



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Sistema Basado en RFID para Mejorar la Seguridad de Acceso a las oficinas de la
Gerencia Regional de Transporte y Comunicaciones -La Libertad, 2019”

TESIS PARA OBTENER TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Br. Chunga Aguilar, Rixi Alexandra (ORCID:0000-0001-5139-3519)

Br. De la Cruz Infantes, Juan Carlos (ORCID:0000-0003-4965-8113)

ASESOR:

Dr. Hugo Romero Ruiz (ORCID:0000-0002-6179-8736)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de Servicio de Redes y Comunicaciones

Trujillo –Perú

2019

DEDICATORIA

En primer lugar, le doy gracia a Dios, por guiarme en la elección de mi carrera y respaldarme hasta el final. Gracias en especial a mi familia en gran parte a mi padre y a mi madre, por su incondicional apoyo tanto moral como en lo económico desde mis inicios hasta el final de mi carrera.

Chunga Aguilar, Rixi Alexandra.

En especial a mi madre ya que es y será mi motivación en mi vida, porque sin su apoyo no hubiera logrado esta meta, sobre todo a toda mi familia y mis compañeros quienes me brindaron su apoyo incondicional en todo momento.

De La Cruz Infantes, Juan Carlos

AGRADECIMIENTO

Primeramente, agradecemos a Dios
por ser nuestro guía celestial
acompañándonos en el día a día,
de nuestras vidas.

Sobre todo, un agradecimiento especial a
nuestros profesores por su formación y
conocimientos brindados, en especial a
nuestro asesor, por habernos dado su
constante ayuda y aportando con
sus grandes conocimientos
para culminar con gran
éxito esta tesis.

Chunga Aguilar, Rixi Alexandra.

De La Cruz Infantes, Juan Carlos

PÁGINA DEL JURADO

DECLARATORIA DE AUTENTICIDAD

Declaratoria de autenticidad

Yo Rixi Alexandra Chunga Aguilar con DNI N° 73088995 y Juan Carlos De La Cruz Infantes con DNI N° 70258611, ponemos en cumplimiento con las disposiciones vigentes consideradas dentro del Reglamento de Grados y Títulos de la Universidad César Vallejo, Facultad de Ingeniería, Escuela de Ingeniería de Sistemas, declaramos bajo juramento que toda la documentación y todos los datos e información es auténtico y veraz en la presente tesis.

En ese sentido, asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada por lo cual nos sometemos a lo dispuesto en las normas académicas de la Universidad César Vallejo.

Trujillo ,24 de diciembre del 2019



Br. Rixi Alexandra Chunga Aguilar
DNI 73088995



Br. Juan Carlos De La Cruz Infantes
DNI 70258611

ÍNDICE

DEDICATORIA	vii
AGRADECIMIENTO	viii
PÁGINA DEL JURADO	ix
DECLARATORIA DE AUTENTICIDAD	xi
ÍNDICE	xii
ÍNDICE DE TABLAS	xiii
ÍNDICE DE ILUSTRACIONES	xiii
RESUMEN.....	xiv
ABSTRACT	xv
I. INTRODUCCIÓN.....	1
II. MÉTODO.....	10
2.1. Diseño de la investigación.....	10
2.1.1. Tipo de investigación.....	10
2.1.2. Clasificación.....	10
2.1.3. Identificación de Variables	11
2.1.4. Operacionalización de variables:.....	12
2.2. Población y muestra	14
2.3. Técnica e Instrumento de recolección de Datos, validación y confiabilidad	15
2.3.1. Técnica e Instrumento de recolección de Datos	15
2.3.2. Validez del Instrumento	15
2.3.3. Confiabilidad.....	16
2.4. Procedimiento.....	18
2.5. Método de Análisis de Datos	19
2.6. Aspecto Ético:.....	20
III. RESULTADOS.....	21
3.1. Contrastación de Hipótesis:	21
IV. DISCUSIÓN.....	37
V. CONCLUSIONES.....	41
VI. RECOMENDACIONES.....	42
VII. REFERENCIAS	43
VIII. ANEXOS	46

ÍNDICE DE TABLAS

Tabla 1. Características de Etiquetas Activas.....	7
Tabla 2. Clasificación de Frecuencia	8
Tabla 3. Operacionalización de Variables.....	12
Tabla 4. Indicadores	13
Tabla 5. Técnica e Instrumento	15
Tabla 6. Tabla de valoración para el Alpha de Cronbach	18
Tabla 7. Contratación Hipótesis - Indicador 01	22
Tabla 8. Criterio para determinar la normalidad - Indicador 01	23
Tabla 9. Contratación Hipótesis - Indicador 02	26
Tabla 10. Criterio para determinar la normalidad - Indicador 02.....	28
Tabla 11. Tabulación de encuesta de satisfacción – Pre Test.....	31
Tabla 12. Tabulación de encuesta de satisfacción – Post Test	32
Tabla 13. Contratación del PRE y POST test	33
Tabla 14. Criterio para determinar la normalidad - Indicador 03	35
Tabla 15. Presupuesto	82
Tabla 16. Flujo de Caja	85

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Bandas de frecuencia utilizando RFID	6
Ilustración 2. Clasificación de la investigación	10
Ilustración 3. Vista de Datos	16
Ilustración 4. Vista de Variables.....	17
Ilustración 5. Fiabilidad de la Encuesta	17
Ilustración 6. Prueba de normalidad - Indicador 01	23
Ilustración 7. Prueba de normalidad-Indicador 2.....	27
Ilustración 8. Resultados prueba t-Student – Indicador 03.....	35
Ilustración 9. Indicador 1: cantidad de accesos no autorizados a las oficinas restringidas	38
Ilustración 10. Indicador 2: Cantidad de registros de accesos dentro de las oficinas restringidas:....	39
Ilustración 11. Indicador 3: Nivel de satisfacción respecto a la seguridad en las oficinas restringidas.	40
Ilustración 12. Diagrama de caso de Uso	64
Ilustración 13. Diagrama de robustez	65
Ilustración 14. Diagrama de modelo de Dominio	66
Ilustración 15. Proceso de Datos mediante un modelo Racional.....	67

RESUMEN

En el presente trabajo de investigación se implementó un sistema de control de acceso basado en tecnología RFID en la Gerencia Regional de Transporte y Comunicaciones con la finalidad de mejorar la seguridad en las oficinas de la institución, permitiendo un control adecuado y seguro en las horas no laborables dentro de las áreas restringidas. Donde para lograr esto en el primer capítulo definimos el planteamiento del problema, al igual que nuestro objetivo principal como también nuestros objetivos específicos. En el segundo capítulo utilizamos como método de estadística la prueba de Shapiro, este método nos permitió hallar el pretest y post test de nuestra investigación, que a su vez sirvieron para realizar evaluaciones de los indicadores del instrumento de observación. En el tercer capítulo, utilizamos la herramienta SPSS logrando ordenar nuestros valores encontrados y verificar que cumple con el requisito de confiabilidad. En el cuarto capítulo, realizamos la discusión de nuestros antecedentes de tesis consultadas y explicamos de manera clara y concisa del aporte hacia el presente trabajo de investigación, en el quinto capítulo realizamos las conclusiones que nos llevó a demostrar de qué manera pudimos alcanzar nuestro objetivo principal y nuestros objetivos específicos, y en el último capítulo se realizó algunas recomendaciones para futuras investigaciones.

Palabras Claves: Tecnología RFID, acceso, seguridad, Test de Shapiro, SPSS

ABSTRACT

In the present research work, an access control system based on RFID technology was implemented in the Regional Management of Transport and Communications in order to improve security in the institution's offices, allowing adequate and safe control in non-hours working within restricted areas. Where to achieve this in the first chapter we define the problem statement, as well as our main objective as well as our specific objectives. In the second chapter we used the Shapiro test as a statistical method, this method allowed us to find the pretest and post test of our research, which in turn served to evaluate the indicators of the observation instrument. In the third chapter, we use the SPSS tool, managing to order our found values and verify that it meets the reliability requirement. In the fourth chapter, we carry out the discussion of our consulted thesis antecedents and explain in a clear and concise way the contribution towards the present research work, in the fifth chapter we make the conclusions that led us to demonstrate how we could achieve our main objective and our specific objectives, and the last chapter made some recommendations for future research.

KEYWORDS: RFID technology, access, security, Shapiro test, SPSS

I. INTRODUCCIÓN

En la actualidad la tecnología avanza cada vez más, y conforme va creciendo surgen nuevas ideas, nuevas necesidades que hoy por hoy gracias al gran avance de la tecnología hacen que nuestra vida se facilite de alguna u otra forma, pero así como la tecnología puede facilitar la vida de muchos, también puede ser una de las herramientas más poderosas tanto para una organización pública como privada, aportando así tanto en el desarrollo como en la seguridad de ellos mismos, por otra parte gracias a la tecnología muchas organizaciones llegan a ser competitivas, pero para lograrlo deben apostar por ello, y en un mundo competitivo como el de ahora con mucha más razón, según (Redondo A., 2017) sostiene en su informe que en un mundo globalizado en el que vivimos, la competencia es feroz y competimos con empresas del otro punto del planeta, que pueden tener un sistema de regulación más beneficioso que el tuyo, por lo que da a entender es que en un mundo globalizado, competimos con empresas a nivel mundial que pueden tener los mismos sistemas pero no los mismos beneficios.

En este sentido que se obtendría si nosotros aplicáramos estas tecnologías a nuestro favor por lo que es importante tener en cuenta para que una organización sea competitiva debe cubrir sus necesidades con tecnologías que les permita cubrirlos para luego así alcanzar esos beneficios y ser competitivo en el mercado empresarial, por lo que debemos tener en cuenta, que hoy en día en muchas organizaciones buscan seguridad de información, en sistemas que les de esos beneficios, pero creemos que no es solo dar seguridad a la información sino también dar seguridad a los exteriores de la organización, es por ello que según la información extraída de FerMaxProfesional nos señala que hoy en día es más frecuente que en muchas empresas obtén por soluciones de control de acceso, ya que gracias a estos sistemas les permite tener un mayor control de quien accede a las instalaciones.

Mientras que por otro lado nos menciona también que en nuestra actualidad en algunas organizaciones las llaves representan un problema de seguridad, ya que si lo vemos desde otra perspectiva una llave no brinda tanta seguridad como se cree, ya sea porque se pueden extraviar o extraer un duplicado y terminar en manos de terceras persona, provocando que en una organización tenga que optar por cambiar todas las cerraduras, que la llave da acceso, por lo que con un sistema de control de acceso mediante tarjeta de proximidad solo bastaría

con bloquear el acceso a la tarjeta sin necesidad de algún cambio o gasto para la organización. (fermax, 2016)

En realidad, la seguridad en una organización hoy en día se ha vuelto un factor principal por lo que muchas de ellos llegan a optar por tecnologías modernas para sobre guardar toda la información que ellos manejan, ya sea documentos importantes o material confidencial, por ello es importante recalcar la importancia que tiene la seguridad en nuestra actualidad, ya que de alguna u otra forma están contribuyendo al crecimiento de ellos mismos, por otra parte para poder optar por estas tecnologías es importante que toda empresa tenga conocimiento de que ventajas brindara tal tecnología y de qué manera les favorecerá, según (Inditar, 2017) nos indica que actualmente, los sistemas de control de acceso es una tipología muy utilizada en organizaciones debido al gran incremento que estas brinda al utilizarlas dentro de sus instalaciones, ya que ofrece ventajas y facilidades tanto a la propia organización como a los clientes, porque gracias a esta tecnología se puede controlar, gestionar y monitorear los movimientos de personas que entran y salen de cualquier lado de una determinada organización.

Por lo tanto es importante resaltar que la tecnología avanza de acuerdo a como se vayan aplicando en cada país, ya que países desarrollados como Estados Unidos, Japón son gran ejemplo de ello, por lo tanto vale mencionar que a comparación de nuestro país, la tecnología no es muy aprovechada en el ámbito empresarial, según (Diario El Comercio, 2018) el Perú sigue rezagado en tecnología, donde nos señala que en contexto de ser competitivo en materia digital, nuestro país se ubica ultimo a nivel mundial, según indico Ranking de competitividad digital, elaborado por el Institute for Management Development (IMD) junto a Centrum Católica como socio local. De esta manera nos damos cuenta de que en nuestro país no se está siendo competitivo en aspecto tecnológico, por lo que creemos que no se está llevando una adecuada implementación de tecnología en ciertas organizaciones, es decir no todas las organizaciones de nuestro país, optan por implementar tecnologías que ayuden a solucionar sus problemas o cubrir sus necesidades.

El cual para esta oportunidad hemos elegido trabajar con una organización publica como lo es la Gerencia Regional de Transporte y Comunicaciones, donde haciendo una encuesta previa se logró percibir ciertos problemas y necesidades con respecto a las áreas que son

restringidas, tales como son el área de módulo de impresión de licencias u el área de conocimientos, ya que en dichas áreas solo está permitido el ingreso de personal autorizado, en el cual la única forma de ingreso habitual es utilizando una llave, como ya se mencionó en párrafos anteriores una llave no brinda tanta seguridad como se cree, por ende se pudo percibir ciertas problemas, sobre todo no cuentan con reportes de entrada y salida del personal autorizado, ya que no se tiene un horario restringido en las horas no laborables en las oficinas, poniendo en riesgo toda la información e insumos que son manejadas por las oficinas de la Gerencia Regional de Transporte y Comunicaciones-La Libertad.

Por ende, dada la problemática señalada, se detectaron los siguientes problemas:

P1: Se detectó cierta cantidad de incidencias (Ingresos indebidos) en las distintas áreas.

P2: No se han encontrado registros diarios actualizados de acceso a las oficinas restringidas de la Gerencia Regional de Transporte y Comunicaciones (Mal control de las entradas y salidas en el área en horas no laborables causando que no se cuenten con reportes de los accesos diarios a las áreas.)

P3: Se ha observado bajo nivel de Satisfacción con respecto a seguridad en tanto a acceso a las áreas restringidas.

En cuanto a trabajos previos que nos darán un aporte en el desarrollo del presente proyecto, se tomaron en cuenta los siguientes, a nivel internacional se consideró el proyecto titulado “Automatización para el control de acceso utilizando dispositivos Móviles y RFID” desarrollado por Rafael de la Rosa Flores, David E. Muñoz Morales, Ervic Pérez Mendoza, José Luis Mora Flores y Hilda Castillo Zacatelco en la Benemérita Universidad Autónoma de Puebla, de la ciudad de Puebla, México en el año 2017, en el que se realizó una arquitectura de hardware con la tecnología de identificación de Radio Frecuencia (RFID), donde se utilizó también un dispositivo Arduino y un dispositivo Ethernet shield con la finalidad de controlar el acceso, en esta oportunidad en un laboratorio, automatizando así los procesos que ahí se realizan, permitiéndoles determinar quién y en qué hora se hizo uso de determinado laboratorio. (Rafael de la Rosa Flores, 2017) en el cual de esta investigación se va a tomar en cuenta la automatización de procesos y de qué manera se implementó el sistema basado en RFID.

Mientras que por otro parte de la siguiente tesis titulada “Sistema de control de acceso y monitoreo con la Tecnología RFID para el departamento de Sistema de la Universidad Politécnica Salesiana Sede Guayaquil” el cual fue desarrollado por Zynnia Verónica Vargas Vergara en la universidad Politécnica Salesiana Sede Guayaquil, Ecuador en el año 2013 en el que se implementó un sistema que fue elaborado en NetBeans a través de una conexión UDP donde el monitoreo se efectuó en LabVIEW utilizando la tecnología RFID, la cual nos permite identificar una etiqueta de tipo electrónico a distancia, esta emite periódicamente una señal de Radiofrecuencia hacia el módulo lector RFID, ayudando a disminuir el costo con el objetivo de reemplazar los equipos perdidos, tener claridad a la hora de necesitar los laboratorios y así poder obviar el control y la supervisión por parte del personal de mantenimiento (Vergara, 2013) dándonos una idea del proceso de implementación de la tecnología RFID, en el cual nuestro proyecto se desarrollara teniendo en cuenta el proceso empleado en esta investigación.

Por otro lado, a nivel nacional se consideró el siguiente proyecto titulado “Diseño del sistema de control de asistencia en la agencia mercado de la Caja Huancayo aplicando tarjeta de proximidad de tecnología RFID” el cual fue desarrollado por Rodolfo Steven Martínez Verand en la Universidad Continental de la ciudad de Huancayo, Perú en el año 2017, en el que se implementó un sistema de control de asistencia basado en una metodología de desintegración funcional que llevo a un análisis e identificación de requerimientos y funcionalidades del sistema planteado tanto a nivel de hardware como software. (Vernard, 2017) por lo cual se tomará en cuenta la metodología empleada en el que nos permitirá tener un análisis previo e identificar los requerimientos y funcionalidades de nuestro sistema.

Mientras que, por otra parte, de la tesis titulada “Diseño de un sistema de seguridad aplicado al laboratorio de Telecomunicación usando Tecnología RFID y GSM” desarrollado por Elvis Andrés Molino Pardo en la Universidad Nacional de Piura, Perú en el año 2015 el cual se planteó un diseño de sistema de seguridad elaborado en tecnología RFID y GSM, en el que le permitió identificar equipos, reportando a través de mensajes de texto en las horas no laborables, proponiendo seguridad a los laboratorios. (Pardo, 2015), el cual del siguiente proyecto nos permitirá tener una idea como el sistema RFID puede enviar a través de un

mensaje de texto un reporte de las actividades que está sucediendo en un área y de qué manera se implementó esta función permitiendo aplicarla en el desarrollo de nuestro sistema.

Respecto a seguridad de la información la norma técnica peruana (NTP –ISO/IEC 27001), en el acápite A.8.1 Responsabilidad por los activos, cita “Identificar los activos de la organización y definir responsabilidades de protección apropiadas” (INDECOPI, 2008)

En cuanto si hablamos de seguridad en definición es tener conocimiento y certeza sobre algo que tiene ausencia de peligro y riesgo, esto quiere decir que la seguridad abarca desde una necesidad de mantener seguro algún objeto o persona, en el cual permite evitar riesgos y garantizar un buen funcionamiento.

