

Fuente: Autoría propia

3.2.4. Ubicación de las Cámaras

TIPO	MODELO	CANTIDAD	UBICACION
Tubular	SONY SNC-CH160	1	Mástil en la azotea puerta av. Cuzco
Tubular	SONY SNC-CH160	1	Mástil en la azotea puerta salida autos
Tubular	SONY SNC-CH160	1	Mástil en la azotea Puerta principal

Tabla 15: Ubicación de Cámaras en la sede principal

Fuente: Autoría propia

TIPO	MODELO	CANTIDAD	UBICACION
Tubular	SONY SNC-CH160	1	Mástil en la pared

Tabla 16: Ubicación de Cámara en la sede Inprex

Fuente: Autoría propia

TIPO	ENLACE	CANTIDAD	UBICACION
Tubular	SONY SNC-CH160	1	Torre de telecomunicaciones

Tabla 17: Ubicación de Cámaras en la sede Local Central

Fuente: Autoría propia

TIPO	MODELO	CANTIDAD	UBICACION
Tubular	SONY SNC-CH160	1	Mástil en la Puerta av. Cuzco

Tabla 18: Ubicación de Cámaras en la escuela de Agronomía

Fuente: Autoría propia

3.3. Revisión y consolidación de resultados

Se asignó IP's para cada equipo realizando la simulación de pruebas de enlace con las antenas de radioenlaces.

3.3.1. Antenas de radioenlace

SEDE: Campus Universitario				
TIPO	**ENLACE**	**IP**	**CANTIDAD**	**UBICACION**
Omnidireccional	Radio	192.168.2.1	1	Torre de telecomunicaciones
Omnidireccional	Radio	192.168.2.2	1	Torre de telecomunicaciones
Omnidireccional	Radio	192.168.2.3	1	Torre de telecomunicaciones
Panel	Radio	192.168.2.4	1	Mástil en la azotea del Comedor
Panel	Radio	192.168.2.5	1	Mástil en la azotea de Jurídicas
Panel	Radio	192.168.2.6	1	Mástil en la azotea de ciencias de Salud
Panel	Radio	192.168.2.7	1	Mástil en la azotea Puerta principal
Panel	Radio	192.168.2.8	1	Mástil en la azotea Educación
Panel	Radio	192.168.2.9	1	Mástil en la azotea Admisión
Panel	Radio	192.168.2.10	1	Mástil en la azotea Alimentarias
Panel	Radio	192.168.2.11	1	Mástil en la azotea Minas
Panel	Radio	192.168.2.13	1	Mástil en la azotea puerta av. Cuzco
Panel	Radio	192.168.2.14	1	Mástil en la azotea puerta salida autos

Panel	Radio	192.168.2.17	1	Mástil en la azotea Arquitectura
Panel	Radio	192.168.2.18	1	Mástil en la azotea Ciencias
Panel	Radio	192.168.2.22	1	Torre de telecomunicaciones

Tabla 19: Ip's de Radioenlaces en la sede principal

Fuente: Autoría propia

SEDE: Local Central				
TIPO	**ENLACE**	**IP**	**CANTIDAD**	**UBICACION**
Panel	Radio	192.168.2.23	1	Torre de telecomunicaciones

Tabla 20: IP de Radioenlace en la sede Local central

Fuente: Autoría propia

SEDE: Inprex				
TIPO	**ENLACE**	**IP**	**CANTIDAD**	**UBICACION**
Panel	Radio	192.168.2.12	1	Mástil en la azotea

Tabla 21: IP de Radioenlace en la sede Inprex

Fuente: Autoría propia

SEDE: Agronomía				
TIPO	**ENLACE**	**IP**	**CANTIDAD**	**UBICACION**
Panel	Radio	192.168.2.16	1	Mástil en la azotea puerta av. Cuzco
Panel	Radio	192.168.2.15	1	Mástil en la azotea

