|  |
| --- |
| *ESTRUCTURA GENERAL* |
| **NOMBRE DEL PROYECTO:**  PROTOTIPO DE SISTEMA INTELIGENTE DE PARQUEADERO PARA LA ZONA DOCENTE DE LA UNIVERSIDAD DE LA AMAZONIA. |
| **INVESTIGADOR PRINCIPAL:** Heriberto Fernando Vargas Losada |
| **OTROS INVESTIGADORES:** Sergio Enrique Hernández Rubio y Estudiantes pertenecientes a GIECOM |
| **1. INFORMACIÓN GENERAL DEL PROYECTO:**  ANEXO 2: FORMATO 2-01 |
| 1. **RESUMEN EJECUTIVO** ANEXO 2: FORMATO 2-02 |
| 1. **DESCRIPCIÓN DEL PROYECTO** |
| * 1. **Planteamiento del Problema:**   La Universidad de la Amazonia en la actualidad cuenta con un área destinada para el parqueadero de los docentes de la institución, la cual está siendo utilizada por distintas personas (estudiantes, particulares, administrativos, terceros vinculados con la Universidad y los docentes). Esto hace que dicha área sea insuficiente y que no satisfaga las necesidades para la cual fue destinada, ya que presenta problemas de congestión impidiendo una buena movilidad en la zona.  La situación antes planteada se da debido a que no existe una administración adecuada de dicha área, la cual está a cargo de los guardas de vigilancia y seguridad de la Universidad quienes de manera flexible, por muchas circunstancias, permiten el acceso a dicha área de vehículos no autorizados para utilizar este servicio en este sitio. |
| * 1. **Impacto Esperado:**   Que el área asignada por la Universidad para el parqueadero de los vehículos de los docentes presente un mejor grado de congestión y por lo tanto mejore la movilidad, y así se garantice que solo estos hagan uso de esta zona. Adicional a la anterior la institución podrá conocer que vehículos se encuentran dentro de esta zona, lo cual permite incrementar las condiciones de seguridad de la Universidad.  También se espera incrementar de manera directa la seguridad prestada a los automotores de los docentes de la institución ya que para poder ser retirados se validará la identidad del conductor. |
| * 1. **Usuarios Directos e Indirectos potenciales de los resultados de investigación:**   El conjunto de docentes que poseen algún tipo de automotor y la vice rectoría administrativa (departamento de vigilancia y parque automotor) de la Universidad. |
| * 1. **Marco Teórico y Estado del Arte:**   **RFID**  La identificación por radio frecuenciaoRFID (Radio Frecuency IDentification) es una tecnología de punta mediante la cual se realiza la identificación al permitir la captación de datos de manera automática mediante radiofrecuencia [8, 12, 19]. Para este proceso de almacenamiento y recuperación de datos remotos se utilizan unos dispositivos denominados etiquetas o tags y un lector.  El modo de funcionamiento de los sistemas RFID es simple. Las etiquetas electrónicas almacenan el código único identificativo del producto al que están adheridas. El lector interroga al tag enviando una serie de ondas de radiofrecuencia, las cuales son captadas por éste mediante una pequeña antena, activando el tag el cual, mediante radiofrecuencia, transmite al lector la información que tiene almacenada. Una vez que el lector ha recibido el código único del producto, este se podría transmitir a una base de datos de respaldo [15].  En esencia, un sistema RFID permite la comunicación entre un lector y una etiqueta inteligente o transponder (tag) a través del aire y mediante una frecuencia conocida por ambos elementos. Así, un sistema RFID básicamente de compone de un lector y un transponder o Tag, cada uno de ellos con su respectiva antena. A este sistema se le puede adicionar un sistema de red que permita transportar la información recuperada del Tag a una base de datos ubicada en un computador [20].  **Lectores RFID**  Un lector RFID consta de un modulo de radio frecuencia (emisor receptor), una unidad de control, y un elemento de acoplamiento o antena. Los lectores de etiquetas interrogan a etiquetas por sus contenidos a través de una interfaz RF. Además de una interfaz RF para las etiquetas, los lectores pueden contener memoria interna, capacidad de procesamiento, o una interfaz para bases de datos de respaldo que proporcionan una funcionalidad adicional. Además el lector también se puede conectar a una red mediante algún tipo interfaz como pueden ser el RS-232 o el Ethernet [35].  **Antenas**  Son los dispositivos que permiten radiar las señales de los lectores y recepcionar las ondas radio de los tags. Un único lector puede gestionar varias antenas creando una zona de interrogación. Como ejemplo se puede citar las *Dock door* (2 antenas) para puertas o el arco (3 antenas) para cintas transportadoras [6].  **Transpondedores o tags**  Las etiquetas RFID o tags consisten típicamente en un microchip que almacena datos y un elemento de acoplamiento, tal como una antena en espiral, que es utilizada para comunicarse a través de una radiofrecuencia (ver Figura 1). Estos dos elementos se encuentran ubicados dentro de un sustrato. En el caso de los tags semiactivos o activos, aparece un cuarto elemento constitutivo, la batería. Los tags RFID según su fuente de energía pueden ser: *Activos,* *Semipasivos,* y *Pasivos* [2, 13, 29].  **Subsistema de procesamiento de datos o** [**Middleware RFID**](http://es.wikipedia.org/wiki/Middleware_RFID)  Normalmente los elementos de un sistema RFID no forman un sistema aislado, sino que se conectan a otros sistemas. El middleware es el sistema (hardware o software) situado entre el hardware RFID y las aplicaciones software del cliente. Su función es la de gestionar todo el sistema RFID a nivel de hardware, recibir la totalidad de la señales de los tags y filtrar la información, para solo transmitir la información útil a las aplicaciones [9, 22, 25].  **Clasificación de los sistemas RFID**  La utilización del espectro RF, está regulado por las normas que cada uno de los países emite al respecto. Una clasificación global y rápida es en bandas licenciadas (pago) y no licenciadas (libres). La tecnología RFID utiliza bandas no licenciadas. Los sistemas RFID utilizan diferentes frecuencias, pero generalmente las más utilizadas son: *Sistemas de Baja Frecuencia (LF)* que operan normalmente en 125 KHz, *Sistemas de Alta Frecuencia (HF)* que opera a 13,56 Mhz, *Sistemas de Ultra Alta Frecuencia (UHF)* que operan entre 860 y 960 MHz, y *Sistemas Microondas* usados para aplicaciones que requieren de grandes distancias y mayor velocidad de obtención de los datos [7, 16, 21, 28].  **ZigBee**  ZigBee es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica. ZigBee y IEEE 802.15.4 son protocolos basados en estándares que proporcionan la infraestructura de red necesaria para aplicaciones de redes de sensores inalámbricos. El estándar IEEE 802.15.4 define el hardware y el software, el cual ha sido descrito en los términos de conexión de redes, como la capa físicas (PHY), y la capa de control de acceso al medio (MAC). El estándar ZigBee (definido por la alianza ZigBee, conjunto de empresas promotoras del estándar) ha añadido las especificaciones de las capas red (NWK) y aplicación (APL) para completar lo que se llama la pila o stack ZigBee [1, 11, 14, 36].    ZigBee ha sido diseñado para soportar un diverso mercado de aplicaciones que requieren bajo coste y bajo consumo, con una conectividad más sofisticada que los anteriores sistemas inalámbricos. El estándar ZigBee se enfoca a un segmento del mercado no atendido por los estándares existentes, como es el de las redes de sensores cuyos requisitos claves de diseño giran en torno a la prolongación de la vida de la batería, un bajo costo, ocupación de poco especio y topología en malla para soportar la comunicación entre un gran número de dispositivos en un entorno interoperable y de múltiples aplicaciones [24, 32, 36].  Existen numerosas aplicaciones que son ideales para las capacidades de redundancia, de auto configuración y de auto configuración de las redes inalámbricas en malla ZigBee. Las principales son [10, 30]:   * **Gestión de la Energía y Eficiencia**: Para proporcionar mayor información y control del uso de la energía, proporcionar a los clientes un mejor servicio y más opciones, mejor manejo de los recursos, y ayudar a reducir el impacto ambiental. * **Automatización de la Casa**: Para proporcionar una gestión más flexible de la iluminación, la calefacción y la refrigeración, la seguridad y los sistemas de entretenimiento desde cualquier lugar de la casa. * **Automatización de Edificios**: Para integrar y centralizar la gestión de la iluminación, la calefacción, la refrigeración y la seguridad. * **Automatización Industrial**: Ampliar a los la existente manofactura y sus procesos sistemas de control confiables.   ZigBee trabaja sobre la banda ISM para usos industriales, científicos y médicos; en concreto, 868MHz en Europa, 915MHz en Estados Unidos y 2.4GHz en todo el mundo. En el rango de frecuencias de 2.4GHz se definen hasta 16 canales, cada uno de ellos con un ancho de banda de 5MHz [27, 34, 36].  La pila de protocolos ZigBee, también conocida como ZigBee Stack, se basa en el nivel físico (PHY) y el control de acceso al medio (MAC) definidos en el estándar IEEE 802.15.4, que desarrolla estos niveles para redes inalámbricas de área personal de baja tasa de transferencia (LR-WPAN, Low Rate - Wireless Personal Area Network). La especificación ZigBee completa este estándar añadiendo cuatro componentes principales: Nivel de red, Nivel de aplicación, Objetos de dispositivo ZigBee (ZDO, ZigBee Device Objects), y Objetos de aplicación definidos por el fabricante [17, 23, 31, 36].  **Biometría**  La Biometría es el método de identificación y autenticación de los seres humanos a través de características fisiológicas, tales como la geometría de la mano, iris, retina, reconocimiento facial, huella dactilar, entre otras; y de comportamiento como firma, voz, dinámica de teclado, etc [4].  En el siglo diecinueve comienzan las investigaciones científicas acerca de la biométrica con el fin de buscar un sistema de identificación de personas con fines judiciales. Con estas investigaciones se producen importantes avances y se comienzan a utilizar los rasgos morfológicos únicos en cada persona para la identificación. Ya en el siglo veinte, 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. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial o la voz [18].  Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación humana. La identificación biométrica se encuentra actualmente en un proceso de crecimiento con una amplia gama de aplicaciones basadas en el diseño de sistemas de Procesamiento Digital de Señales [18, 26].  **Reconocimiento Dactilar**  Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo [3].  Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella [3].  Las huellas digitales se toman de los dedos índices de ambas manos, tanto por la comodidad al capturarlas, como porque estos dedos están menos propensos que los pulgares a sufrir accidentes que dejen cicatriz [3].  Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente [5].  Los patrones de huellas digitales están divididos en 4 tipos principales, todos ellos matemáticamente detectables. Esta clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente [5].  En la figura aparecen 8 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 ( por ejemplo 10 horquillas 12 empalmes 15 islotes, etc) A estos puntos también se llaman minutae (minucias o minutias) término utilizado en la medicina forense que significa “punto característico” [33].    Con este conjunto de puntos, el método biométrico de huella digital genera un modelo en dos dimensiones que se almacena en una base de datos, con la debida referenciación de la persona que ha sido objeto del estudio [33].  Para ello, la ubicación de cada punto característico o minutia se representa mediante una combinación de números (*x.y*) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minutias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible. Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes [5, 33].   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | El dedo es leído por un captor de huellas. | El dedo es codificado por el captor. | Una plantilla es generada y la imagen es comprimida | El captor guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla. |   Los sistemas basados en reconocimiento de huellas son relativamente baratos (en comparación con otros biométricos, como los basados en patrones retinales); sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas. Otro factor a tener muy en cuenta contra estos sistemas es psicológico, no técnico: un sistema de autenticación de usuarios ha de ser aceptado por los mismos, y generalmente el reconocimiento de huellas se asocia a los criminales, por lo que muchos usuarios recelan del reconocedor y de su uso [5, 33]. |
| * 1. **Objetivos:**   **General**  Diseñar un prototipo de monitoreo y control de acceso al parqueadero de docentes de la Universidad de la Amazonia mediante identificadores de radio frecuencia y biometría, con el fin de administrar de forma eficiente esta área.  **Específicos**  Diseñar y Construir un prototipo de control de entrada y salida para los vehículos utilizando tecnología de identificación por radiofrecuencia (RFID).  Diseñar y construir un prototipo de identificación biométrico, con el fin de administrar los datos de los docentes y administrativos que utilizan el servicio de parqueadero.  Construir un automatismo a través de sensores de presencia para control de ocupación de cada sitio de estacionamiento de los vehículos en el parqueadero.  Implementar un sistema de información web información a través de metodologías de ingeniería del software que administre los datos de los controles de acceso al parqueadero de la Universidad de la Amazonia. |