Es por ello la importancia que tienen hoy en día las organizaciones hacia sus activos, ya sean físicos y digitales se han vuelto una parte fundamental ya que de alguna manera se exponen a diferentes amenazas, ya sea fraude, sabotaje, espionaje y entre otras amenazas que se observan en diferentes organizaciones y muchos de ellos son ocasionados ya sea por hackers o empleados negligentes que de alguna manera buscan dañar la organización tal como nos menciona (Universidad veracruzana, 2018).

Hoy en día en las organizaciones es importante ver la seguridad como un valor corporativo, ya que hoy por hoy como ya se mencionó anteriormente la seguridad se ha vuelto una parte fundamental ya que no solo brinda beneficios y hace a las organizaciones más competitivas, sino que gracia a ello trae consigo un gran efecto social en los países permitiendo tener desarrollo y competitividad.

Según (Mutual de Seguridad, 2018) nos señala que al gestionar la seguridad como valor corporativo no viene a ser lo mismo que con un valor competitivo, a pesar de que ambas son muy fundamentales para una organización, porque gracias a estos dos valores una organización puede alcanzar una cultura de excelencia no solo en el ámbito de seguridad sino también impulsa hacia una cultura de calidad, eficiencia e innovación.

Según Revista web de la empresa “PROSEGUIR” (Proseguir Seguridad de confianza, 2017) empresa encargada de brindar servicios de seguridad en organizaciones el cual define el control de acceso como sistema que permite tener un mejor control, rastreo y administración de los clientes y trabajadores que visitan las diferentes áreas de una organización ya sea

pública o privada de la mano de tecnologías permitiendo así asegurar el registro de todo lo acontecido dentro de una determinada organización, que es lo que queremos lograr con nuestro sistema basado en tecnología RFID.

La tecnología RFID según (Reviriego, 2016) describe a esta tecnología como un sistema de identificación que funciona de manera inalámbrica a través de radiofrecuencias, el cual puede almacenar y recuperar datos, en donde la misión de esta tecnología es identificar un dispositivo RFID de un lector, identificándose de inmediato y sin contacto alguno.

De acuerdo con (by.com, 2018) nos señala que la tecnología de radiofrecuencia viene a ser un sistema que nos permite tener dos o más equipo en constante comunicación en donde se puede emitir señales de radio y el otro responde en función de la señal recibida.

Principal frecuencia RFID:

-UHF RFID Pasivo (860-960 MHz)

-NFC y HF RFID Pasivo(13,56MHz)

Esta tecnología funciona a través de un lector que está continuamente lanzando peticiones mediante radiofrecuencia con destino al chip que está integrado en la tarjeta en el cual al recibir la petición automáticamente emite una respuesta permitiendo una comunicación entre el lector y la tarjeta brindando seguridad de identificación, precisión y sobre todo efectuándose en tiempo real.

Ilustración 1. Bandas de frecuencia utilizando RFID

Banda de frecuencias	Descripción	Rango
125 kHz	LF (Baja Frecuencia)	Hasta 50 cm.
13,56 MHz	HF (Alta Frecuencia)	De 8 cm.
400 MHz – 1.000 MHz	UHF (Ultra Alta Frecuencia)	De 3 a 10 m.
2,45 GHz – 5,4 GHz	Microondas	Más de 10 m.

Fuente: by.com

Los tags (etiquetas) es un pequeño dispositivo que en el interior cuenta con un chip pequeño y una antena para comunicarse con el lector, el cual cuenta con un número (ID) de serie que

lo hace único entre los demás y poder así identificarse, sobre todo este dispositivo también cuenta con una pequeña memoria que le permite guardar datos, que los lectores son capaces de leer y escribir.

Las tarjetas RFID son una llave incopiable así nos señala (tarjetashid-mifare-rfid.com, 2018) el cual nos dice que estas etiquetas no requieren alimentación eléctrica interna, mientras que las tarjetas activas sí lo requieren, por lo tanto se considera como una ventaja el uso de radiofrecuencia, ya que no se requiere visión directa entre emisor y receptor.

Es por ello que el uso de Tecnología RFID vendría a ser uno de los componentes más importantes al implementar tecnología dentro de una empresa, ya que es sin duda la utilización de etiquetas del tipo RFID, serían las encargadas para transportar información relevante, debido a las múltiples ventajas que estas brinda. (Tecnologías Informatica , 2018)

Por lo cual existen dos tipos de etiquetas RFID que lo diferencia por el funcionamiento que cumple cada uno:

Etiqueta RFID Pasivos: Se activa cuando reciben la señal de cercanía de un RFID, en la cual captura la energía necesaria para utilizar para su activación. Permite alcanzar una distancia de entre 10 cm a unos pocos metros tiene como antena de frecuencia HF y UHF.

Por lo general son conocido como semipasivas o semiactivas, en el que requiere de una alimentación independiente para funcionar por lo cual cuenta con la utilización de la energía de una batería interna que se encuentra en la etiqueta.

Tabla 1.Características de Etiquetas Activas

Características
> Fuente de alimentación propia mediante batería tarjeta proximidad de larga duración.
> Distancias de lectura escritura mayor de 10 cm a 100m generalmente.
> Memoria generalmente entre 4 y 32 Kbyte.
> Diversas tecnologías y frecuencias. <ul style="list-style-type: none">▪ Hasta 868 MHz (UHF) o según estándares aplicados.▪ 2,4 GHz utilizados (banda ISM, Industrial Scientific and Medical), la misma que para dispositivos Wireless LAN.▪ Batería de larga duración (generalmente batería tarjetas proximidad de litio/dióxido de manganeso)

Elaboración: Propia

Según (tarjetashid-mifare-rfid.com, 2018) nos señala los tipos de frecuencias y sus características a las cuales son orientadas dependiendo el rango de distancia tal como se muestra en el siguiente cuadro.

Tabla 2. Clasificación de Frecuencia

Frecuencia	Características
125 KHz: Baja Frecuencia (LF)	Aplicaciones de lectura de 5 cm de distancia, Control de acceso de personas. No se recomienda para identificar vehículos u objetos. Requiere línea de vista libre entre tarjeta y lector.
13.56 MHz: Alta Frecuencia (HF)	Aplicaciones de lectura de 60 cm de distancia, Control de acceso de personas dentro de vehículos. La señal puede pasar a través del vidrio.
433.8 MHz: Muy Alta Frecuencia (VHF)	Aplicaciones de lectura de hasta 100m, Con un buen balance entre penetración y distancia. Control de acceso vehicular, Monitoreo de equipo e inventarios en tiempo real.
902 MHz: Ultra Alta Frecuencia (UHF)	Aplicaciones de lectura de 400m, Muy buen control del rango de la señal, sensible a interferencias por agua ya que disminuye el rango (incluyendo el cuerpo humano).

Elaboración: Propia

De acuerdo con (Misana Ingeniería, SL, 2017) nos señala que gracias a este módulo podemos enviar y recibir SMS, datos GPRS (conexiones TCP, UDP y FTP) y de hacer peticiones HTTP. Módulo adecuado para aplicaciones M2M (máquina a máquina), en el que también nos dice que este pequeño, ligero y robusto dispositivo fue diseñado para ser incorporado de manera modular a cualquier solución electrónica en el que requiera de conectividad GPRS.

De acuerdo con lo descrito en párrafos anteriormente acerca de la problemática se formuló el siguiente problema: ¿De qué manera un sistema basado en Radio Frecuencia de Identificación - RFID mejora la Seguridad de Acceso a las oficinas de la Gerencia Regional de Transporte y Comunicaciones - La Libertad 2019? Es por ende el presente proyecto de investigación es justificado a nivel tecnológico, porque actualmente muchas organizaciones tanto públicas como privadas buscan mejorar su organización a través de implementación de tecnología y sobre todo lograr así mejorar sus procesos, por ende, también buscan mejorar la seguridad de su información, por lo cual implementar un sistema basado en RFID, permitirá a la Gerencia Regional de Transporte y Comunicaciones mantener en constante control los

accesos a las áreas restringidas, brindando mayor seguridad más de lo que daría un cerradura y una llave, porque no solo permitirá dar acceso sino que también guardara información de toda la actividad durante las horas no laborables, por ende el sistema trabaja a través de una tarjeta donde solo podrán tener acceso las personas encargadas del área siendo así que los accesos sean más rápido y seguro.

Mientras que por el lado operativo al implementar un sistema basado en RFID permitirá a la Gerencia Regional de Transporte y Comunicaciones mejorar el nivel de seguridad, ya que a través de ella permitirá a la organización, llevar un control adecuado de los ingresos y salidas a las áreas restringidas en horas no laborables, permitiendo así sobre guardar todo los equipos y sobre todo la información manejada por ellos mismo y por el lado económico con la implementación de este sistema ya no habrá necesidad de hacer gasto de dinero en compra de cerradura y llaves, ya que, de alguna forma, con este sistema ya no habrá necesidad de hacer esto cuando se extravíe una llave ya que con este sistema solo bastara con bloquear el acceso si esto llegara a ocurrir en esta ocasión con las tarjetas, aportando no solo en la seguridad sino en lo económico.

Para ello en la presente investigación se planteó la siguiente Hipótesis: Con un sistema basado en RFID se mejoró significativamente la seguridad de acceso a las oficinas de la Gerencia Regional de Transporte y Comunicaciones-La Libertad, por otra parte como objetivo general se planteó lo siguiente: “Mejorar la seguridad de acceso a las oficinas de la Gerencia Regional de Transporte y Comunicaciones-La Libertad con un Sistema basado en RFID” mientras que como objetivos específicos se plantearon los siguientes:

Como primer objetivo nos planteamos disminuir la cantidad de accesos no autorizados a las oficinas restringidas, es decir reducir la cantidad de accesos no permitidos a personas que no son de las oficinas y que se generan en cada cierto tiempo, por otro lado como segundo objetivo se planteó incrementar la cantidad de registros de accesos dentro de las oficinas restringidas, en el cual se busca aumentar de manera significativa la cantidad de registros de los accesos que se pueden generar diariamente en las oficinas, mientras que por último como tercer objetivo se planteó incrementar el nivel de seguridad en las oficinas restringidas de la institución, el cual se medirá a través de la satisfacción de los trabajadores con respecto a seguridad en las oficinas.

II. MÉTODO

2.1. Diseño de la investigación

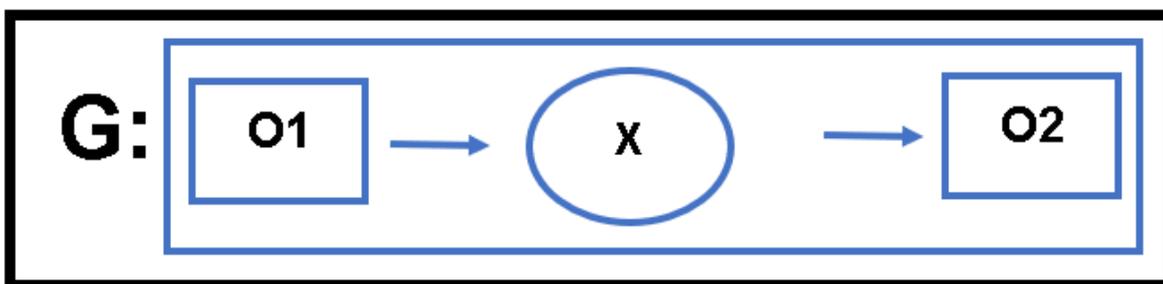
2.1.1. Tipo de investigación

Cuantitativa; Experimental, Pre-Experimental

2.1.2. Clasificación

Es Pre-Experimental ya que va a existir el manejo de nuestra variable dependiente y aleatoriedad de nuestra muestra.

Ilustración 2. Clasificación de la investigación



Fuente: 2.1 Diseño de Investigación
Elaboración: propia

Dónde:

-G: Grupo Experimental

-O1: Seguridad de acceso a las oficinas de la Gerencia Regional de Transporte y Comunicaciones **antes** del sistema basado en RFID.

-X: Sistema basado en RFID para mejorar la seguridad de acceso.

-O2: Seguridad de acceso a las oficinas de la Gerencia Regional de Transporte y Comunicaciones **después** del sistema basado en RFID.

2.1.3. Identificación de Variables

-Variable Dependiente:

Sistema basado en RFID.

-Variable Independiente:

Mejorar la seguridad de acceso.

2.1.4. Operacionalización de variables:

Tabla 3. Operacionalización de Variables

Variable	Concepto	Operación	Indicador	Escala de medición
Mejorar la seguridad de acceso. (VD)	Según (Universidad Nacional de Educación a Distancia (UNED), 2015) define la seguridad, una necesidad humana y una función de protección por otro lado es tener conocimiento y certeza sobre algo que se tiene que proteger.	Está relacionada con la protección de aquellos elementos existentes como los equipos e infraestructura, tener el acceso a las instalaciones, comprometiendo a la integridad física de los equipos causando daños en la prestación del servicio de la información almacenada. Se deben reducir los riesgos de pérdidas.	Cantidad de accesos no autorizados a las oficinas restringidas.	De razón
			Cantidad de registros de accesos dentro de las oficinas restringidas.	
			Nivel de satisfacción respecto a la seguridad en las oficinas restringidas.	
Sistema basado en RFID(VI).	Según (Gibbs, 2015)La define a la tecnología radiofrecuencia, como un método que nos permite tener más de un equipo en constante comunicación en donde se puede emitir señales de radio y el otro responde a la señal recibida.	Esta herramienta permitirá la identificación y mantener un control adecuado de los accesos que se dan en las oficinas, dando una mejor seguridad.	Pruebas Funcionales	De razón

Elaboración Propia

Tabla 4. Indicadores

N°	INDICADOR	DESCRIPCIÓN	OBJETIVO	TÉCNICA/ INSTRUMENTO	TIEMPO EMPLEADO	MODO DE CALCULAR
1	Cantidad de accesos no autorizados a las oficinas restringidas.	Determina el número de accesos no autorizados que se dan en las oficinas.	Disminuir la cantidad de accesos no autorizados a las oficinas restringidas.	Encuesta / Cuestionario	Semanal	$\text{CANAOR} = \frac{\sum_{i=1}^n (\text{PSANA})_i}{n}$ <p>CANAOR = Cantidad de accesos no autorizados a las oficinas restringidas. PSANA=Promedio Semanal de Accesos no autorizados. n = número de accesos diarios</p>
2	Cantidad de registros de accesos dentro de las oficinas restringidas.	Determina el número de registros de los accesos dentro de las oficinas.	Aumentar la cantidad de registros de accesos dentro de las oficinas restringidas.	Encuesta / Cuestionario	Semanal	$\text{CRADOR} = \frac{\sum_{i=1}^n (\text{PSRA})_i}{n}$ <p>CRADOR = Cantidad de registros de accesos dentro de las oficinas restringidas. PSRA= Promedio Semanal de Registro de Accesos n = número de registros diarios</p>
3	Nivel de Satisfacción respecto a la seguridad en las oficinas restringidas	Determina el nivel de Satisfacción con respecto a la seguridad.	Incrementar nivel de satisfacción respecto a la seguridad en las oficinas restringidas.	Encuesta / Cuestionario	Mensual	$\text{NSRSOR} = \frac{\sum_{i=1}^n (\text{NP})_i}{n}$ <p>NSRSOR = Nivel de Satisfacción respecto a la seguridad en las oficinas restringidas NP = número de preguntas n= número de trabajadores</p>

Elaboración: Propia

2.2. Población y muestra

- Indicador 1- cantidad de accesos no autorizados a las oficinas restringidas

Indicador	Población	Muestra
cantidad de accesos no autorizados a las oficinas restringidas.	15	15

Para nuestro indicador número 1 se consideró una cantidad de 15 accesos no autorizados que se dan en las oficinas durante un mes, el cual representa nuestra población y muestra que fue determinada por muestreo no probabilístico por conveniencia.

- Indicador 2- Cantidad de registros de accesos dentro de las oficinas restringidas

Indicador	Población	Muestra
Cantidad de registros de accesos dentro de las oficinas restringidas.	20	20

Para nuestro indicador número 2 se consideró una cantidad de 20 registros de accesos que se pueden dar a diario en una semana, el cual representa nuestra población y muestra que fue determinada por muestreo no probabilístico por conveniencia.

- Indicador 3- Satisfacción respecto a la seguridad en las oficinas restringidas

Indicador	Población	Muestra
Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas.	5	5

Debido a que la población es menor a 30, tanto la muestra como la población es igual a 5 personas.

2.3. Técnica e Instrumento de recolección de Datos, validación y confiabilidad

2.3.1. Técnica e Instrumento de recolección de Datos

Tabla 5. Técnica e Instrumento

Técnica	Instrumento	Fuente	Informantes
Encuesta	Cuestionario	Gerencia Regional de Transporte y Comunicaciones	Trabajadores
Encuesta	Cuestionario	Gerencia Regional de Transporte y Comunicaciones	Trabajadores
Encuesta	Cuestionario	Gerencia Regional de Transporte y Comunicaciones	Trabajadores

Elaboración: Propia

2.3.2. Validez del Instrumento

Para realizar la validación del instrumento de recolección de datos primeramente será sometido a una evaluación por un experto, donde al finalizar la evaluación redacta sus observación y recomendaciones que son consideradas para el respectivo cuestionario.