Tabla 22: Ip's de Radioenlaces en la escuela de Agronomía

Fuente: Autoría propia

3.3.2. Relojes Biométricos

EQUIPO	IP	CANTIDAD	UBICACION
Biométrico	192.168.2.101	1	Edificio Comedor
Biométrico	192.168.2.102	1	Edificio Jurídicas
Biométrico	192.168.2.103	1	Edificio ciencias de Salud
Biométrico	192.168.2.104	1	Edificio Biblioteca
Biométrico	192.168.2.114	2	Puerta principal
	192.168.2.115		
Biométrico	192.168.2.105	1	Edificio Educación
Biométrico	192.168.2.106	1	Edificio Admisión
Biométrico	192.168.2.107	1	Edificio Alimentarias
Biométrico	192.168.2.108	1	Edificio Minas
Biométrico	192.168.2.111	1	Edificio Arquitectura
Biométrico	192.168.2.112	1	Edificio Ciencias

Tabla 23: Ip's de Biométricos en la sede principal

Fuente: Autoría propia

EQUIPO	IP	CANTIDAD	UBICACION
Biométrico	192.168.2.113	1	Edificio postgrado

Tabla 24: IP de Biométrico en la sede Local Central

Fuente: Autoría propia

EQUIPO	IP	CANTIDAD	UBICACION
Biométrico	192.168.2.109	1	Edificio

Tabla 25: IP de Biométrico en la sede Inprex

Fuente: Autoría propia

EQUIPO	IP	CANTIDAD	UBICACION
Biométrico	192.168.2.110	1	Edificio

Tabla 26: IP de Biométrico en la escuela de Agronomía

Fuente: Autoría propia

3.3.3. Cámaras IP

SEDE: Principal				
TIPO	**MODELO**	**IP**	**CANTIDAD**	**UBICACION**
Tubular	SONY SNC-CH160	192.168.2.124	1	Mástil en la azotea puerta av. Cuzco
Tubular	SONY SNC-CH160	192.168.2.125	1	Mástil en la azotea puerta salida autos
Tubular	SONY SNC-CH160	192.168.2.122	1	Mástil en la azotea Puerta principal

Tabla 27: IP de Cámaras en la sede Principal

Fuente: Autoría propia

SEDE: Agronomía				
TIPO	**MODELO**	**IP**	**CANTIDAD**	**UBICACION**
Tubular	SONY SNC-CH160	192.168.2.121	1	Mástil en la azotea puerta av. Cuzco

Tabla 28: IP de Cámara en la sede Escuela de Agronomía

Fuente: Autoría propia

SEDE: Inprex				
TIPO	**MODELO**	**IP**	**CANTIDAD**	**UBICACION**
Tubular	SONY SNC-CH160	192.168.2.126	1	Mástil en la Pared

Tabla 29: IP de Cámara en la sede Inprex

Fuente: Autoría propia

SEDE: Local Central				
TIPO	**ENLACE**	**IP**	**CANTIDAD**	**UBICACION**
Tubular	SONY SNC-CH160	192.168.2.123	1	Torre de telecomunicaciones