| * 1. **Metodología Propuesta: (Si requiere calibración presentación metodología propuesta para la misma)**   El presente trabajo se desarrollará en cuatro fases:  **Diseño del Sistema de Identificación del Automotor ( Sistema RFD)**  En esta fase en primer lugar se determinarán los requerimientos del sistema de identificación del automotor, al igual que se determinarán las condiciones del medio que afectan severamente el desempeño del Hardware que lo compone. Igualmente se diseñará el sistema RFD mediante las siguientes actividades:   * Determinación de requerimientos del sistema RFD. * Selección de Tag. * Identificar la ubicación del Tag en los vehículos. * Selección del lector * Ubicación del lector * Definir el tipo de antena a construir para la recepción y transmisión de los tag. * Especificar el sitio de ubicación de la antena en la barrera de acceso. * Desarrollar el brazo mecánico de la barrera de acceso. * Construir el protocolo de comunicación entre barrera, antena y tag. * Construcción e instalación de la barrera de seguridad (Entrada y salida de vehículos).   **Diseño del Sistemas de Identificación Biométrico del Conductor del Automotor (ANFIS)**  En esta fase inicialmente se determinarán los requerimientos del sistema de identificación biométrico del conductor del automotor. Igualmente se diseñará el sistema ANFIS mediante:   * Selección del lector de huella digital. * Selección del método de comparación de la huella capturada con la que reposa en el sistema de información. * Desarrollo del sistema de captura y validación. * Diseño de estructuras para la captura de datos (ubicación de scanner)   **Diseño del Sistema de Control de Ocupación (Red ZigBee)**  Esta fase se desarrollará mediante:   * Diagnóstico actual del parqueadero * Desarrollo estratégico del plan de ordenamiento. * Determinación de las condiciones del medio ambiente que dificulten el establecimiento de comunicación inalámbrica. * Definición de los sensores para determinar la ocupación o no de un sitio de parqueo * Diseño de la red de comunicación inalámbrica de sensores * Determinación de la topología de red * Determinación del número necesario de Routers ZigBee * Selección del tipo de Reuter ZigBee a usar * Construcción e instalación de estructuras para routers y sensores.   **Diseño e Implementación del Sistema de Información Web de Administración**  Para esto se realizará:   * Diseño de la arquitectura del sistema. * Diseño de la base de datos del sistema. |
| * 1. **Resultados Esperados:**   Mejorar y controlar la zona de estacionamiento de los automotores de los docentes de la Universidad.  Ofrecer seguridad a la zona de estacionamiento de la Universidad.  Sistema web de gestión del estacionamiento de la Universidad.  Desarrollo de un Prototipo de acceso Rfid aplicable a varios entornos.  Desarrollo de un Prototipo de Acceso Biométrico para el registro, entrada y salida de los vehículos. |
| * 1. **Estrategia a utilizar para la transferencia de resultados:**   Socialización de cada uno de los componentes del proyecto a nivel académico, ofreciendo el modelo del desarrollo empleado.  Ofrecer a la sociedad productiva de la región el resultado del proyecto, su aplicabilidad, su nivel inversión y su beneficio, buscando los usuarios potenciales. |
| * 1. **Estrategia de comunicación:**   Desarrollo de los resultados en artículos de cada uno de los componentes del proyecto.  Foro académico de socialización de los resultados obtenidos en los eventos institucionales. |
| * 1. **Trayectoria del Grupo Investigador y Presentación del equipo de Investigadores:**   (Investigador Principal, Investigador Auxiliar y Jóvenes Investigadores)  Sergio Enrique Hernández Rubio y Heriberto Fernando Vargas Losada investigadores pertenecientes al grupo GIECOM reconocido por Colciencias, con la vinculación futura de varios estudiantes que desean desarrollar sus trabajos de grado. |
| * 1. **Cronograma de actividades:** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CONCEPTO** | **Semestre 1** | **Semestre 2** | **Semestre 3** |  |  |  |  |  |  |  |  |  |  |
| OBJETIVO GENERAL |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Diseñar y Construir un prototipo de control de entrada y salida para los vehículos utilizando tecnología de identificación por radio frecuencia (rfid). |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Prototipo RFID |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Determinación de requerimientos del sistema RFD. | **X** |  |  |  |  |  |  |  |  |  |  |  |
|  | Selección de Tag. |  | **X** |  |  |  |  |  |  |  |  |  |  |
|  | Identificar la ubicación del Tag en los vehículos. |  | **X** |  |  |  |  |  |  |  |  |  |  |
|  | Selección del lector |  | **X** |  |  |  |  |  |  |  |  |  |  |
|  | Ubicación del lector |  | **X** |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Diseño de Antena de recepción y transmisión |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Definir el tipo de antena a construir para la recepción y transmisión de los tag. |  |  | **X** |  |  |  |  |  |  |  |  |  |