2.3.3. Confiabilidad

Ilustración 3. Vista de Datos

Visible: 8 de 8 variables

	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
1	2	3	4	2	2	1	4	5
2	1	4	4	2	2	2	4	5
3	2	4	4	2	2	2	5	5
4	2	2	4	1	2	2	4	4
5	2	4	5	2	2	2	4	5
6	2	4	4	2	2	2	4	5
7	1	1	4	2	1	1	5	5
8	2	4	3	2	2	2	4	5
9	1	5	3	2	2	2	5	4
10	3	4	4	2	2	2	5	5
11	2	4	4	2	2	2	5	4
12	3	3	4	2	2	2	4	5
13	1	4	3	1	2	1	4	5
14	2	2	4	2	1	2	5	5
15	2	4	4	2	2	2	5	4
16								
17								

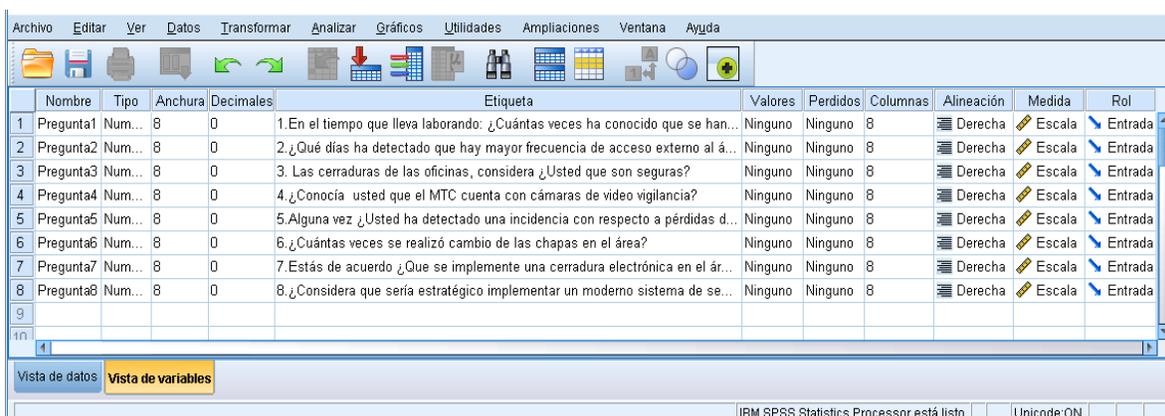
Vista de datos Vista de variables

IBM SPSS Statistics Processor está listo Unicode:ON

Fuente: IBM SPSS STATISTICS VERSION 24

En la siguiente Ilustración 6 detalla el resultado tabulado de la encuesta dirigida a los trabajadores de la Gerencia Regional de Transporte y Comunicaciones, donde se empleó la escala Likert utilizando IBM SPSS STATISTICS VERSION 24, con la finalidad de definir el valor de los datos obtenidos de la encuesta.

Ilustración 4. Vista de Variables



Fuente: IBM SPSS STATISTICS VERSION 24

En la siguiente Ilustración 7, detalla la confiabilidad nuestro instrumento dándonos como principal observación a las variables, de acuerdo con las preguntas de la encuesta.

Ilustración 5.Fiabilidad de la Encuesta

Resumen de procesamiento de casos

		N	%
Casos	Válido	8	100,0
	Excluido ^a	0	,0
	Total	8	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,851	,864	8

Fuente: IBM SPSS STATISTICS VERSION 24

2.4. Procedimiento

La prueba Alpha de Cronbach va a ser empleada en la medición de la fiabilidad de los instrumentos que permitirá obtener la recolección de la información para la presente investigación.

Cálculo:

$$\alpha = \frac{x}{x - 1} \left[1 - \frac{\sum S_{iS}^2}{S_T^2} \right]$$

x = Número de ítems

$\sum S_{iS}^2$ = Sumatoria de variables de los ítems

S_T^2 = Varianza de cada suma por ítem

α = Alpha Cronbach

Tabla 6. Tabla de valoración para el Alpha de Cronbach

Valor Alpha Cronbach	Apreciación
[0.95 - >]	Muy Elevado o Excelente
[0.90 - 0.95]	Elevado
[0.85 - 0.90]	Muy bueno
[0.80 - 0.85]	Buena
[0.75 - 0.80]	Muy respetable
[0.70 - 0.75]	Respetable
[0.65 - 0.70]	Mínimamente aceptable
[0.40 - 0.65]	Moderada
[0.00 - 0.40]	Inaceptable

Elaboración: Propia

El valor mínimo aceptable para que el instrumento sea confiable es de 0.75

2.5. Método de Análisis de Datos

El método que se empleara en la presente investigación es Pre-Test – Post Test, por lo tanto, para probar la hipótesis se utilizará la prueba T – Student, puesto que la muestra es inferior a 30.

Proceso:

1. Definir variables

Ia = Pre-Test (Indicador)

Ip = Post-Test (Indicador)

2. Hipótesis estadística

Hipótesis Nula:

$$H_0 = I_a - I_p \leq 0$$

Expone que el indicador del Pre-Test es óptimo que el de Post-Test.

Hipótesis alternativa:

$$H_1 = I_a - I_p > 0$$

Expone que el indicador del Post-Test es óptimo que el de Pre-Test.

3. Nivel de significancia

$$\alpha = 5\% \text{ (error)}$$

$$\text{Nivel de confiabilidad } ((1-\alpha)=0.95)$$

4. Estadística de prueba:

$$t = \frac{D\sqrt{n}}{SD}$$

Donde:

D = Diferencia de promedio

n = Muestra

SD = Desviación estándar

5. Región de rechazo

La región de rechazo es $t = t_x$

Dónde t_x es tal que:

$$P [T > T_x] > 0.05$$

Dónde $t_x =$ Valor Tabulador

Luego Región de rechazo: $t > t_x$

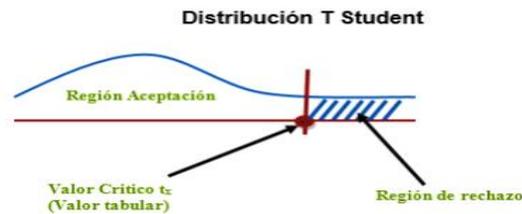
a. Diferencia de promedios

$$D = \frac{\sum_{i=1}^n D_i}{n}$$

b. Desviación estándar

$$SP = \sqrt{\frac{n \sum_{i=1}^n D_i^2 - (\sum_{i=1}^n D_i)^2}{n(n-1)}}$$

c. Conclusión



2.6. Aspecto Ético:

La información presentada en este proyecto de investigación es real, teniendo en cuenta la veracidad de los autores.

III. RESULTADOS

3.1. Contratación de Hipótesis:

Indicador 1: cantidad de accesos no autorizados a las oficinas restringidas

a. Definición de variables

- **CANAOR_{sa}** = cantidad de accesos no autorizados a las oficinas restringidas sin el sistema RFID.
- **CANAOR_{sp}** = cantidad de accesos no autorizados a las oficinas restringidas con el sistema RFID.

b. Hipótesis estadística

Hipótesis H₀ = cantidad de accesos no autorizados a las oficinas restringidas es mayor o igual sin el sistema basado en RFID que la cantidad de accesos no autorizados a las oficinas restringidas con el sistema basado en RFID.

$$H_0 = CANAOR_{sa} - CANAOR_{sp} \geq 0$$

Hipótesis H_a = cantidad de accesos no autorizados a las oficinas restringidas es menor sin el sistema basado en RFID que la cantidad de accesos no autorizados a las oficinas restringidas con el sistema basado en RFID

$$H_a = CANAOR_{sa} - CANAOR_{sp} < 0$$

c. Nivel de significancia

El nivel de significancia (α) empleado en la investigación para ejecutar la prueba de hipótesis es de 0.5 (5%). Por lo tanto, el nivel de confianza ($1 - \alpha = 0.95$), correspondiente a 95%.

d. Contratación

Tabla 7. Contratación Hipótesis - Indicador 01

N°	Pre	Post	Diferencia	D2
	CANAORsa	CANAORsp		
1	3	0	3	9
2	2	0	2	4
3	4	0	4	16
4	3	0	3	9
5	5	0	5	25
6	3	0	3	9
7	5	0	5	25
8	4	0	4	16
9	4	0	4	16
10	3	0	3	9
11	5	0	5	25
12	3	0	3	9
13	4	0	4	16
14	2	0	2	4
15	5	0	5	25
Total	55	0	55	217
promedio	3.66	0	3.66	14.46

Elaboración: propia

Ilustración 6. Prueba de normalidad - Indicador 01

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CANAORsa	,205	15	,091	,882	15	,052
CANAORsp	.	15	.	.	15	.

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS STATISTICS VERSION 24

Dado que nuestra población es menor a 30 se aplica **Shapiro-Wilk** para la prueba de normalidad de nuestros datos del pre test y post test.

Tabla 8. Criterio para determinar la normalidad - Indicador 01

Normalidad		
P-Valor (PRE-TEST) = 0.052	≥	α = 0.05
P-Valor (POST-TEST) = 0.00	<	α = 0.05
P-Valor ≥ α Acepta H ₀ = El origen de los datos es de una distribución normal		
P-Valor < α Acepta H _a = El origen de los datos NO es de una distribución normal		
Se Acepta la H_a		

e. Cálculo de Promedios

$$CANAORsa = \frac{\sum_{i=1}^n (PSANA)_i}{n} = \frac{55}{15} = 3.66$$

$$\text{CANAORsp} = \frac{\sum_{i=1}^n (\text{PSANA})_i}{n} = \frac{00}{15} = 00$$

$$\bar{D}_i = \frac{\sum_{i=1}^n D_i}{n} = \frac{55}{15} = 3.66$$

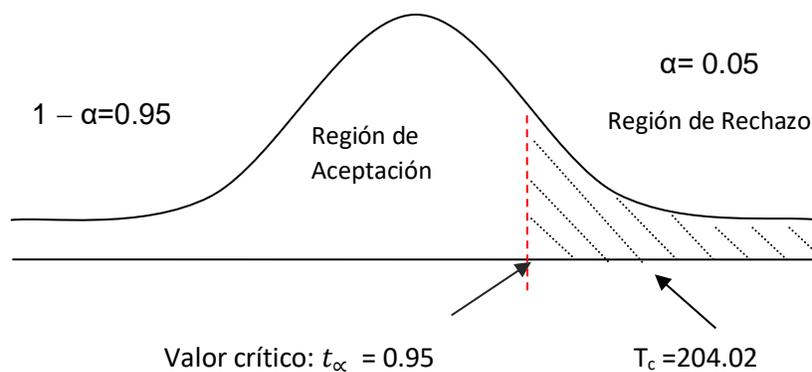
f. Cálculo de la varianza

$$S_D^2 = \frac{n \sum_{i=1}^n D_i^2 - (\sum_{i=1}^n D_i)^2}{n(n-1)}$$

$$S_D^2 = \frac{15(217) - (55)^2}{15(15-1)} = 1.09$$

g. Cálculo de prueba t

$$t_c = \frac{\bar{D}\sqrt{n}}{\sqrt{S_D}} = \frac{(55)(\sqrt{15})}{\sqrt{1.09}} = 204.02$$



Después de calcular $T_c = 204.02$ se verifica que es mayor a $T_\alpha = 0.95$, en lo cual observamos que el valor de T_c se encuentra dentro de la región de rechazo. Por lo tanto, se rechaza H_0 y se acepta H_a .

CANAORsa		CANAORsp		Decremento	
cantidad (núm.)	%	Cantidad (núm.)	%	Cantidad (núm.)	%
55	100	00.00	00	55	100

En el siguiente cuadro nos muestra detalles de cómo se logró disminuir significativamente la cantidad de accesos no autorizados en las oficinas restringidas, donde **CANAORsa** representa la cantidad de accesos no autorizados que se obtuvo antes de nuestro sistema basado en RFID mientras que **CANAORsp** es la cantidad que se obtuvo después de nuestro sistema basado en RFID, por lo tanto se concluye que se logró disminuir la cantidad de accesos no autorizados que afectando a un 100% en los accesos no autorizados en las oficinas de la Gerencia Regional de Transportes y Comunicaciones .

Indicador 2: Cantidad de registros de accesos dentro de las oficinas restringidas.

a. Definición de variables

- **CRADOR_{sa}** = Cantidad de registros de accesos dentro de las oficinas restringidas sin el sistema basado en RFID.
- **CRADOR_{sp}** = Cantidad de registros de accesos dentro de las oficinas restringidas con el sistema basado en RFID.

b. Hipótesis estadística

Hipótesis Ho = Cantidad de registros de accesos dentro de las oficinas restringidas es menor o igual sin el sistema basado en RFID que la cantidad de registros de accesos dentro de las oficinas restringidas con el sistema basado en RFID.

$$H_o = CRADOR_{sa} - CRADOR_{sp} \leq 0$$

Hipótesis H_a = Cantidad de registros de accesos dentro de las oficinas restringidas es mayor sin el sistema basado en RFID que la cantidad de registros de accesos dentro de las oficinas restringidas con el sistema basado en RFID.

$$H_a = CRADOR_{sa} - CRADOR_{sp} > 0$$

c. Nivel de significancia

El nivel de significancia (α) empleado en la investigación para ejecutar la prueba de hipótesis es de 0.5 (5%). Por lo tanto, el nivel de confianza ($1 - \alpha = 0.95$), correspondiente a 95%.

d. Contrastación

Tabla 9. Contrastación Hipótesis - Indicador 02

N°	Pre	Post	Diferencia	D2
	<i>CRADOR</i> sa	<i>CRADOR</i> sp		
1	0	4	4	16
2	0	6	6	36
3	0	5	5	25
4	0	4	4	16
5	0	5	5	25
6	0	8	8	64
7	0	7	7	49
8	0	8	8	64
9	0	6	6	36
10	0	8	8	64
11	0	5	5	25
12	0	9	9	81
13	0	7	7	49

14	0	5	5	25
15	0	9	9	81
16	0	8	8	64
17	0	7	7	49
18	0	9	9	81
19	0	6	6	36
20	0	8	8	64
Total	0	134	134	950
Promedio	0	6.7	6.7	47.5

Elaboración Propia

Ilustración 7. Prueba de normalidad-Indicador 02

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
CRADORsa	.	20	.	.	20	.
CRADORsp	,184	20	,076	,917	20	,086

a. Corrección de significación de Lilliefors

Fuente: IBM SPSS STATISTICS VERSION 24

Dado que nuestra población es menor a 30 se aplica **Shapiro-Wilk** para la prueba de normalidad de nuestros datos del pre test y post test.

Tabla 10. Criterio para determinar la normalidad - Indicador 02

Normalidad		
P-Valor (PRE-TEST) = 0.000	≤	α = 0.05
P-Valor (POST-TEST) = 0.086	>	α = 0.05
P-Valor ≤ α Acepta H ₀ = El origen de los datos es de una distribución normal		
P-Valor > α Acepta H _a = El origen de los datos NO es de una distribución normal		
Se Acepta la H _a		

Elaboración: Propia

e. **Cálculo de Promedios**

$$\text{CRADORsa} = \frac{\sum_{i=1}^n (\text{PSRA})_i}{n} = \frac{00}{20} = 0.00$$

$$\text{CRADORsp} = \frac{\sum_{i=1}^n (\text{PSRA})_i}{n} = \frac{134}{20} = 6.7$$

$$\bar{D}_i = \frac{\sum_{i=1}^n D_i}{n} = \frac{134}{20} = 6.7$$

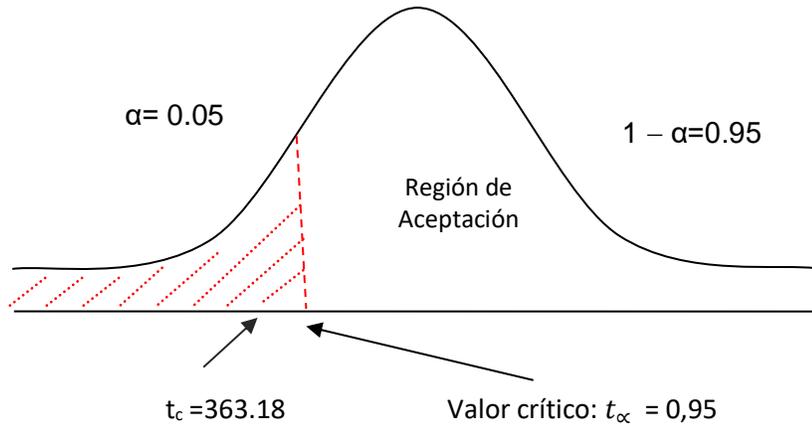
f. **Cálculo de la varianza**

$$S_D^2 = \frac{n \sum_{i=1}^n D_i^2 - (\sum_{i=1}^n D_i)^2}{n(n-1)}$$

$$S_D^2 = \frac{20(950) - (134)^2}{20(20-1)} = 2.74$$

g. Cálculo de prueba t

$$t_c = \frac{\bar{D}\sqrt{n}}{\sqrt{S_D}} = \frac{(134)(\sqrt{20})}{\sqrt{2.74}} = 363.18$$



Después de calcular $T_c = 363.18$ se verifica que es mayor a $T_\alpha = 0.95$, en lo cual observamos que el valor de T_c se encuentra dentro de la región de rechazo. Por lo tanto, se rechaza H_0 y se acepta H_a .

CRADORsa		CRADORsp		Decremento	
cantidad (núm.)	%	Cantidad (núm.)	%	Cantidad (núm.)	%
00.00	00	134	100	134	100

En el siguiente cuadro nos muestra detalles de cómo se logró aumentar significativamente la cantidad de registros de los accesos que se dan dentro de cada oficina, donde CRADORsa representa la cantidad de registros de accesos dentro de las oficinas restringidas antes de nuestro sistema basado en RFID, mientras que CRADORsp viene a ser la cantidad de registros de accesos dentro de las oficinas restringidas que se obtuvo significativamente después de nuestro sistema basado en RFID, por lo tanto se concluye que se logró aumentar

la cantidad de registros de accesos dentro de las oficinas restringidas que afectando a un 100% en los registros de accesos en las oficinas de la Gerencia Regional de Transportes y Comunicaciones, mejorando el control de los accesos permitidos en las oficinas restringidas.

Indicador 3: Nivel de satisfacción respecto a la seguridad en las oficinas restringidas.