Tabla 30: IP de Cámara en la sede Local Central

Fuente: Autoría propia

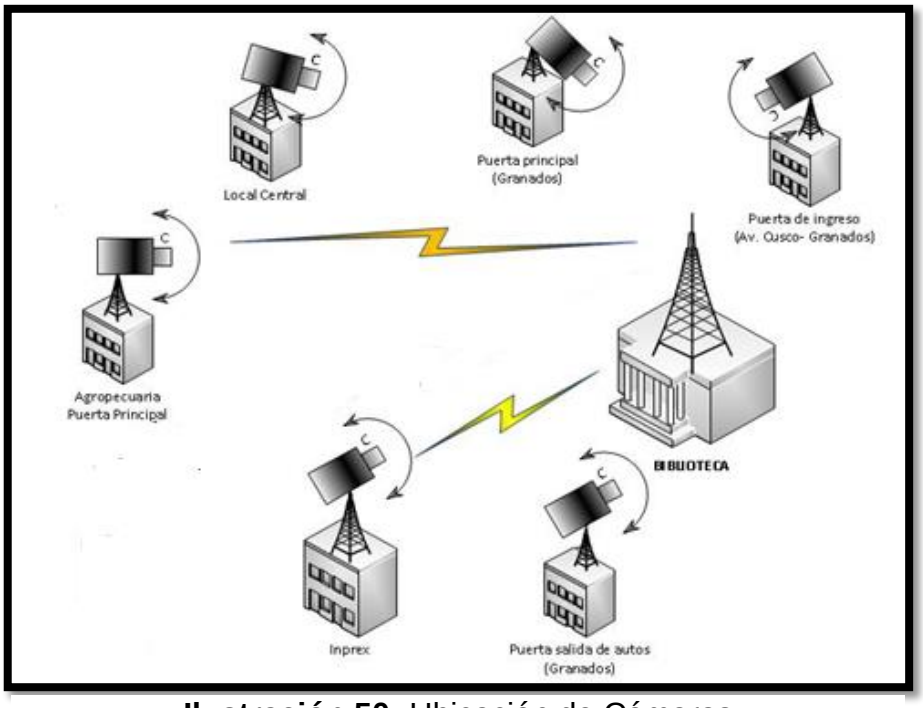

Ilustración 50: Ubicación de Cámaras

Fuente: Autoría propia

3.4. CONCLUSIONES

La sistematización de documentos forma parte del proceso operativo y administrativo de una organización, especialmente en las áreas administrativas de recursos humanos, finanzas, facturación, contabilidad, desarrollo de sistemas informáticos, departamentos jurídicos, etc.

En la Universidad Nacional Jorge Basadre Grohmann, la informatización del área es una necesidad urgente, lo primero es señalar que la firma biométrica ayuda a interactuar con los sistemas para la identificación, lo que facilita la gestión y administración de datos para el área de contabilidad. En la actualidad cada día son más abundantes las instituciones que cuentan con instrumentos biométricos para llevar un control de asistencia y de tareas; como impartición de cursos, jornadas laborales en las empresas.

Los beneficios que traería la implementación de una firma biométrica son principalmente ahorro de recursos económicos, horas empleado-trabajo y espacio de trabajo. Adicionalmente la firma biométrica es más amigable con el personal ya que no necesitan estar firmando cada vez, y eficaz con la administración de los datos puesto que los maestros no tendrían la facilidad de manipular la hora en que llega, así el administrador puede estar más seguro que el personal llega en tiempo y en forma a su empleo.

3.5. RECOMENDACIONES

- Se recomienda un mantenimiento de los equipos una vez al año, después de un año de entrega del proyecto.

- Se recomienda protección para los equipos instalados a la intemperie, como el reloj biométrico a instalar en la sede Inprex

- Se recomienda la vigilancia de los equipos instalados para evitar que sean dañado por terceros.

BIBLIOGRAFIA

[1] Luis Eduardo Balmelli Chuquisengo (2006), Verificación de Identidad de Personas mediante Sistemas Biométricos para el Control de Acceso a una Universidad. Proyecto de Tesis presentado en la Pontificia Universidad Católica del Perú.

[2] Cernańdes Gómez Harry Alejandro, Zapata Ramírez Elmer Kristopher (2006), Identificación de Personas Mediante el Reconocimiento Dactilar y su Aplicación a la Seguridad Organizacional. Proyecto de Tesis presentado en la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional Mayor de San Marcos.

[3] Pasco Olguín Christian (2011), Sistema Biométrico de Huellas para Control de Asistencia del Personal de la Empresa SIDERPERU. Proyecto implementado en la empresa SIDERPERU.

[4] Gilber Rafaele Juárez (2011), “Software de Control de Asistencia del Personal Administrativo Mediante el Uso de la Tecnología Biométrica de Huellas Digitales para la Municipalidad Provincial de Grau - 2011”. Trabajo de Investigación para la Municipalidad Provincial Grau.

[5] Fabiola González (2011), Sistema Biométrico Propuesto de Huella Dactilar para la Dirección de Informática y Sistemas de la Gobernación del Estado Bolívar. Proyecto aplicado en el Gobierno del Estado Bolívar - Venezuela.

[6] Edgar Enrique Moreno Guerrero (2008), tesis: Sistema de Registro y Control de Asistencia Utilizando Lectores Biométricos de Huella Digital.

[7] Alejandro Olivares Morales (2010), Automatización del Proceso de Control de Asistencia del Personal Académico en Tiempo Real a través de Reconocimiento Biométrico. Proyecto de Tesis presentado en la Universidad Nacional Autónoma de México – México.

[8] Yamith Arturo Velasco Reyes, Mario Fernando Villacrés Maldonado (2012), Control Biométrico de Docentes de la Universidad Central del Ecuador. Proyecto de Tesis presentado en la Universidad Central del Ecuador.