|  | Especificar el sitio de ubicación de la antena en la barrera de acceso. |  |  | **X** |  |  |  |  |  |  |  |  |  |
| Diseño de la Barrera automática |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Desarrollar el brazo mecánico de la barrera de acceso. |  |  |  | **X** |  |  |  |  |  |  |  |  |
|  | Construir el protocolo de comunicación entre barrera, lector y tag. |  |  |  | **X** |  |  |  |  |  |  |  |  |
| Diseñar y construir un prototipo de identificación biométrico, con el fin de administrar los datos de los docentes y administrativos que utilizan el servicio de parqueadero. |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Sistema biométrico |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Determinación de los requerimientos del sistema de identificación biométrico del conductor. |  |  |  |  | **X** |  |  |  |  |  |  |  |
|  | Componentes necesarios para el sistema biométrico. |  |  |  |  |  | **X** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Sistema de validación del registro biométrico |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Desarrollo del sistema de captura y validación. |  |  |  |  |  |  | **X** |  |  |  |  |  |
| Construir un automatismo a través de sensores de presencia para control de ocupación de cada sitio de estacionamiento de los vehículos en el parqueadero. |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Control de ocupación |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Determinación de las condiciones del medio ambiente que dificulten el establecimiento de comunicación inalámbrica. |  |  |  |  |  |  | **X** |  |  |  |  |  |
|  | Definición de los sensores para determinar el estado del sitio |  |  |  |  |  |  |  | **X** |  |  |  |  |
| Diseño de la red inalámbrica de sensores |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Determinación de la topología de red |  |  |  |  |  |  |  | **X** |  |  |  |  |
|  | Determinación del número necesario de Reuters ZigBee |  |  |  |  |  |  |  | **X** |  |  |  |  |
|  | Selección del tipo de Reuter ZigBee a usar |  |  |  |  |  |  |  | **X** |  |  |  |  |
| Plan de ordenamiento de estacionamiento |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Diagnostico actual del parqueadero |  |  |  |  | **X** |  |  |  |  |  |  |  |
|  | Desarrollo estratégico del plan de ordenamiento. |  |  |  |  | **X** |  |  |  |  |  |  |  |
| Implementar un sistema de información web información a través de metodologías de ingeniería del software que administre los datos de los controles de acceso al parqueadero de la Universidad de la Amazonia. |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Sistema de Información web. |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | Determinación de requerimientos para el sistema de información Web |  |  |  | **X** | **X** |  |  |  |  |  |  |  |
|  | Diseño de la arquitectura del sistema. |  |  |  |  |  | **X** |  |  |  |  |  |  |
|  | Diseño de la base de datos del sistema. |  |  |  |  |  | **X** | **X** |  |  |  |  |  |
|  | Desarrollo del prototipo del sistema de información Web |  |  |  |  |  |  | **X** | **X** | **X** | **X** | **X** | **X** |

|  |
| --- |
| * 1. **Consideraciones adicionales:**   Este proyecto integra diferentes áreas como son redes, teleinformática, control, análisis, ingeniería de software y bases de datos, donde los estudiantes puede participar de manera activa y proponer ideas para futuros desarrollos de tesis, siempre buscando las mejores soluciones a problemas ya sea aplicando conocimiento o desarrollando aportes tecnológicos. |
| 1. **PRESUPUESTO** |
| * 1. **Fuentes de Financiación:** |
| * + 1. Recursos Externos (Universidad de la Amazonia)     2. Recursos Propios (Recursos que el grupo de investigación buscará con apoyos de empresas, grupos de investigación interesados en la propuesta) |
| * 1. **Equipos: 8.000.000**   Kit de desarrollo RFID.  Computadores personales.  Enrutadores (Wifi).  Enrutadores ZigBee  Lector de Biométrico (Huella). |
| * 1. **Materiales e insumos y servicios técnicos: 6.000.000**   Tag pasivos y activos RFID.  SDK para desarrollo Biométrico.  Software para desarrollo (.net y java).  Motor de Base de Datos (Oracle, Sql server, Mysql o Postgres).  Sensores de ocupación ZigBee. |
| * 1. **Gastos de transporte para salidas al campo: 3.000.000**   Estos recursos serán utilizados en el momento en que algunos materiales e insumos no existan en la Universidad pero que otras instituciones pueden realizar estos préstamos. |
| * 1. **Compra material bibliográfico: 3.000.000** |
| * 1. **Publicaciones: 2.000.000** |

Los recursos específicos determinados en los puntos 4, detallan algunos rubros generales del presupuesto, es de aclarar que no son los totales del presupuesto del proyecto.