Rango	Nivel de Satisfacción	Peso
MB	Muy Bueno	5
B	Bueno	4
R	Regular	3
M	Malo	2
MM	Muy Malo	1

Para determinar el nivel de satisfacción con respecto a la seguridad, se hará uso de la escala de Likert para medir el grado de positividad, neutralidad y negatividad del personal encargado de las áreas restringidas.

Fórmula para calcular el puntaje total:

$$\overline{PP}_i = \frac{PT_i}{n}$$

Dónde:

\overline{PP}_i = Promedio del puntaje total de la pregunta i -esima.

n = 5 (número preguntas)

Para determinar el cálculo del puntaje total y puntaje promedio se desarrollará de la siguiente manera; se multiplica la cantidad de personas encargadas dentro de las áreas restringidas de la Gerencia Regional de Transporte y Comunicaciones por el peso según su rango y luego se realiza la sumatoria de toda la fila para hallar el puntaje total. Al final, se divide por la

cantidad de personas encargadas dentro de las áreas restringidas para así determinar el puntaje promedio.

Tabla 11. Tabulación de encuesta de satisfacción – Pre Test

N°	Pregunta	MB	B	R	M	MM	Puntaje Total	Puntaje Promedio
		5	4	3	2	1		
1	¿Cómo calificaría usted la seguridad en las áreas restringidas?	0	0	1	2	2	9	1.8
2	¿Cómo calificaría el método que emplea la Gerencia Regional de Transporte y Comunicaciones para dar seguridad en las áreas restringidas?	0	0	2	1	2	10	2
3	¿Cómo calificaría usted la disponibilidad de la información respecto al registro de control de accesos a las áreas de la Gerencia Regional de Transporte y Comunicaciones?	0	0	1	1	3	8	1.6
4	¿Cómo califica la manera en cómo se realiza control de accesos actualmente?	0	0	0	1	4	6	1.2
5	¿Cómo califica la seguridad de las evidencias (fotografías, videovigilancia) en las áreas de la Gerencia Regional de Transporte y Comunicaciones?	0	0	2	2	1	11	2.2
							Total	8.2

Elaboración: Propia

Tabla 12. Tabulación de encuesta de satisfacción – Post Test

N°	Pregunta	M	B	R	M	MM	Puntaje Total	Puntaje Promedio
		B						
		5	4	3	2	1		
1	¿Cómo calificaría usted la seguridad en las áreas restringidas?	2	2	1	0	0	21	4.2
2	¿Cómo calificaría el método que emplea la Gerencia Regional de Transporte y Comunicaciones para dar seguridad en las áreas restringidas??	2	3	0	0	0	14	2.8
3	¿Cómo calificaría usted la disponibilidad de la información respecto al registro de control de accesos a las áreas de la Gerencia Regional de Transporte y Comunicaciones?	2	1	2	0	0	20	4
4	¿Cómo califica la manera en cómo se realiza control de accesos actualmente?	2	3	0	0	0	18	4.4
5	¿Cómo califica la seguridad de las evidencias (fotografías, video vigilancia) en las áreas de la Gerencia Regional de Transporte y Comunicaciones?	1	2	2	0	0	19	3.8
							Total	19.2

Elaboración: Propia

Tabla 13. Contrastación del PRE y POST test

Pregunta	NSRSORsa	NSRSORsp	D	D ²
1	1.8	4.2	-2.4	5.76
2	2	2.8	-0.8	0.64
3	1.6	4	-2.4	5.76
4	1.2	4.4	-3.2	10.24
5	2.2	3.8	-1.6	2.56
Total	8.8	19.2	-10.4	24.96
Promedio	1.76	3.84	-5.2	4.99

Elaboración: Propia

Calculamos los niveles de satisfacción del personal encargado de las áreas restringidas de la Gerencia Regional de Transporte y Comunicaciones tanto para antes de la implementación del sistema basado en RFID para Mejorar la Seguridad de Acceso como para después de la implementación del sistema basado en RFID para Mejorar la Seguridad de Acceso.

$$NSRSORsa = \frac{\sum_{i=1}^n (NP)_i}{n} = \frac{8.8}{5} = 1.76$$

$$NSRSORsp = \frac{\sum_{i=1}^n (NP)_i}{n} = \frac{19.2}{5} = 3.84$$

a. Definición de variables

NSRSORsa = Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas.

NSRSORsp = Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas.

b. Hipótesis estadística:

Hipótesis H₀ = El Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas es menor o igual sin el sistema basado en RFID que el Nivel de

satisfacción con respecto a la seguridad en las oficinas restringidas con el sistema basado RFID.

$$H_0 = NSRSOR_{sa} - NSRSOR_{sp} \leq 0$$

Hipótesis H_a = El Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas es mayor sin el sistema basado en RFID que el Nivel de satisfacción con respecto a la seguridad en las oficinas restringidas con el sistema basado en RFID.

$$H_a = NSRSOR_{sa} - NSRSOR_{sp} > 0$$

c. Nivel de significancia

El nivel de significancia (α) empleado en la investigación para ejecutar la prueba de hipótesis es de 0.5 (5%). Por lo tanto, el nivel de confianza ($1 - \alpha = 0.95$), correspondiente a 95%.

d. Contrastación

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE_NSRSOR	,274	5	,200 [*]	,979	5	,254
POST_NSRSOR	,274	5	,200 [*]	,867	5	,254

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

Dado que nuestra población es menor a 30 se aplica **Shapiro-Wilk** para la prueba de normalidad de nuestros datos del pre test y post test.

Tabla 14. Criterio para determinar la normalidad - Indicador 03

Normalidad		
P - Valor (PRE - TEST) = 0.254	≥	α = 0.05
P - Valor (POST - TEST) = 0.254	>	α = 0.05
P - Valor α ≤ Acepta H ₀ = El origen de los datos es de una distribución normal		
P - Valor > α Acepta H ₁ = El origen de los datos NO es de una distribución normal		
Se Acepta la Ha		

Elaboración: Propia

Ilustración 8. Resultados prueba t-Student – Indicador 03

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	PRE_NRSOR	1,7600	5	,38471	,17205
	POST_NRSOR	3,8400	5	,62290	,27857

Correlaciones de muestras emparejadas				
		N	Correlación	Sig.
Par 1	PRE_NRSOR & POST_NRSOR	5	-,618	,267

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	PRE_NRSOR - POST_NRSOR	-2,08000	,91214	,40792	-3,21257	-,94743	-5,099	4	,007

Fuente: IBM SPSS STATISTICS VERSION 24

e. Cálculo de Promedios

$$NSRSOR_{sa} = \frac{\sum_{i=1}^n NP_i}{n} = \frac{8.8}{5} = 2.56$$

$$NSRSOR_{sp} = \frac{\sum_{i=1}^n NP_i}{n} = \frac{22.8}{5} = 4.56$$

$$\bar{D} = \frac{\sum_{i=1}^n D_i}{n} = -\frac{-10.4}{5} = -2.08$$

f. Cálculo de la varianza

$$S_D^2 = \frac{n \sum_{i=1}^n D_i^2 - (\sum_{i=1}^n D_i)^2}{n(n-1)}$$

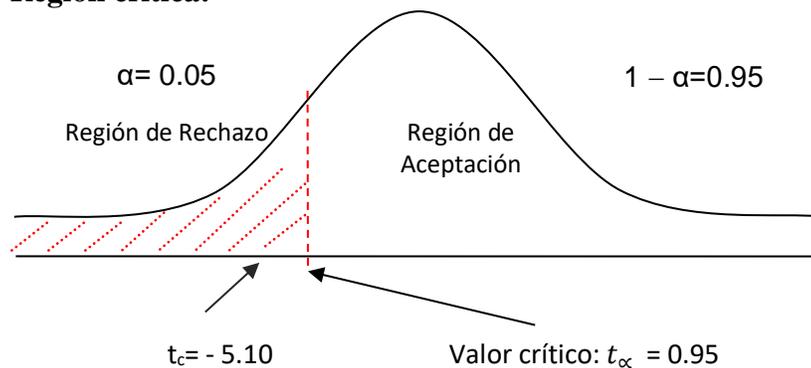
$$S_D^2 = \frac{5(24.96) - (-10.4)^2}{5(5-1)} = 0.83$$

g. Cálculo de prueba t

$$t = \frac{\bar{D}\sqrt{n}}{\sqrt{S_D}} = \frac{(-2.08)(\sqrt{5})}{\sqrt{0.83}}$$

$$t = -5.10$$

h. Región crítica:



Después de realizar los cálculos $T_c = -5.10$ se verifica que es menor que $T_\alpha = 0.95$, es decir observamos que el valor se encuentra dentro de la región de rechazo. Por lo tanto, $NSRSOR_{sa} - NSRSOR_{sp} < 0$, llegándose a la conclusión de que se rechaza H_0 y se acepta H_a .

IV. DISCUSIÓN

Según nuestra investigación podemos decir que el uso de las tecnologías puede ser una herramienta fundamental hoy en día en una organización, permitiéndoles tener mejor desarrollo en tecnologías que aporten tanto en la crecimiento mismo como en la seguridad , tal cual es el factor principal que logramos mejorar con nuestro sistema basado en RFID en esta ocasión aplicada en las oficinas restringidas de la Gerencia Regional de Transporte y Comunicaciones, donde luego de realizar un estudio de la realidad problemática nos pudimos dar cuenta que la organización antes de la implementación del Sistema tenía una cantidad no aceptable en accesos no autorizados en las oficinas, es decir no se llevaba un control adecuado de los accesos no permitidas a las oficinas, por otra parte no se llevaba a cabo un registro de todos los accesos que se daban diariamente , por lo que esto también provocaba un nivel de satisfacción muy baja en los trabajadores con respecto a seguridad.

Mientras que por otra parte para esta investigación se realizó técnicas de recolección de datos a través de una guía de observables en la que se pudo determinar la realidad del problema, sobre todo la metodología de desarrollo donde para esta oportunidad se aplicara Iconix el cual se determinó en 5 fases Requerimientos, Arquitectura de Hardware, Proceso de Aplicación, Diseño , Pruebas Funcionales, donde de acuerdo a los trabajos previos empleados para esta investigación nos permitió tener una idea clara en tanto el desarrollo de nuestro sistema por lo cual de acuerdo al proyecto de (Vernard, 2017) pudimos definir los requerimientos y funcionalidad que nuestro sistema requería , mientras que por otra parte para definir la arquitectura y parte de los proceso para nuestro sistema se empleó de la investigación realizado por (Rafael de la Rosa Flores, 2017) ,ya que la finalidad del desarrollo de su tesis fue llevar un control adecuado de quien y en que horario se usó cada laboratorio, en tanto para definir los procesos en nuestro sistema se determinó de acuerdo a lo empleado por (Vergara, 2013), el cual para el desarrollo de su sistema utilizo un módulo Rfid permitiéndolo tener un control y supervisión del personal en un laboratorio , por último en nuestra investigación se consideró lo empleado por (Pardo, 2015) en el que utilizo un módulo GSM para reportar en mensajes que indiquen en que horarios se está haciendo uso de tal equipo en un laboratorio, función empleada en nuestro sistema el cual a través de mensajes

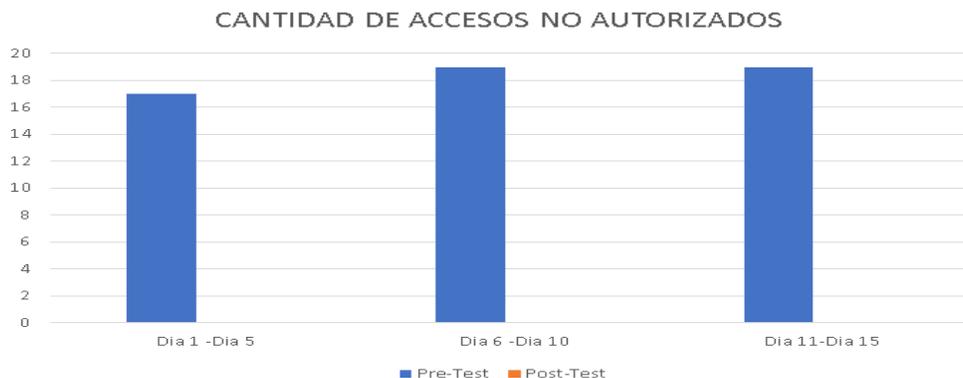
de texto enviara alertas de quien ingreso a la oficina o si hubo algún ingreso no autorizado dando así mejoras en seguridad y registros en las oficinas.

Por otra parte, con nuestro sistema se logró alcanzar de manera satisfactoriamente estas necesidades en tanto a seguridad dentro de las oficinas de la Gerencia Regional de Transporte y Comunicaciones en el que se ve reflejado dentro del Pre-test y Post-test dándonos los resultados esperados, el cual nos permitió ver cómo era la seguridad antes del desarrollo de nuestro sistema y como fue mejorando con nuestro sistema, y para determinar estos puntos se tuvo en cuenta los siguientes indicadores.

Indicador 1: cantidad de accesos no autorizados a las oficinas restringidas

Según resultados obtenidos de las encuesta a los trabajadores encargados de las oficinas de la Gerencia Regional de Transporte y comunicaciones se demostró que en las oficinas se generan una cantidad alta de accesos no autorizados y que en algunos casos no son comunicados al encargado de la oficina, porque no se tiene un control adecuado de los accesos que se dan durante el día en las oficinas restringidas, es por ello que antes de nuestro sistema basado en RFID se obtuvieron los siguientes resultado con respecto a la cantidad de accesos en el día 1 al día 5 se pudo reportar 17 accesos no autorizados en total, en el día 6 al día 10 se reportó 19 accesos no autorizados, mientras que para el día 11 al día 15 se reportó la misma cantidad, a diferencia cuando se implementó el sistema basado en RFID donde podemos decir que ya no se reportaron ningún acceso no autorizado, por lo que se disminuyó significativamente , mejorando así la seguridad en accesos.

Ilustración 9. Indicador 1: cantidad de accesos no autorizados a las oficinas restringidas

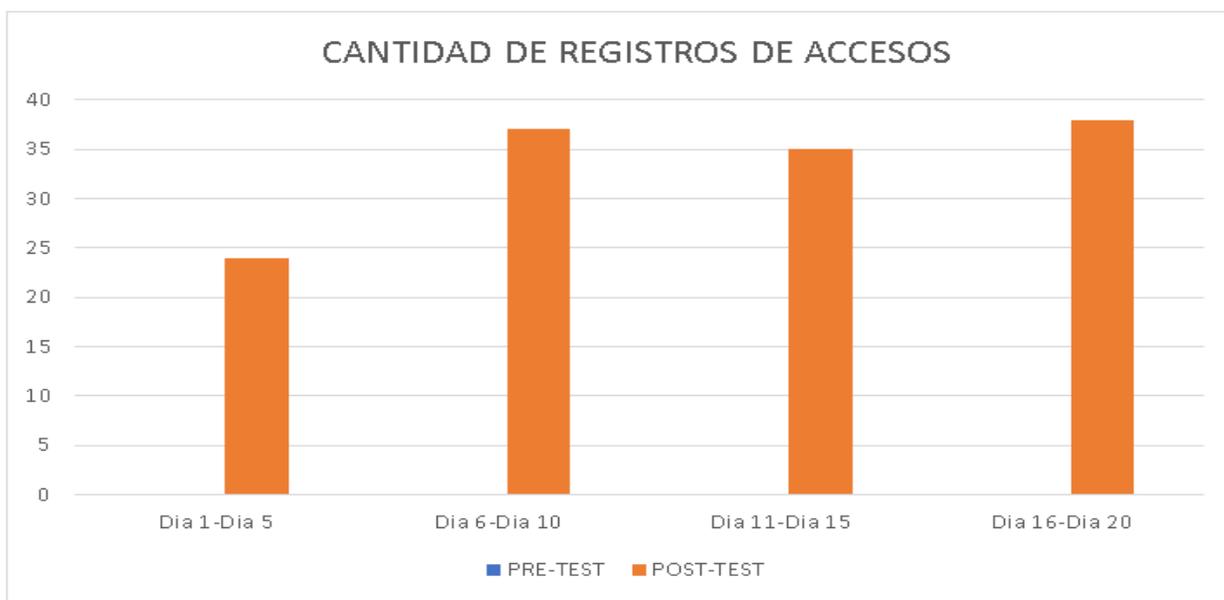


Elaboración: Propia

Indicador 2: Cantidad de registros de accesos dentro de las oficinas restringidas:

Según resultados obtenidos de las encuestas a los trabajadores encargados de las oficinas restringidas de la Gerencia Regional de Transporte y comunicaciones se demostró que en las oficinas no se llevaba un registro adecuado de todos los accesos que se pueden dar, es decir la organización no cuenta con algún sistema adecuado que ayude a registrar que accesos se dieron durante el día, por lo que gracias a nuestro sistema basado en RFID se logró significativamente mejorar en cuanto a los registros de accesos que se dan dentro de las oficinas, obteniendo en el día 1 al día 5 una cantidad total de 24 registros de accesos, en el día 6 al día 10 una cantidad de 37 registros de accesos, en el día 11 al día 15 un cantidad de 35 y para el día 16 al día 20 se obtuvo 38 registros de accesos permitidos, por lo que se puede decir que se aumentó la cantidad de registros de accesos permitidos en las oficinas restringidas de la Organización, aportando sobre todo en la seguridad de accesos.

Ilustración 10. Indicador 2: Cantidad de registros de accesos dentro de las oficinas restringidas:



Elaboración: Propia

Indicador 3: Nivel de satisfacción respecto a la seguridad en las oficinas restringidas.

Según el puntaje obtenidos del cuestionario aplicado a los trabajadores encargados de las oficinas restringidas de la Gerencia Regional de Transporte y comunicaciones se demostró que el nivel de satisfacción respecto a la seguridad sin el sistema es un nivel bajo con un total de 8.8 puntos dándonos un porcentaje de 27% a comparación del nivel mostrado con el Sistema donde nos dio un total de 19.2 puntos subiendo significativamente a un 73%, donde nos muestra que gracias al Sistema basado en RFID se aumentó el nivel de satisfacción con respecto a seguridad en las oficinas restringidas de la Gerencia Regional de Transporte y Comunicaciones.

Ilustración 11. Indicador 3: Nivel de satisfacción respecto a la seguridad en las oficinas restringidas.



Elaboración: Propia

V. CONCLUSIONES

Según nuestros indicadores se determinó la importancia que tiene la seguridad de acceso en las áreas restringidas de la Gerencia Regional de Transporte y Comunicaciones llegando así a concluir lo siguiente:

1. Según nuestras mediciones con respecto a la cantidad de acceso no autorizado en la Gerencia Regional de Transporte y Comunicaciones se determinó que fue de un 100% de ingresos no autorizados al área, y que después de la implementación del sistema basado en RFID se llegó a reducir a un 0% de los ingresos no autorizados basado en los valores con respecto al pretest, mejorando así significativamente el control en cuanto a los accesos no autorizados y sobre todo aportando en la seguridad de la organización.
2. Se llegó a determinar que después de la implementación del sistema basado en RFID se mejoró el registro de acceso por día en las áreas restringidas de la Gerencia Regional de Transporte y Comunicaciones, aportando de cierto modo al mejoramiento en cuanto al control de los accesos que se dan diariamente.
3. Basado en nuestros indicadores se determinó un bajo nivel de satisfacción respecto a la seguridad en las oficinas restringidas en la Gerencia Regional de Transporte y Comunicaciones en el cual después de la implementación de nuestro sistema basado en RFID llegamos a incrementar el nivel de satisfacción en los trabajadores del área con respecto a la seguridad en las oficinas restringidas, logrando así un nivel de seguridad aceptable para la organización.

VI. RECOMENDACIONES

- De acuerdo a nuestra investigación, se sugiere a futuras investigaciones investigar más a cerca de estas tecnologías que puede ser aplicada con el mismo fin de control o búsqueda a través de algún código, ya que esta tecnología puede ser fundamental en un futuro por lo complejo y sencillo que es al aplicar en ciertos sistemas.
- Se propone a la Gerencia Regional de Transporte y Comunicaciones puedan en un futuro optar implementar este sistema en las demás áreas de la organización el cual les aportara mayor seguridad y beneficios a todos, ya que con este sistema solo bastaría con bloquear el acceso a cierta tarjeta y agregar una nueva si en caso se perdiera, en lugar de optar por el cambio de una chapa, que hasta puede generar ciertos gastos para la organización misma.
- Según lo investigado planteamos a las futuras investigaciones innovar la aplicación de esta tecnología en futuros sistemas que opten este tipo de tecnología ya que más adelante puede ser aplicada a sistemas que trabajen mediante reconocimiento de código RFID, por ejemplo ya sea para algún sistema de transporte publico donde gracias a este tecnología se pueda dar acceso a algún transporte y automáticamente se genere un pago permitiendo así a los pasajeros de alguna u otra manera facilitarles la vida al transitar en unos de estos servicios públicos.
- Se sugiere a la Gerencia Regional de Transporte y Comunicaciones seleccionar un personal apto que conozca más acerca de esta tecnología, y pueda de alguna u otra forma innovar este tipo de sistema, por otra parte, también se recomendaría capacitar a los trabajadores encargados de las diferentes áreas sobre qué medidas se tendría que dar para el buen uso y cuidado del Sistemas RFID.

VII. REFERENCIAS

- Actum. 2018.** Actum. *Actum*. [En línea] 18 de noviembre de 2018. <https://www.actum.es/preguntas-frecuentes/tipos-de-tags>.
- 2018.** Arduino.cl. *Arduino.cl*. [En línea] 14 de Octubre de 2018. <https://arduino.cl/arduino-uno/>.
- by.com. 2018.** ¿Que es RFID? *¿Que es RFID?* [En línea] 27 de Noviembre de 2018. <https://www.by.com.es/blog/que-es-rfid/>.
- Diario El Comercio. 2018.** Diario El Comercio. 20 de Junio de 2018.
- es.farnell.com. 2018.** Farnell Element14. [En línea] 8 de Diciembre de 2018. <https://es.farnell.com/multicomp/tip120/trans-darlington-npn-60v-5a-to/dp/9294210>.
- fermax. 2016.** fermax. *fermax*. [En línea] 4 de Octubre de 2016. [Citado el: 25 de Junio de 2019.] <https://blog.fermax.com/esp/sistemas-de-control-de-accesos-para-empresas-cu%C3%A1ndo-es-necesario>.
- Gibbs, Ariel J. Coba. 2015.** Implementación de un sistema de controlde entrada y salida empleando el módulo de lectura RFID con la tecnología Arduino. [En línea] 18 de Noviembre de 2015. [Citado el: 05 de Junio de 2019.] <https://revistas.utp.ac.pa/index.php/ric/article/view/1245/html>.
- INDECOPI. 2008.** EDI Tecnología de Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. [En línea] 2008. <https://www.gobiernodigital.gob.pe/docs/isoiec27001.pdf>.
- Inditar. 2017.** inditar.com. *inditar.com*. [En línea] 3 de JULIO de 2017. [Citado el: 10 de Mayo de 2019.] www.inditar.com.
- JMORALES. 2017.** Lector RFID basado en RC522. *Lector RFID basado en RC522*. [En línea] 22 de enero de 2017. <http://www.playbyte.es/electronica/arduino/lector-rfid-basado-en-rc522/>.
- Lara, Eduardo. 2015.** <https://hetpro-store.com/TUTORIALES/lcd-16x2-arduino-ew162b0ymy/>. <https://hetpro-store.com/TUTORIALES/lcd-16x2-arduino-ew162b0ymy/>. [En línea] 5 de marzo de 2015. <https://hetpro-store.com/TUTORIALES/lcd-16x2-arduino-ew162b0ymy/>.
- Misana Enginyeria, SL. 2017.** interempresas.net. *interempresas.net*. [En línea] 2017. [Citado el: 20 de junio de 2019.] <http://www.interempresas.net/Electronica/FeriaVirtual/Producto-Modulos-GSM-GPRS-Misana-GPRSA-139098.html>.
- Mutual de Seguridad. 2018.** La Seguridad como un valor cooperativo . *La Seguridad como un valor cooperativo*. [En línea] 23 de Noviembre de 2018. https://www.mutual.cl/portal/wcm/connect/ef57dd38-9711-42e9-80f9-b9cac17f9927/la_seguridad_como_un_valor_corporativo.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-ef57dd38-9711-42e9-80f9-b9cac17f9927-m5RTXvt.
- naylampmechatronics.com. 2018.** Válvula solenoide 1/2" 12V DC. [En línea] 8 de Diciembre de 2018. <https://naylampmechatronics.com/valvulas/314-valvula-solenoide-12-12v.html>.

Pardo, Elvis Andres Molino. 2015. *“Diseño de un sistema de seguridad aplicado al laboratorio de Telecomunicación usando Tecnología RFID y GSM.* Piura -Peru : s.n., 2015.

Proseguir Seguridad de confianza. 2017. Sistemas Electrónicos de Seguridad. [En línea] 2017. [Citado el: 17 de JUNIO de 2019.] <https://www.prosegur.com.pe/empresas-instituciones/servicios/servicios-de-prevencion/sistemas-electronicos-de-seguridad>.

Rafael de la Rosa Flores, David E. Muñoz Morales, Ervic, Perez Mendoza, Jose Luis, Mora Flores, Hilda Castillo Zacatelco. 2017. *Automatización para el control de acceso utilizando dispositivo móvil y Rfid.* Puebla-Mexico : s.n., 2017. Proyecto de Investigación.

Redondo A., Francisco Javier. 2017. *NUEVAS TECNOLOGIAS APLICABLES A EMPRESAS.* Santander : s.n., 2017. TRABAJO FIN DE GRADO.

Reviriego, Luis Vidal-Aragón. 2016. *Estudio de la tecnología de comunicación por.* Sevilla : s.n., 2016.

Sistemas de control de accesos para empresas: ¿cuándo es necesario? **Profesional, FerMax. 2016.** 4 de Octubre de 2016, FerMax Profesional.

tarjetashid-mifare-rfid.com. 2018. Proximidad.mx. *Proximidad.mx.* [En línea] 16 de Diciembre de 2018. http://www.tarjetashid-mifare-rfid.com/tarjeta_proximidad_rfid.html.

—. **2018.** tarjetashid-mifare-rfid.com. *tarjetashid-mifare-rfid.com.* [En línea] 29 de Noviembre de 2018. <http://www.tarjetashid-mifare-rfid.com>.

Tecnologías Informatica . 2018. Tecnologías Informatica. *Tecnologías Informatica.* [En línea] 16 de Diciembre de 2018. <https://tecnologia-informatica.com/tecnologia-rfid-tags/>.

todoelectronica.com. 2018. TodoElectronica . *TodoElectronica .* [En línea] 10 de Diciembre de 2018. <https://www.todoelectronica.com/es/electro-cerradura-normalmente-cerrado-nc-placa-de-montaje-larga-resistencia-de-carga-500-k-p-95906.html>.

Universidad Nacional de Educación a Distancia (UNED). 2015. Universidad Nacional de Educación a Distancia (UNED). *Universidad Nacional de Educación a Distancia (UNED).* [En línea] 2015. [Citado el: 06 de 06 de 2019.] http://portal.uned.es/portal/page?_pageid=93,47794967&_dad=portal&_schema=PORTAL&idAsignatura=32201039.

Universidad veracruzana. 2018. Seguridad de la Información. *Seguridad de la Información.* [En línea] 24 de Noviembre de 2018. <https://www.uv.mx/celulaode/seguridad-info/tema1.html>.

Vergara, zynnica Veronica Vargas. 2013. *“Sistema de control de acceso y monitoreo con la Tecnología RFID para el departamento de Sistema de la Universidad Politécnica Salesiana Sede Guayaquil.”.* Guayaquil-Ecuador : s.n., 2013.

Vernard, Rodolfo Steven Martinez. 2017. *Diseño del sistema de control de asistencia en la agencia mercado de la Caja Huancayo aplicando tarjeta de proximidad de tecnología RFID .* Huancayo-Peru : s.n., 2017.

viewnext.com. 2018. viewnext.com. *viewnext.com*. [En línea] 25 de Noviembre de 2018.
<https://www.viewnext.com/tipos-de-seguridad-informatica/>.

VIII. ANEXOS

Anexo 1: Instrumento de recolección de datos



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERIA
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS
ENCUESTA A LOS TRABAJADORES DE LAS OFICINAS RESTRINGIDAS
EN EL MTC

Buenos días,
Nuestros nombres son Juan Carlos de la Cruz Infantes y Rixi Alexandra Chunga Aguilar. Somos estudiantes X ciclo de la escuela de Ingeniería de Sistemas, presente encuesta tiene por finalidad identificar el nivel de seguridad con el que cuentan las oficinas restringidas en el MTC.
La información que usted brindara es muy importante y será utilizara en forma confidencial y anónima. Se muy honesto al brindar la información.

- ✓ Marque su respuesta anotando check o X.
- ✓ Selecciones solo una respuesta por cada ítem planteado

PERFIL DE ENCUESTADO

ÁREA:

ENCUESTA

1. En el tiempo que lleva laborando: ¿Cuántas veces ha conocido que se han extraviado las llaves de las puertas de las áreas laborales del MTC?

<input type="checkbox"/> 1 vez	<input type="checkbox"/> 2 veces	<input type="checkbox"/> 3 veces	<input type="checkbox"/> más de 3 veces
--------------------------------	----------------------------------	----------------------------------	---

2. ¿Qué días ha detectado que hay mayor frecuencia de acceso externo al área laboral u oficina?

<input type="checkbox"/> Lunes	<input type="checkbox"/> Martes	<input type="checkbox"/> Miércoles	<input type="checkbox"/> Jueves	<input type="checkbox"/> Viernes
--------------------------------	---------------------------------	------------------------------------	---------------------------------	----------------------------------

3. Las cerraduras de las oficinas, considera ¿Usted que son seguras?

<input type="checkbox"/> En total desacuerdo	<input type="checkbox"/> En desacuerdo	<input type="checkbox"/> Ni en desacuerdo, ni de acuerdo	<input type="checkbox"/> De acuerdo	<input type="checkbox"/> Totalmente de acuerdo
--	--	--	-------------------------------------	--

4. ¿Conocía usted que el MTC cuenta con cámaras de video vigilancia?

<input type="checkbox"/> SI	<input type="checkbox"/> NO
-----------------------------	-----------------------------

Si la respuesta de la pregunta anterior fue SÍ... ¿Dónde se almacena la información grabada por las cámaras de video vigilancia y quien es responsable de su gestión?

Si la respuesta fue NO pase a la siguiente Pregunta.



UNIVERSIDAD CÉSAR VALLEJO

5. Alguna vez ¿Usted ha detectado una incidencia con respecto a pérdidas de documentos en el área?

<input type="checkbox"/> SI	<input type="checkbox"/> NO
-----------------------------	-----------------------------

6. ¿Cuántas veces se realizó cambio de las chapas en el área?

<input type="checkbox"/> Ninguno	<input type="checkbox"/> 1 vez	<input type="checkbox"/> 2 veces	<input type="checkbox"/> 3 veces	<input type="checkbox"/> más de 3 veces
----------------------------------	--------------------------------	----------------------------------	----------------------------------	---

7. Estás de acuerdo ¿Que se implemente una cerradura electrónica en el área?

<input type="checkbox"/> Ninguno	<input type="checkbox"/> En total desacuerdo	<input type="checkbox"/> En desacuerdo	<input type="checkbox"/> Ni en desacuerdo, ni de acuerdo	<input type="checkbox"/> De acuerdo	<input type="checkbox"/> Totalmente de acuerdo
----------------------------------	--	--	--	-------------------------------------	--

8. ¿Considera que sería estratégico implementar un moderno sistema de seguridad en las oficinas restringidas del MTC?

<input type="checkbox"/> En total desacuerdo	<input type="checkbox"/> En desacuerdo	<input type="checkbox"/> Ni en desacuerdo, ni de acuerdo	<input type="checkbox"/> De acuerdo	<input type="checkbox"/> Totalmente de acuerdo
--	--	--	-------------------------------------	--

Muchas gracias por su colaboración y por el tiempo dedicado a contestar esta encuesta

Anexo 2: Planilla para la evaluación de instrumento de recolección de datos



PLANTILLAS PARA LA EVALUACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

1. IDENTIFICACION DEL EXPERTO

NOMBRE DEL EXPERTO: VICTOR IVAN PEREDA GONZALEZ
DNI 18161683 PROFESION: ESTADISTICO
LUGAR DE TRABAJO: UCV-TRUJILLO
CARGO QUE DESEMPEÑA: DOCENTE - TIEMPO PARCIAL
DIRECCION: AV. LARCO
TELEFONO FIJO: 252318 MOVIL: 952065117
DIRECCION ELECTRONICA: vperedag@dirsa.la.libertad.gob.pe
FECHA DE EVALUACIÓN: _____
FIRMA DEL EXPERTO: [Firma manuscrita]

2. PLANILLA DE VALIDACION DEL INSTRUMENTO

CRITERIOS	APRECIACION CUALITATIVA			
	EXCELENTE (4)	BUENO (3)	REGULAR (2)	DEFICIENTE (1)
Presentación del instrumento	X			
Claridad en la redacción de los ítems	X			
Pertinencia de las variables con los indicadores		X		
Relevancia del contenido	X			
Factibilidad de la aplicación		X		

APRECIACION CUALITATIVA: MUY BUENO

OBSERVACIONES: _____

3. JUICIO DE EXPERTOS:

- En líneas generales, considera Ud. que los indicadores de las variables están inmersos en su contexto teórico de forma:

SUFICIENTE <input checked="" type="checkbox"/>	MEDIANAMENTE SUFICIENTE	INSUFICIENTE
--	----------------------------	--------------

OBSERVACION:

Aplicable

- Considera que los reactivos del cuestionario miden los indicadores seleccionados para la variable de manera:

SUFICIENTE <input checked="" type="checkbox"/>	MEDIANAMENTE SUFICIENTE	INSUFICIENTE
--	----------------------------	--------------

OBSERVACION:

MUY BUENO

- El instrumento diseñado mide la variable de manera:

SUFICIENTE <input checked="" type="checkbox"/>	MEDIANAMENTE SUFICIENTE	INSUFICIENTE
--	----------------------------	--------------

OBSERVACION:

Excelente

- El instrumento diseñado es:

EXCELENTE

4. VALIDACION DEL INSTRUMENTO:

ITEMS	ESCALA				OBSERVACIONES
	DEJAR	MODIFICAR	ELIMINAR	INCLUIR	
01	X				
02	X				
03	X				
04	X				
05	X				
06	X				ordenar según lo sugerido
07	X				
08	X				
09					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

DESEARIA INCLUIR	COMO LO MODIFICARIA
—	—

Anexo 3: Encuesta de selección de metodología

ENCUESTA DE SELECCIÓN DE LA METODOLOGÍA

Nombre del Proyecto: "Sistema basado en RFID para Mejorar la Seguridad de Acceso a las Oficinas en la Subgerencia del MTC de La Libertad, 2018"

Nombre del Especialista:
Ricardo D. Mendoza Rianza

Profesión:
Ingr.

Lugar de Trabajo:
UCV

Cargo que desempeña:
Docente

Fecha:
13/11/2018

DNI:
18070765



Formato de Encuesta a Expertos para la Selección de Metodología

Objetivo: Reunir información esencial para la selección de la metodología a aplicar en el desarrollo de la tesis.

Dirigido a: Profesionales con experiencia en metodologías de desarrollo para la elaboración de la tesis.