|  |  |  |  |
| --- | --- | --- | --- |
| **PRESUPUESTO** |  |  |  |
|  |  | En miles de pesos |  |
| **CONCEPTO** | **Solicitud Externa** | **Contrapartida** | **Total** |
|  |  |  |  |
| **I. GASTOS DE FUNCIONAMIENTO** |  |  |  |
|  |  |  |  |
| **1 Servicios personales** |  |  |  |
| 1.1 Nómina |  |  |  |
| **2 Gastos generales** |  |  | **8000** |
| 2.1 Materiales y suministros |  | 6000 | 6000 |
| 2.2 Servicios públicos |  | 2000 | 2000 |
|  |  |  |  |
| **II. GASTOS DE INVERSION** |  |  |  |
|  |  |  |  |
| **1 Gastos operativos** |  |  | **41000** |
| **1.1 Gastos de personal** |  |  | **30000** |
| 1.1.1 Equipo ejecutor |  | 17000 | 17000 |
| 1.1.2 Asesorías y consultorías | 10000 |  | 10000 |
| 1.1.3 Mano de obra no calificada |  | 3000 | 3000 |
|  |  |  |  |
| **1.2 Viáticos y gastos de viaje** |  |  | **3000** |
| 1.2.1 Alojamiento y alimentación |  | 2000 | 2000 |
| 1.2.2 Transporte |  | 1000 | 1000 |
| **1.3 Educación y capacitación** |  |  | **3000** |
| 1.3.1 Talleres |  | 3000 | 3000 |
| **1.4 Impresos y publicaciones** |  | 2000 | **2000** |
| **1.5 Insumos** |  | 3000 | **3000** |
|  |  |  |  |
| **2. Gastos de inversión** |  |  |  |
|  |  |  |  |
| **2.1 Maquinaria y equipo** |  | 8000 | **8000** |
| **TOTAL** | 10000 | 47000 | 57000 |

|  |
| --- |
| 1. **REFERENTE BIBLIOGRÁFICO** 2. 802.15.4, Part 15.4: Wireless Medium Access Control(MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs). 3. Juels, R. Rivest, andM. Szydlo. The blocker tag: selective blocking of RFID tags for consumer privacy. In *10th ACM Conf. Comp. and Comm. Sec.*, pages 103–111, 2003. 4. A.J. Willis and L. Myers, “A cost-effective fingerprint recognition system for use with low-quality prints and damage fingertips”, Pattern Recognition, vol. 34, No 2, pp. 255-270, February 2001. 5. B. Miller, “*Vital signs of identity”, IEEE Spectrum,* 31(2), 1994, pp. 22-30. 6. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, 2003. 7. E. Schuman. RFID trials show mixed results. eWEEK.com, Nov. 15, 2006. 8. G. Karjoth and P.Moskowitz. Disabling RFID tags with visible confirmation: clipped tags are silenced. In *2005 ACM Workshop on Privacy in the Electronic Society*. 9. H. Tsai, K. Chen, and Y. Liu, “*Report on Demonstration (DEMO) of Radio Frequency Identification (RFID) Tracking System*,” Argonne National Laboratory, Argonne, IL, September 30, 2008. 10. H.C. Tsai, K. Chen, Y. Liu, et al., “*Applying RFID Technology in Nuclear Materials Management*,” Packaging, Transport, Storage & Security of Radioactive Material, Vol. 19, No. 1, 2008. 11. <http://www.palowireless.com/zigbee/tutorials.asp> 12. IEEE 802 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, IEEE Computer Society, 2003. 13. J. Brusey, C. Floerkemeier, M. Harrison, and M. Fletcher. Reasoning about uncertainty in location identification with RFID. In *Workshop on Reasoning with Uncertainty in Robotics at IJCAI*, Aug. 2003. 14. J. Lindsay and W. Reade. Cascading RFID tags. Dec. 6, 2012, http://www.jefflindsay.com/rfid3.shtml. 15. Jacob Munk-Stander, Implementing a ZigBee Protocol Stack and Light Sensor in TinyOS,White Paper dated October 2005. 16. K. Chen, H. Tsai, Y. Liu, and J. Shuler, “*A Radiofrequency Identification (RFID) Temperature-Monitoring System for Extended Maintenance of Nuclear Materials Packaging*,” Proceedings of 2009 ASME Pressure Vessels and Piping Division Conference, Prague, Czech Republic, July 2009. 