1. Nombres y Apellidos: Jicardo D. Mendoza Rivera

2. Generalidades:

2.1. Profesión:

Ing. de Sistemas () Ing. Informático ()

Ing. de Software () Otros (x)

2.2. Años de Experiencia:

1 – 5 () 5 – 10 () 10 a más años (x)

2.3. Elección de la Metodología:

Para la elección de la Metodología se aplicarán los siguientes criterios:

- ✓ **Flexibilidad:** Se refiere a la adaptabilidad de la metodología frente a la multiplicidad de acontecimientos que tienen lugar en el proceso de desarrollo de software.
- ✓ **Información:** Se refiere a si existe información (bibliografía, antecedentes, etc.) de la metodología.
- ✓ **Compatibilidad:** Si es o no compatible para el desarrollo web.
- ✓ **Costo de desarrollo:** Se refiere a que tanto cuesta el desarrollo de software como consecuencia de usar la metodología.

- ✓ **Tiempo de desarrollo:** Si la metodología ayuda a extender un poco de tiempo de desarrollo del proyecto, sin perjudicarlo.
- ✓ **Herramienta a medida:** Se refiere a que si hay una herramienta de modelamiento exclusiva para esta metodología.
- ✓ **Participación del cliente:** Se refiere a la participación que tiene el cliente en el proceso de desarrollo de software.

Para la adición de la puntuación de seguirá la siguiente escala de Valorización:

VALORACIÓN	ESCALA
Pésimo	1
Malo	2
Regular	3
Bueno	4
Excelente	5

Calificación de la Metodología de acuerdo a Criterios y Escala de Valoración:

CRITERIO	RUP	XP	ICONIX	SCRUM
Flexibilidad	4	5	5	4
Información	4	4	5	4
Compatibilidad	4	5	5	5
Costo de Desarrollo	5	4	5	5
Tiempo de Desarrollo	3	4	5	4
Herramienta a medida	2	4	5	4
Simplicidad	3	5	5	4
Participación del cliente	4	4	5	4

ENCUESTA DE SELECCIÓN DE LA METODOLOGÍA

Nombre del Proyecto: "Sistema basado en RFID para Mejorar la Seguridad de Acceso a las Oficinas en la Subgerencia del MTC de La Libertad, 2018"

Nombre del Especialista:

Yosy Uyuro Oliva

Profesión:

Ingeniero de Sistemas

Lugar de Trabajo:

UCV

Cargo que desempeña:

DTP

Fecha:

13/11/18

DNI:

18206887

Oliva

Formato de Encuesta a Expertos para la Selección de Metodología

Objetivo: Reunir información esencial para la selección de la metodología a aplicar en el desarrollo de la tesis.

Dirigido a: Profesionales con experiencia en metodologías de desarrollo para la elaboración de la tesis.

1. Nombres y Apellidos: Yany Yany Ochoa

2. Generalidades:

2.1. Profesión:

Ing. de Sistemas	<input checked="" type="checkbox"/>	Ing. Informático	<input type="checkbox"/>
Ing. de Software	<input type="checkbox"/>	Otros	<input type="checkbox"/>

2.2. Años de Experiencia:

1 - 5 () 5 - 10 () 10 a más años ()

2.3. Elección de la Metodología:

Para la elección de la Metodología se aplicarán los siguientes criterios:

- ✓ **Flexibilidad:** Se refiere a la adaptabilidad de la metodología frente a la multiplicidad de acontecimientos que tienen lugar en el proceso de desarrollo de software.
- ✓ **Información:** Se refiere a si existe información (bibliografía, antecedentes, etc.) de la metodología.
- ✓ **Compatibilidad:** Si es o no compatible para el desarrollo web.
- ✓ **Costo de desarrollo:** Se refiere a que tanto cuesta el desarrollo de software como consecuencia de usar la metodología.

- ✓ **Tiempo de desarrollo:** Si la metodología ayuda a extender un poco de tiempo de desarrollo del proyecto, sin perjudicarlo.
- ✓ **Herramienta a medida:** Se refiere a que si hay una herramienta de modelamiento exclusiva para esta metodología.
- ✓ **Participación del cliente:** Se refiere a la participación que tiene el cliente en el proceso de desarrollo de software.

Para la adición de la puntuación de seguirá la siguiente escala de Valorización:

VALORACIÓN	ESCALA
Pésimo	1
Malo	2
Regular	3
Bueno	4
Excelente	5

Calificación de la Metodología de acuerdo a Criterios y Escala de Valoración:

CRITERIO	RUP	XP	ICONIX	SCRUM
Flexibilidad	4	5	5	4
Información	4	5	5	4
Compatibilidad	4	4	5	5
Costo de Desarrollo	2	4	5	5
Tiempo de Desarrollo	2	4	5	4
Herramienta a medida	3	5	5	4
Simplicidad	2	5	5	4
Participación del cliente	4	4	5	4

ENCUESTA DE SELECCIÓN DE LA METODOLOGÍA

Nombre del Proyecto: "Sistema basado en RFID para Mejorar la Seguridad de Acceso a las Oficinas en la Subgerencia del MTC de La Libertad, 2018"

Nombre del Especialista:

Edum Raúl Mendoza Torres

Profesión:

ING. INFORMÁTICO

Lugar de Trabajo:

UCV

Cargo que desempeña:

DOCENTE T.P.

Fecha:

14/11/2018

DNI:

18176211



Formato de Encuesta a Expertos para la Selección de Metodología

Objetivo: Reunir información esencial para la selección de la metodología a aplicar en el desarrollo de la tesis.

Dirigido a: Profesionales con experiencia en metodologías de desarrollo para la elaboración de la tesis.

1. Nombres y Apellidos: Edum Mendoza Torres

2. Generalidades:

2.1. Profesión:

Ing. de Sistemas	()	Ing. Informático	(X)
Ing. de Software	()	Otros	()

2.2. Años de Experiencia:

1 - 5 () 5 - 10 () 10 a más años (X)

2.3. Elección de la Metodología:

Para la elección de la Metodología se aplicarán los siguientes criterios:

- ✓ **Flexibilidad:** Se refiere a la adaptabilidad de la metodología frente a la multiplicidad de acontecimientos que tienen lugar en el proceso de desarrollo de software.
- ✓ **Información:** Se refiere a si existe información (bibliografía, antecedentes, etc.) de la metodología.
- ✓ **Compatibilidad:** Si es o no compatible para el desarrollo web.
- ✓ **Costo de desarrollo:** Se refiere a que tanto cuesta el desarrollo de software como consecuencia de usar la metodología.

- ✓ **Tiempo de desarrollo:** Si la metodología ayuda a extender un poco de tiempo de desarrollo del proyecto, sin perjudicarlo.
- ✓ **Herramienta a medida:** Se refiere a que si hay una herramienta de modelamiento exclusiva para esta metodología.
- ✓ **Participación del cliente:** Se refiere a la participación que tiene el cliente en el proceso de desarrollo de software.

Para la adición de la puntuación de seguirá la siguiente escala de Valorización:

VALORACIÓN	ESCALA
Pésimo	1
Malo	2
Regular	3
Bueno	4
Excelente	5

Calificación de la Metodología de acuerdo a Criterios y Escala de Valoración:

CRITERIO	RUP	XP	ICONIX	SCRUM
Flexibilidad	4	5	5	4
Información	4	5	5	4
Compatibilidad	4	5	5	5
Costo de Desarrollo	2	4	5	5
Tiempo de Desarrollo	2	4	5	4
Herramienta a medida	3	5	5	4
Simplicidad	2	4	5	4
Participación del cliente	4	4	5	4

Anexo 4. Metodología de desarrollo.

1. Fase 1: Requerimientos.

1.1. Requerimientos Funcionales

➤ Registro de Datos

-El sistema tendrá registrado:

- ✓ **Nombre**
- ✓ **Número de celular de la Persona encargada**
- ✓ **Código ID de la Tarjeta**

➤ Muestra de datos:

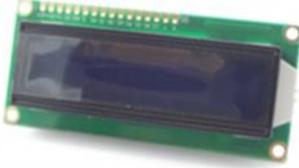
-El sistema al insertar la tarjeta al módulo RFID mandara luego de 15 segundos un mensaje mostrando:

- ✓ Nombre de la persona que tiene la tarjeta
- ✓ El horario en el que se hizo el ingreso
- ✓ Mensaje de alerta indicando que la tarjeta insertada es invalida en caso de que no esté registrada dicha tarjeta.

1.2. Requerimientos No Funcionales

- ✓ Muestra el nombre de la Persona que ingreso en tiempo real.
- ✓ Rápida respuesta con respecto a los mensajes enviados.
- ✓ Enfocado a dar accesos
- ✓ Protegido por un case color blanco.
- ✓ Tiempo corto en implementación.
- ✓ Fácil reemplazo de componentes.
- ✓ Integridad de la información del sistema.
- ✓ Fácil mantenimiento del hardware.
- ✓ Interfaz amigable y dinámica.
- ✓ Mayor portabilidad del equipo.
- ✓ Disposición a la información correcta.
- ✓ Disponibilidad de las 24 horas a la semana.
- ✓ Basado en tecnología Arduino Uno
- ✓ Basado en tecnología RFID
- ✓ Soporte Inmediato

1.3. Requerimientos de Hardware

Nombre	Descripción	Dispositivo
Arduino Modelo ARD-UNO	<p>Arduino Uno R3 posee 14 entradas/salidas digitales (6 pueden usarse como PWM), 6 entradas analógicas, un resonador cerámico de 16 MHz, conexión USB, conector de alimentación, conector ICSP y un botón de Reset. La tarjeta contiene todo lo necesario para el funcionamiento del microcontrolador; basta conectarlo al puerto USB o alimentarlo con una fuente de voltaje continuo o una batería para empezar a usarlo.</p>	
Display Alfanumérico LCD 1602	<p>Pantalla alfanumérica de 2 filas y 16 columnas. Backlight tipo LED color Azul. Interfaz paralela. Controlador compatible HD44780.</p>	
Módulo RFID RC522	<p>El Módulo RC522 es Lector-Grabador RFID, posee comunicación SPI permitiéndole trabajar fácilmente con la mayoría de los microcontroladores. Utiliza un sistema de modulación y demodulación para todo tipo de dispositivos pasivos de 13.56MHz. El dispositivo maneja el ISO14443A y soporta el algoritmo de encriptación</p>	

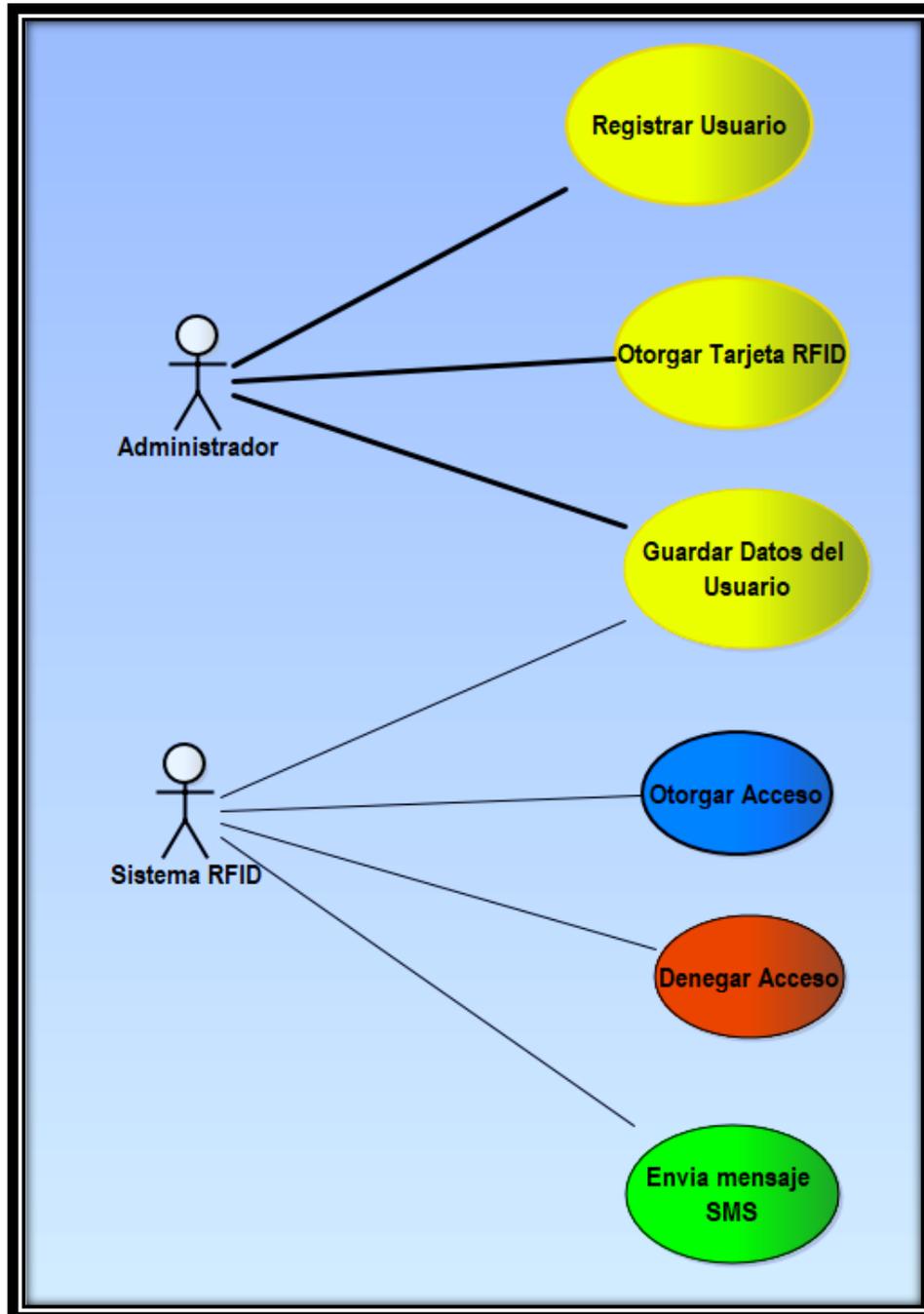
		Quick CRYPTO1 y MIFARE. El rango de detección de tags RFID es de aprox. 5-7 cm.	
Led difuso	5mm-Modelo LED-01	Los leds agregan siempre un toque llamativo a nuestros proyectos. Este modelo de led tiene la cubierta difusa, por lo que la luz se difumina por casi todo el led, logrando un efecto más agradable a la vista. Hemos seleccionado especialmente este led para nuestro starter kit por sus excelentes prestaciones. Ideal para trabajar con Arduino y Protoboard, puedes cargar el sketch: "Blink" para tus primeras pruebas.	
Shield	SIM900 GSM/GPR-Modelo SHD-GSM/GPRS-900	El Shield GPRS/GSM SIM900 es la forma más sencilla de conectar tus proyectos con Arduino a la red celular y de esta forma poder enviar y recibir mensajes de texto (SMS), llamadas de voz y hasta conectarte a Internet vía GPRS y entrar así al mundo del Internet de las cosas (IoT).	
Cable Dupont hembra a macho 10cm / 20Und-	Modelo CABLE-DPHM-10	Cable Dupont hembra a macho 10cm para realizar conexiones entre Arduino y sus módulos de forma sencilla.	

<p>Piezo Buzzer activo 12mm-Modelo SOUND- BUZZER-12</p>	<p>Este modelo de buzzer es de tipo activo por lo que su funcionamiento es muy sencillo, solo es necesario alimentar el buzzer para emitir sonido.</p>	
<p>Solenoides Tipo Chapa 12V</p>	<p>Este solenoide tiene un eje con un corte inclinado y un soporte de montaje. Es básicamente una cerradura electrónica diseñada para un gabinete, una puerta, un seguro etc.</p>	

2. Fase 2: Análisis y Diseño

➤ Diagrama de caso de Uso:

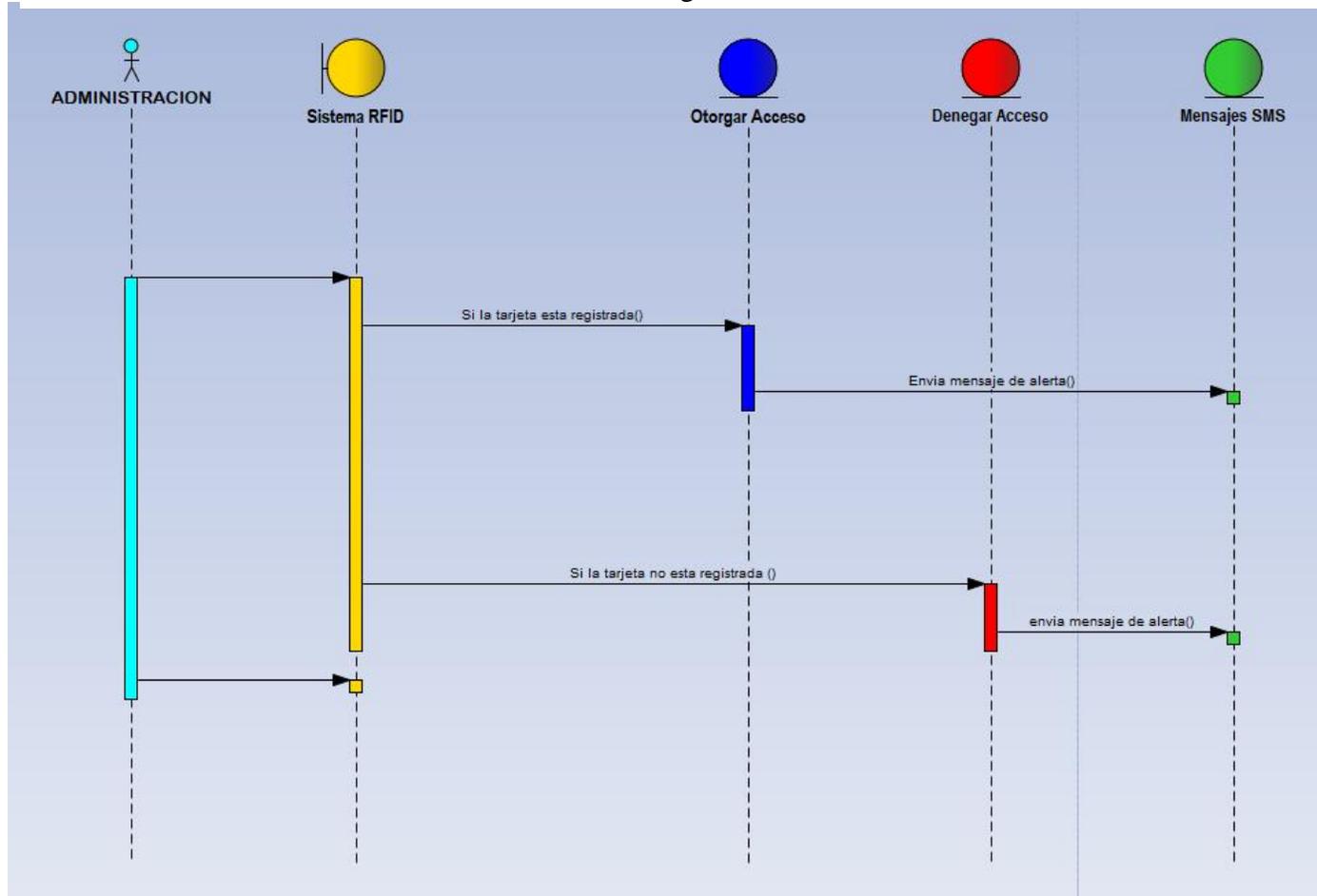
Ilustración 12. Diagrama de caso de Uso



Elaboración: Pro

➤ Diagrama de robustez

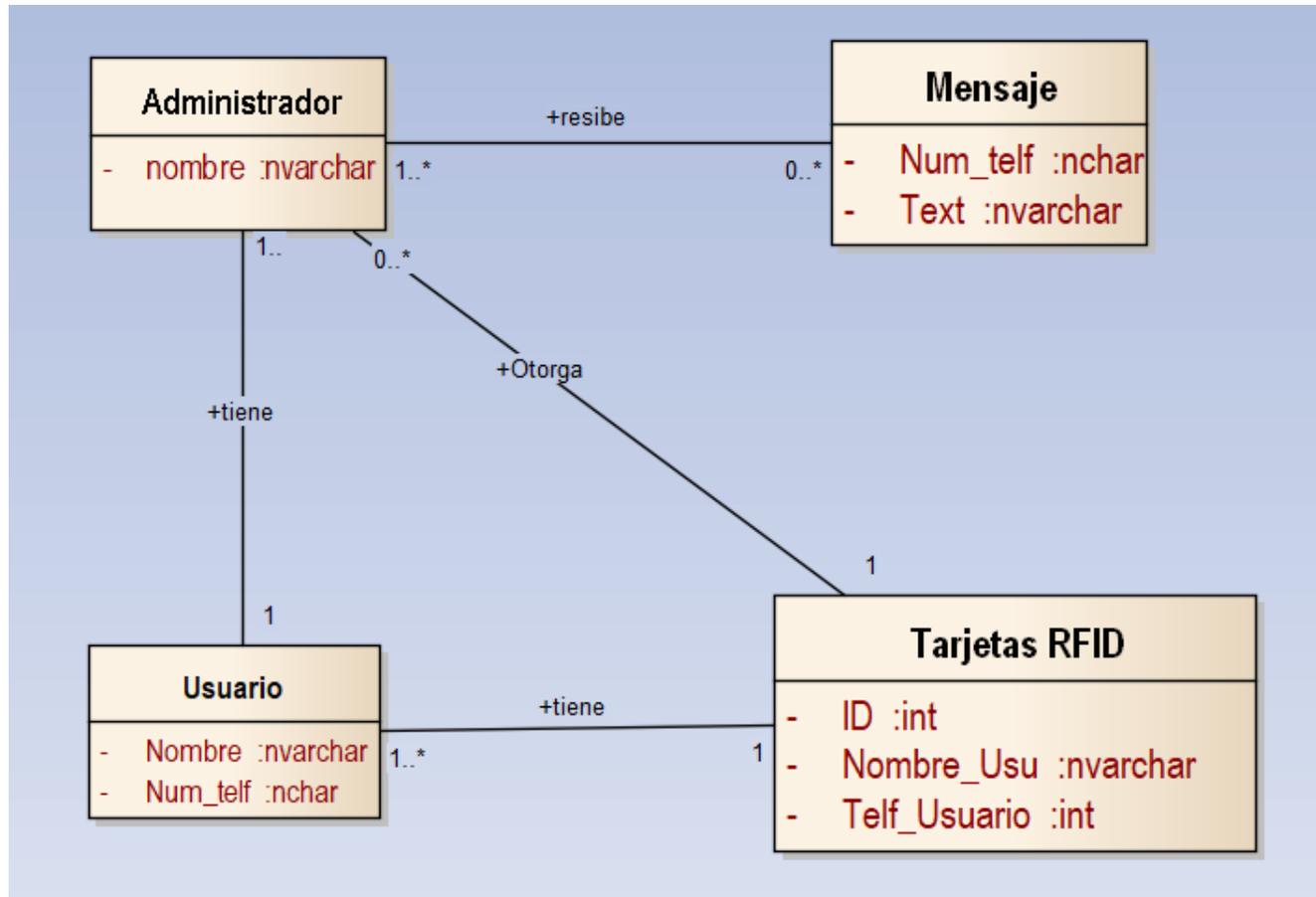
Ilustración 13. Diagrama de robustez



Elaboración propia

➤ Diagrama mediante modelo de Dominio

Ilustración 14. Diagrama de modelo de Dominio

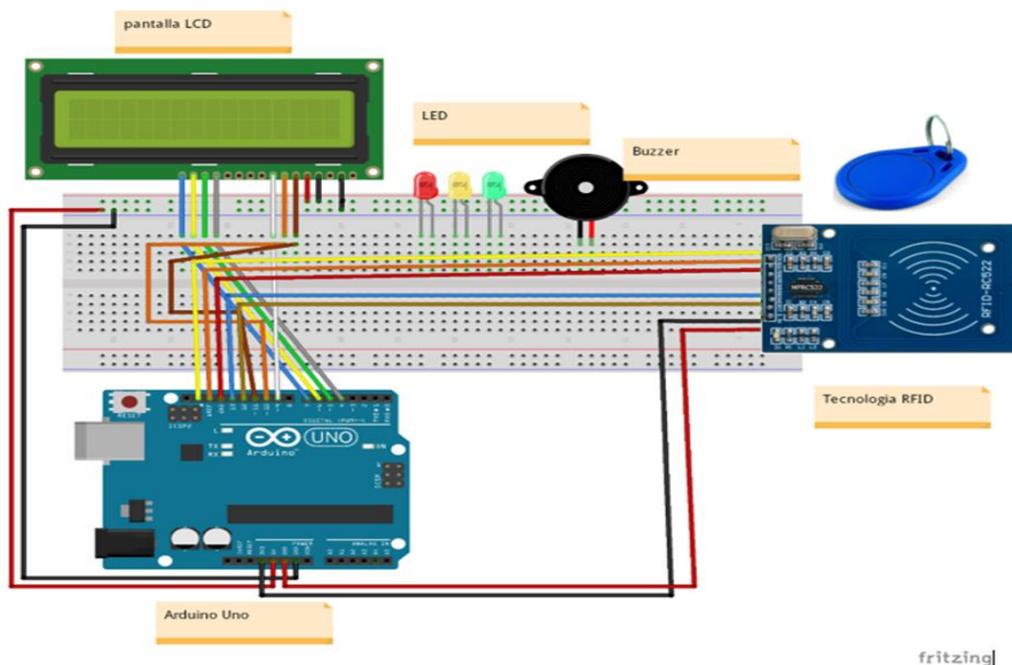


Elaboración: Propia

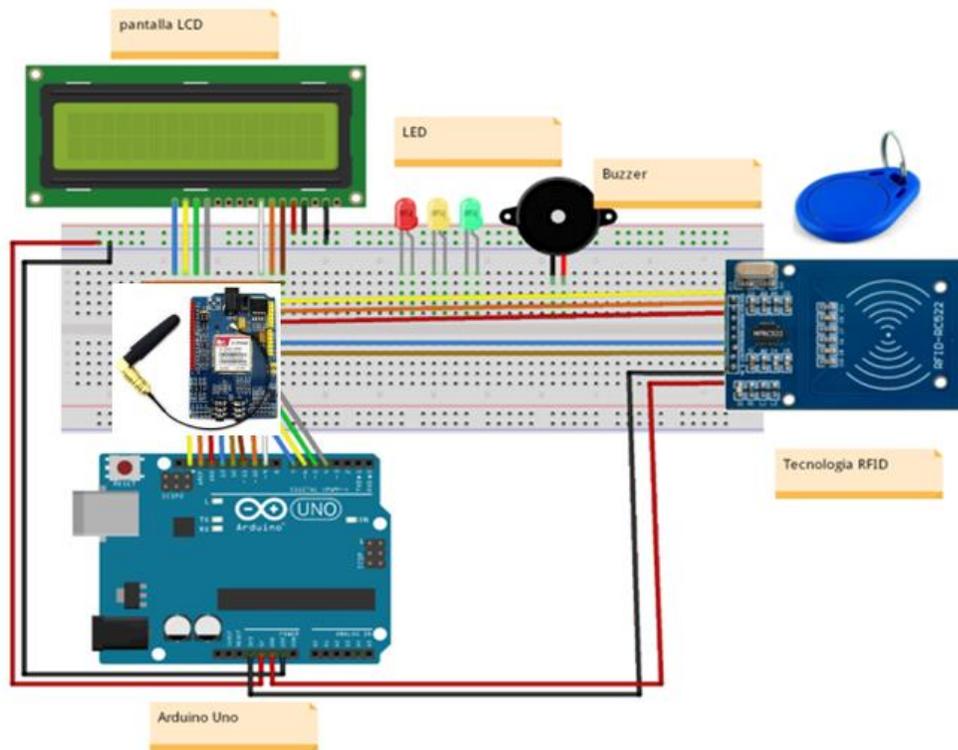
3. Fase 3: Diseño:

3.1. Arquitectura del Hardware:

3.1.1. Circuito del prototipo Inicial del Sistema



DESCRIPCIÓN: En el siguiente prototipo nos muestra los componentes que empleamos para el desarrollo inicial de nuestro Sistema, donde inicialmente se observa la pantalla led, Arduino Uno, los leds, el buzzer, el módulo Rfid, como se puede observar en esta oportunidad aún no se define si se usara el módulo GSM.



DESCRIPCIÓN: En el siguiente prototipo se determinó el uso de GSM, el cual enviara mensaje tanto para cuando haya habido un acceso o un acceso denegado por algún Trabajador del área.

3.1.2. Diseño final de nuestro Sistema:

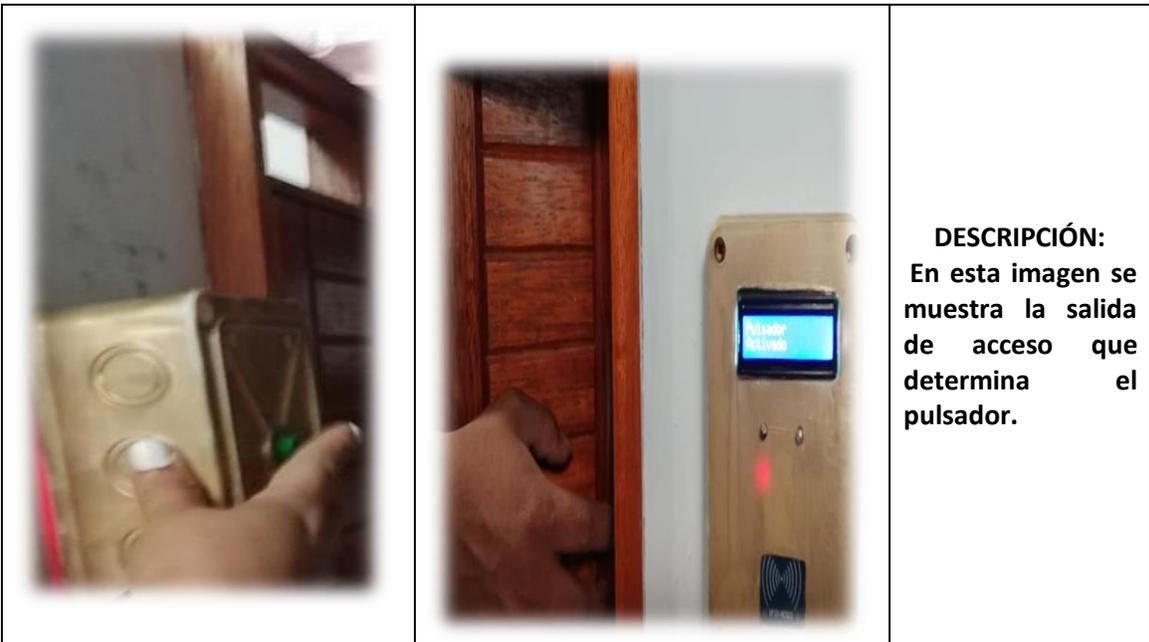


DESCRIPCIÓN: Como se puede apreciar nuestro prototipo fue elaborado en una caja de paso donde se observa una pantalla Led, y debajo se colocaron dos leds una Verde y otro Azul, en el que el led verde nos indicara que al insertar la tarjeta Rfid el acceso es concedido, pero si la tarjeta no se encuentra se activara el led Azul y a su vez enviara un mensaje en tiempo real indicando que el acceso esta denegado.

4. Fase 4: Implementación:

4.1. Pruebas Funcionales:







DESCRIPCIÓN:

En esta imagen se muestra el acceso denegado al usuario donde no se le ha otorgado el ingreso, debido a que la tarjeta no está registrada en el sistema.



DESCRIPCIÓN:

En esta imagen se muestra los mensajes que el sistema envía después de cada ingreso y alerta que se generan durante el día.

Anexo 5. Prototipo del Sistema RFID.