17. K. Ramakrishnan and D. Deavours. Performance benchmarks for passive UHF RFID tags. In *13th GI/ITG Conf. Measurement, Modeling, and Eval. of Comp. and Comm. Sys.*, pages 137-154, 2006. 18. Kohvakka, M., Kuorilehto, M., Hännikäinen, M., & Hännikäinen, T. D. (2006). Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications. Paper presented at the Proceedings of the 3rd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Terromolinos, Spain. 48-57. 19. L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, Intelligent biometric techniques in fingerprint and face recognition, 1999. 20. L. Ni, Y. Liu, Y. Lau, and A. Patil. LANDMARC: Indoor location sensing using active RFID. In *Wireless Networks*, 10(6): 701-710. 2004. 21. M. Kodialam and T. Nandagopal. Fast and reliable estimation schemes in RFID systems. In *Proc. 12th MOBICOM*, pages 322–333, Sep. 2006. 22. M. Rieback, B. Crispo, and A. Tanenbaum. The evolution of RFID security. In IEEE Perv. Comp. 5(1): 62-69, 2006. 23. N. Vaidya and S. Das. RFID-based networks - exploiting diversity and redundancy, UIUC, WINGS Lab TR, 2006. 24. P. Kinney, ZigBee Technology: Wireless Control that Simply Works, White Paper dated 2 October 2003. 25. Pister K. S. J., Kahn J. M., and Boser B. E. (1999). Smart dust: Wireless networks of millimeter-scale sensor nodes. In 1999 UCB Electronics Research Laboratory Research Summary 26. R. Shawn, G. Minos, and J. Michael. Adaptive cleaning for RFID data streams. In *Proc. 32nd VLDB*, pages 163–174, 2006. 27. Ram Sathappan, *DSP for Smart Biometric Solutions*, Digital Signal Processor Group, Texas Instruments Inc., 2003. 28. Ran, P., Sun, M., Zou, Y. (2006). ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing. APSCC '06, December 2006, 400-404. 29. S. Garfinkel, A. Juels, and R. Pappu. RFID privacy: an overview of problems and proposed solutions. In *IEEE Security and Privacy Magazine*, 3(3): 34–43, 2005. 30. S. Inoue, D. Hagiwara, and H. Yasuura. Systematic error detection for RFID reliability. In *Conf. Avail., Rel. and Sec. (ARES 2006)*, pages 280–286. 31. Schlessman, J., Shim, J., Kim, I., Baek, Y. C., & Wolf, W. (2006). Low power, low cost, wireless camera sensor nodes for human detection. Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, October 2006, 363-364. 32. Sheng-Fu Su, The Design and Implementation of the ZigBee Protocol Driver in Linux, White Paper dated 26 July 2005. 33. Tseng, Y., & Pan, M. (2006). Quick convergecast in ZigBee/IEEE 802.15.4 treebased wireless sensor networks. MobiWac '06: Proceedings of the international workshop on Mobility management and wireless access, 2006, 60-66. 34. U. Halici, G. Ongun, “Fingerprint classification through Self-Organizing features maps modified to treat uncertainties”, The Proceedings of the IEEE, vol. 84, No 10, pp 1497-1512, 1996 35. William Stalling, “Wireless Communication and Networks”, Fourth Edition, Pearson Publication Limited, 2004, Pp 39-118. 36. Wood, S.D, et al., Journal of Research of the National Bureau of Standards, Vol. 83, Issue 3, pp. 247–263, May-June, 1978. 37. ZigBee Specification v1.0, ZigBee Alliance, December 14th, 2004. |