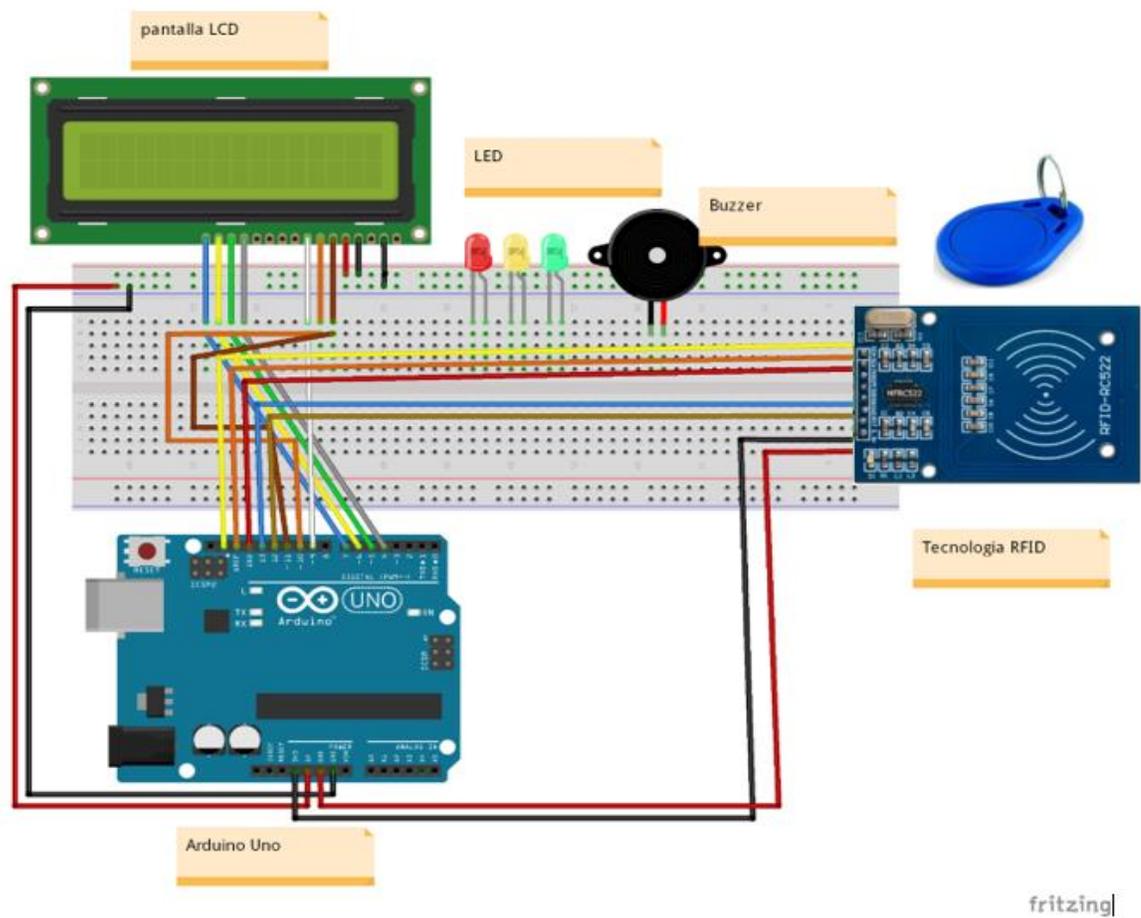


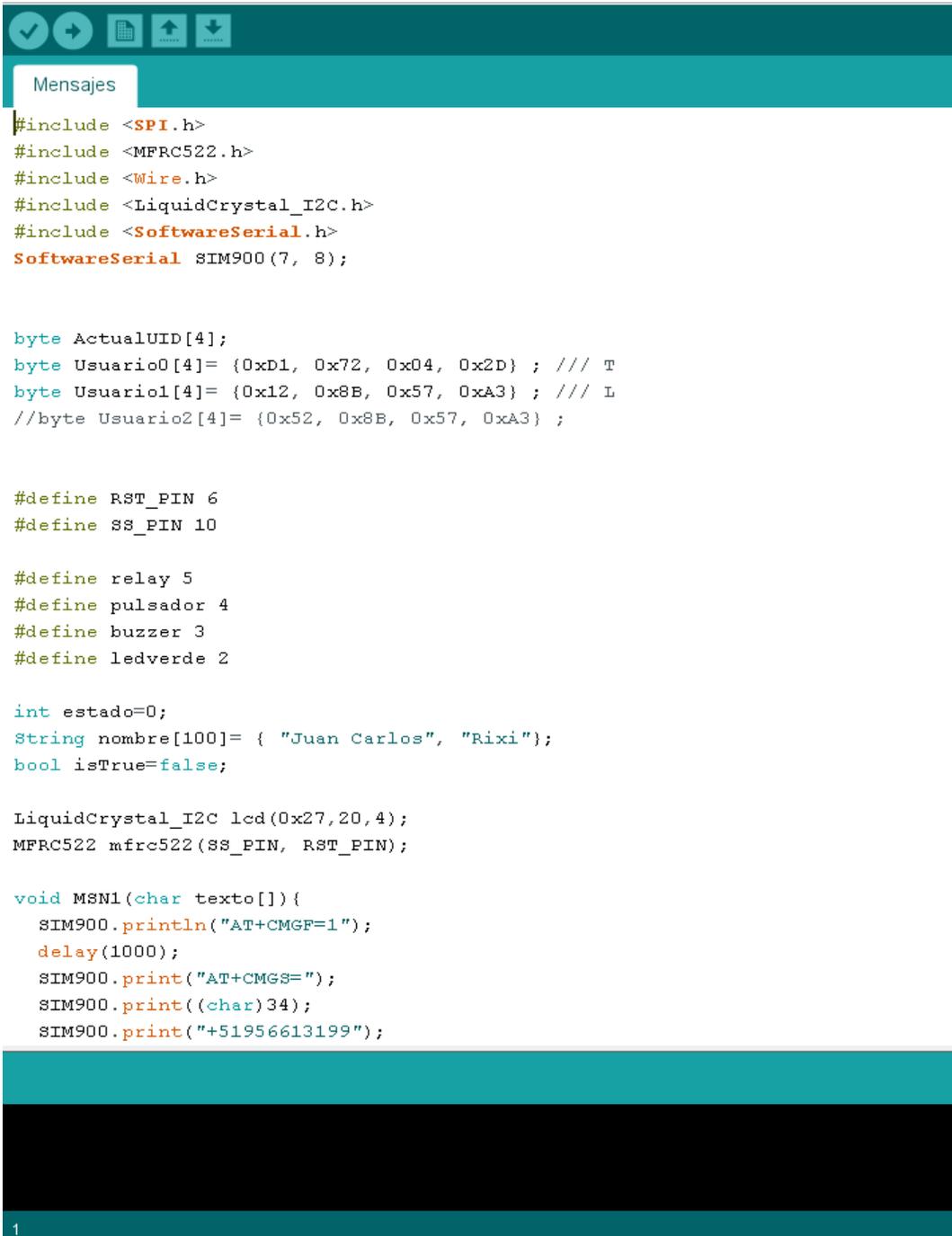
Ilustración 16. Prototipo del Sistema Rfid

Fuente: Elaboración Propia

Anexo 6. Código Empleado en el Sistema

Mensajes Arduino 1.8.9

Archivo Editar Programa Herramientas Ayuda



```
#include <SPI.h>
#include <MFRC522.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SoftwareSerial.h>
SoftwareSerial SIM900(7, 8);

byte ActualUID[4];
byte Usuario0[4]= {0xD1, 0x72, 0x04, 0x2D} ; /// T
byte Usuario1[4]= {0x12, 0x8B, 0x57, 0xA3} ; /// L
//byte Usuario2[4]= {0x52, 0x8B, 0x57, 0xA3} ;

#define RST_PIN 6
#define SS_PIN 10

#define relay 5
#define pulsador 4
#define buzzer 3
#define ledverde 2

int estado=0;
String nombre[100]= { "Juan Carlos", "Rixi"};
bool isTrue=false;

LiquidCrystal_I2C lcd(0x27,20,4);
MFRC522 mfrc522(SS_PIN, RST_PIN);

void MSN1(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);
  SIM900.print("AT+CMGS=");
  SIM900.print((char)34);
  SIM900.print("+51956613199");
```

```

Mensajes

SIM900.print((char)34);
SIM900.print("+51956613199");
SIM900.println((char)34);
delay(200);
SIM900.print(texto);
SIM900.print((char)26);
Serial.print("Mensaje 1 enviado");
}

void MSN2(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);
  SIM900.print("AT+CMGS=");
  SIM900.print((char)34);
  SIM900.print("+51924501982");
  SIM900.println((char)34);
  delay(200);
  SIM900.print(texto);
  SIM900.print((char)26);
  Serial.print("Mensaje 2 enviado");
}

void MSN3(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);
  SIM900.print("AT+CMGS=");
  SIM900.print((char)34);
  SIM900.print("+51947212223");
  SIM900.println((char)34);
  delay(200);
  SIM900.print(texto);
  SIM900.print((char)26);
  Serial.print("Mensaje 3 enviado");
}

void MSN4(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);

```

```

SIM900.println("AT+CMGF=1");
delay(1000);
SIM900.print("AT+CMGS=");
SIM900.print((char)34);
SIM900.print("+51956613199");
SIM900.println((char)34);
delay(200);
SIM900.print(texto);
SIM900.print((char)26);
Serial.print("Mensaje 4 enviado");
}

void MSN5(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);
  SIM900.print("AT+CMGS=");
  SIM900.print((char)34);
  SIM900.print("+51924501982");
  SIM900.println((char)34);
  delay(200);
  SIM900.print(texto);
  SIM900.print((char)26);
  Serial.print("Mensaje 5 enviado");
}

void MSN6(char texto[]){
  SIM900.println("AT+CMGF=1");
  delay(1000);
  SIM900.print("AT+CMGS=");
  SIM900.print((char)34);
  SIM900.print("+51947212223");
  SIM900.println((char)34);
  delay(200);
  SIM900.print(texto);
  SIM900.print((char)26);
  Serial.print("Mensaje 6 enviado");
}

```



```

boolean COMPARAR(byte array1[],byte array2[]){
    if(array1[0] != array2[0])return(false);
    if(array1[1] != array2[1])return(false);
    if(array1[2] != array2[2])return(false);
    if(array1[3] != array2[3])return(false);
    return(true);
}

void RF(){
    estado=digitalRead(pulsador);
    if(estado==0){
        lcd.clear();
        lcd.setCursor(0,0);
        lcd.print("Pulsador");
        lcd.setCursor(0,1);
        lcd.print("Activado");
        //digitalWrite(ledverde,HIGH);
        digitalWrite(relay,LOW);
        delay(2000);
        //digitalWrite(ledverde,LOW);
        digitalWrite(relay,HIGH);
        lcd.clear();
        lcd.print("Pase tarjeta...");
    }

    if ( mfr522.PICC_IsNewCardPresent()){

        if ( mfr522.PICC_ReadCardSerial()){

            lcd.clear();
            //lcd.setCursor(0,0);
            //lcd.print("Card UID: ");
            lcd.setCursor(0,1);
            for (byte i = 0; i < mfr522.uid.size; i++) {
                //lcd.print(mfr522.uid.uidByte[i] < 0x10 ? " 0" : " ");
            }
        }
    }
}

```

```

//lcd.print(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " ");
//lcd.print(mfrc522.uid.uidByte[i], HEX);
ActualUID[i]= mfrc522.uid.uidByte[i];
}
delay(1000);

if(COMPARE(ActualUID, Usuario0)){
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.println("Acceso concedido...");
  lcd.setCursor(0, 1);
  lcd.println(nombre[0]);      //Juan Carlos
  digitalWrite(ledverde,HIGH);
  digitalWrite(relay,LOW);
  MSN1("Ingreso de Juan Carlos");
  delay(1000);
  MSN2("Ingreso de Juan Carlos");
  delay(1000);
  MSN3("Ingreso de Juan Carlos");
  delay(1000);
  MSN4("Ingreso de Juan Carlos");
  delay(1000);
  MSN5("Ingreso de Juan Carlos");
  delay(1000);
  MSN6("Ingreso de Juan Carlos");
  lcd.clear();
  lcd.print("Espere por favor...");
  isTrue=true;
}else
if(COMPARE(ActualUID, Usuario1)){
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.println("Acceso concedido...");
  lcd.setCursor(0, 1);
  lcd.println(nombre[1]);

```

```

    lcd.setCursor(0, 1);
    lcd.println(nombre[1]);
    digitalWrite(ledverde, HIGH);
    digitalWrite(relay, LOW);
    MSN1("Ingreso de Rixi Alexandra");
    delay(1000);
    MSN2("Ingreso de Rixi Alexandra");
    delay(1000);
    MSN3("Ingreso de Rixi Alexandra");
    delay(1000);
    MSN4("Ingreso de Rixi Alexandra");
    delay(1000);
    MSN5("Ingreso de Rixi Alexandra");
    delay(1000);
    MSN6("Ingreso de Rixi Alexandra");
    lcd.clear();
    lcd.print("Espere por favor...");
    isTrue=true;
}
lcd.clear();
lcd.println("Acceso denegado...");
digitalWrite(buzzer, HIGH);
delay(500);
digitalWrite(buzzer, LOW);
delay(300);
digitalWrite(buzzer, HIGH);
delay(500);
digitalWrite(buzzer, LOW);
delay(1000);
digitalWrite(buzzer, HIGH);
MSN1("ALERTA, Ingreso denegado");
delay(1000);
MSN2("ALERTA, Ingreso denegado");
delay(1000);
MSN3("ALERTA, Ingreso denegado");

```

```

    digitalWrite(buzzer, HIGH);
    delay(500);
    digitalWrite(buzzer, LOW);
    delay(300);
    digitalWrite(buzzer, HIGH);
    delay(500);
    digitalWrite(buzzer, LOW);
    delay(1000);
    digitalWrite(buzzer, HIGH);
    MSN1("ALERTA, Ingreso denegado");
    delay(1000);
    MSN2("ALERTA, Ingreso denegado");
    delay(1000);
    MSN3("ALERTA, Ingreso denegado");
    delay(100);
    MSN4("ALERTA, Ingreso denegado");
    delay(1000);
    MSN5("ALERTA, Ingreso denegado");
    delay(1000);
    MSN6("ALERTA, Ingreso denegado");
    lcd.clear();
    lcd.print("Espere por favor...");
    isTrue=false;
  }
  isTrue=false;
  delay(3000);
  digitalWrite(buzzer, LOW);
  digitalWrite(ledverde, LOW);
  digitalWrite(relay, HIGH);
  lcd.clear();
  lcd.print("Pase tarjeta...");
  mfr522.PICC_HaltA();
}
}
}

```



```
lcd.backlight();
Serial.begin(9600);
SIM900.begin(9600);

lcd.setCursor(0,0);
lcd.print("Actualizando");
lcd.setCursor(0,1);
lcd.print("Sistema...");

pinMode(relay, OUTPUT);
pinMode(pulsador, INPUT);
pinMode(buzzer, OUTPUT);
pinMode(ledverde, OUTPUT);
pinMode(9, OUTPUT);
digitalWrite(relay, HIGH);
delay(2000);

delay(500);

digitalWrite(9, LOW);
delay(1000);
digitalWrite(9, HIGH);
delay(2000);
digitalWrite(9, LOW);
delay(1000);

lcd.clear();
lcd.print("Pase tarjeta...");
delay(2000);

}

void loop() {
RF();
}
```

Anexo 7. Presupuesto:

Tabla 15.Presupuesto

Clasificador de Gastos (2019)	Descripción	Cantidad	Precio unitario (S/.)	Costo Total
Recursos Humanos				
2.1.1.5.1.1	Tesistas	8 meses	210.00	7,440.00
2.1.1.5.1.2	Asesor Proyecto	32 asesorías	50.00	1,600.00
Sub Total S/.				S/9,040.00
Recursos Materiales				
2.2.1.5.1.1	Lapiceros	02	1.00	2.00
2.2.1.5.1.2	Memoria USB 8 GB	02	30.00	60.00
2.2.1.5.1.3	Fólder manila A4 c/Fast	20	1.00	20.00
2.2.1.5.1.4	Laptop	02	2500.00	5000.00
2.2.1.5.1.5	Engrapador	01	12.00	12.00
2.2.1.5.1.6	Grapas	02	5.00	10.00
2.2.1.5.1.7	Perforador	01	8.50	8.50
Sub Total S/.				S/5,112.50
Hardware				
2.3.1.5.1.1	Arduino Uno	01	40.00	40.00
2.3.1.5.1.2	Pantalla LED	01	16.00	16.00
2.3.1.5.1.3	RFID	01	20.00	20.00
2.3.1.5.2.4	LED	02	0.20	0.40
2.3.1.5.2.5	Módulo GSM	01	170.00	170.00
2.3.1.5.2.6	Jumper	01	10.00	10.00
2.3.1.5.2.7	Buzzer	01	1.00	1.00

2.3.1.5.3.8	Cerradura Eléctrica	01	28.00	28.00
2.3.1.5.3.9	Módulo Relay 5vdc	01	6.00	6.00
2.3.1.5.3.10	Puerta de madera	01	150.00	150.00
2.3.1.5.3.11	Resistencia	01	0.10	0.10
2.3.1.5.3.12	Pulsador	01	1.00	1.00
2.3.1.5.3.13	Pines digitales	04	0.50	2.00
2.3.1.5.3.14	Soldador eléctrico	01	18.00	18.00
2.3.1.5.3.15	Cautín	01	15.00	15.00
2.3.1.5.3.16	Pasta de soldar	01	12.00	12.00
2.3.1.5.3.17	Caja de paso	01	7.00	7.00
2.3.1.5.3.18	Modulo adaptador LED a I2C	01	7.00	7.00
2.3.1.5.3.19	Chip	01	5.00	5.00
2.3.1.5.3.20	Cinta negra de electricidad	01	6.50	6.50
Sub Total S/.				S/. 515.00
Software				
2.4.1.5.3.1	Windows 10 Home	02	30.00	60.00
2.4.1.5.3.2	Office 2016	02	55.00	110.00
2.4.1.5.3.3	IDE de Arduino	01	00.00	00.00
Sub Total S/.				S/.170.00
Otros Servicios				
2.5.2.2.2.1	Internet de hogar	8 meses	129.00	1,032.00
	Internet de hogar	8 meses	70.00	560.00

2.5.2.1.2.2	Transporte x 2	80 pasajes	2.00	160.00
2.5.2.1.2.3	Visitas x 2	6 pasajes	3.00	36.00
2.5.2.2.2.4	Impresiones	300 hojas	0.10	30.00
2.5.2.2.2.5	Energía eléctrica	8 meses	80.00	640.00
	Energía eléctrica	8 meses	80.00	640.00
Sub Total S/.				S/. 3,098.00
Total, S/.				S/.17,935.50

Elaboración: Propia

Anexo 8. Viabilidad Económica

➤ Flujo de Caja

Tabla 16. Flujo de Caja

Descripción	Año 0	Año 1	Año 2	Año 3
INVERSIÓN (S/)				
Recursos Humanos	9,040.00	9,200.00	9,400.00	9,600.00
Materiales e Insumos	5,112.50	5,200.00	5,400.00	5,600.00
Hardware	515.00	580.00	600.00	650.00
Software	170.00	200.00	300.00	400.00
Servicios y Otros	3,098.00	3,200.00	3,400.00	3,600.00
COSTO TOTAL (S/)	17,935.50	18,380.00	19,100.00	19,835.00
BENEFICIOS				
Beneficios Tangibles		18,380.00	19,100.00	19,835.00
TOTAL (S/)	-17,935.50	18,380.00	19,100.00	19,835.00
FLUJO DE CAJA (S/)	-17,935.50	444.50	19,544.50	39,379.50

Elaboración: Propia

➤ Análisis de rentabilidad

✓ VAN (Valor Actual Neto)

Si VAN es mayor a 0 entonces el proyecto es rentable y se acepta.

$$VAN = -A + \sum_{t=1}^n \frac{Q_t}{(1+k)^t}$$

Donde:

A = Desembolso inicial

Qt = Flujo de caja en el periodo t

k = Costo capital

n = Vida útil estimada para la inversión

Reemplazamos:

$$VAN = -17,935.50 + \sum \left[\frac{444.50}{(1+0.06)^1} + \frac{19,544.50}{(1+0.06)^2} + \frac{39,380.00}{(1+0.06)^3} \right]$$

$$VAN = -17,935.50 + 50,878.09$$

$$VAN = 32,942.59$$

El proyecto es rentable y se acepta.

✓ **C/B (Costo Beneficio)**

$$BC = \frac{\text{Valor Actual}}{\text{Desembolso Inicial}}$$

$$BC = \frac{32,942.59}{17,935.50} = 1.83$$

Por cada S/ 1.00 invertido se obtendrá una ganancia de S/ 0.83

✓ **TIR (Tasa Interna de Retorno)**

Se compara con la tasa que ofrecen los bancos en este caso se utilizara la tasa de interés del Banco de crédito ($i = 45\%$).

$$TIR = -Ci + \sum_{i=1}^n \frac{(Flujo\ de\ Caja)}{(1+i)^n} = 0$$

$$TIR = -17,935.50 + \frac{444.50}{(1+0.45)^1} + \frac{19,544.50}{(1+0.45)^2} + \frac{39,380.00}{(1+0.45)^3} = 0$$

$$TIR = 0,45$$

Conociendo que el valor del TIR es de 45% definimos este valor es mayor que el interés que ofrece el banco de crédito, por lo que puede ser provechoso sin invertir este dinero.

✓ **Tiempo de recuperación del capital**

$$TRC = \frac{InversionInicial}{PromedioBeneficioNeto}$$

$$TRC = \frac{17,935.50}{19,835.00}$$

$$TRC = 0.90$$

Convertir a Meses y Días

$$0.90 * 12\ Meses = 10.80$$

$$0.80 * 31\ Dias = 24.8$$

El capital se recupera en 10 meses y 25 días.