



UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.
PROCESO DE TITULACIÓN
DICIEMBRE 2021 – ABRIL 2022
EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA
PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

**ANÁLISIS Y DISEÑO DE UN SISTEMA QUE PERMITA EL CONTROL DE
ACCESO AL PERSONAL ADMINISTRATIVO UBICADO EN LA MATRIZ DE LA
UNIVERSIDAD TECNICA DE BABAHOYO, UTILIZANDO TECNOLOGIA RFID.**

ESTUDIANTE:

CRISTIAN WASHINGTON AVILÉS MAYORGA

TUTOR:

MSc. NARCISA MARIA CRESPO TORRES

AÑO 2022

Resumen

Esta situación de análisis tiene como intención facilitar al ingreso al personal administrativo localizado en la matriz de la Universidad Técnica de Babahoyo debido a que con esta finalidad se lograría mejorar la estabilidad la cual se trabajaría con tecnología rfid o identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID.

Como estudiante de la Universidad Técnica de Babahoyo de la facultad de administración finanzas e informática he podido palpar que no hay un preciso control en el acceso del personal administrativo situado en la matriz de la universidad técnica de Babahoyo, es por ello que estoy convencido que mi caso de estudio tiene alto porcentaje de factibilidad, ya que actualmente el desarrollo y uso de nuevas tecnologías nos permite supervisar a los sujetos de manera eficiente y eficaz.

Palabras claves

Seguridad, Optimizando, arduino, autenticidad.

PLANTEAMIENTO DEL PROBLEMA

El presente caso de estudio está enfocado en el análisis y diseño de un sistema que permita el control de acceso al personal administrativo ubicado en la matriz de la Universidad Técnica de Babahoyo, utilizando la tecnología rfid.

En la ciudad de Babahoyo ha incrementado en un gran porcentaje el índice de delincuencia organizada, por lo que ha surgido la necesidad de crear un sistema eficiente que controle el acceso del personal que labora y se ubica en las instalaciones de la matriz de la Universidad Técnica de Babahoyo para precautelar la seguridad e integridad de valiosa documentación que ahí se encuentran, con esto se protege y evita que haya información falseada o mal utilizada, además también se cuida la integridad de material físico y tecnológico que reposa dentro de la institución ya que solo podrá acceder personal autorizado, y serán responsables específicos los individuos que tienen acceso a la matriz.

Un breve estudio realizado en la Universidad Técnica de Babahoyo, en la Facultad de Administración, Finanzas e Informática se ha podido palpar que dicha institución cuenta con un sistema ineficiente de vigilancia, por lo que no hay un estricto control en el acceso del personal administrativo ubicado en la matriz de la Universidad Técnica de Babahoyo, Lo que de cierta manera genera gran preocupación sobre el tema de la inseguridad que existe en esta área donde reposan muchos documentos de gran importancia y equipos como: ordenadores de escritorios y laptops que contienen información vital para cada uno de los educandos que han confiado su carrera universitaria en la entidad.

La Universidad Técnica de Babahoyo con la implementación de un sistema de control basado en la tecnología RFID, debido a esto tendríamos que seguir manteniendo los procedimientos manuales de control de acceso que se practican en la Universidad Técnica de Babahoyo.

Esta institución está ubicada en la Av. Universitaria km 2 ½ Av. Montalvo Babahoyo, contando con varias facultades como medicina, agronomía y algunas otras entre ellas la facultad de administración y finanzas a la que soy perteneciente.

No existe el acompañamiento de un sistema biométrico de control con el personal de seguridad, debido a que las personas encargadas (guardias de seguridad), no cuentan con un sistema informático viable al control de acceso del personal administrativo que se encuentra ubicado en la matriz de la Universidad Técnica de Babahoyo.

JUSTIFICACION

El presente caso de estudio es conducente por la necesidad de controlar el ingreso de personas no autorizadas a la matriz de la Universidad Técnica de Babahoyo.

La inseguridad nos conlleva al diseño de un sistema que permita controlar el acceso del personal, para evitar pérdidas, alteraciones y falseamientos en documentos y equipos tecnológicos de la misma.

La realización del proyecto consiente en la optimización de tiempo y recursos para la universidad, brindando estabilidad y seguridad para el personal de la entidad, además se ahorra la molesta tarea de buscar a la persona encargada de abrir y cerrar las puertas, de recoger la firma de entrada y salida ya que se automatiza y al aprobar el acceso también registra hora de ingreso y de abandono del lugar de trabajo permitiendo un control eficiente y eficaz a el mismo tiempo.

OBJETIVOS

OBJETIVO GENERAL

Analizar el diseño de un sistema que permita controlar el acceso al personal administrativo en la matriz de la Universidad Técnica de Babahoyo, optimizando tiempo y recursos con la facilidad y confiabilidad del uso de la tecnología RFID.

OBJETIVOS ESPECIFICOS

- ✓ Establecer un acceso correcto único y confiable para el personal administrativo que está ubicado en la matriz de la Universidad Técnica de Babahoyo.
- ✓ Utilizar la tecnología RFID, adquiriendo equipos biométricos como lectores de huellas para llevar a cabo el control de acceso del personal administrativo que está ubicado en la matriz de Universidad Técnica de Babahoyo.
- ✓ Convertir el obsoleto sistema manual de control de acceso al personal administrativo ubicado en la matriz de la Universidad Técnica de Babahoyo, en uno nuevo moderno y automatizado que facilite y agilite el trabajo generando seguridad y autenticidad solo de las personas que ahí laboran.

LÍNEAS DE INVESTIGACIÓN

Este caso de estudio pertenece a la línea de investigación de:

- ✓ sistema de información y comunicación.

Adquisición de conocimiento acerca de los diferentes sistemas de información que se manejan a nivel tecnológico, aprovechando así, los canales de comunicación para hacer viable este proyecto.

- ✓ emprendimiento e innovación.

Enfocado en el incremento de la productividad, basado en la mutación del futuro, con ideas nuevas que nos permitan crear con automatización y precisión.

MARCO CONCEPTUAL

Es muy importante reconocer que **seguridad** es la palabra clave para impulsar el análisis y diseño de un sistema que permita el ingreso de personas autorizadas a un lugar específico, en este caso se va a analizar y diseñar un sistema que permita el acceso al personal administrativo ubicado en la matriz de la Universidad Técnica de Babahoyo.

Desde los inicios de la tierra ha sido importante cuidar y proteger persona u objetos que los humanos consideran de gran importancia para ellos, desde aquellos tiempos hasta ahora se han suscitado una serie de cambios en el entorno y los avances tecnológicos han abarcado y facilitado gran parte de la vida, ahora contamos con la tecnología rfid o identificación por radiofrecuencia la que ha llegado con mucha fuerza y precisión a desplazar la mano de obra convencional posicionándose por ser muy segura, veraz, veloz y precisa con las lecturas de identificaciones y siendo actualizada constantemente.

Según el autor (CARRION, 2016; CARRION, 2016) La seguridad es un elemento de desarrollada importancia en la estructura fresca, su dispersión en todos los círculos sociales, determina el papel predominante de las actuales tecnologías que minimizando el desliz convencional del hombre ofrece amplia cobertura y despliegue para la catalogación de servicios, de esta manera, se puede decir que RFID es un sistema o método de descomplicada utilización que evita el error humano, esta tecnología ha demostrado auge en los últimos años hablando de auto caracterización de elementos ya que es muy segura y su valor no es elevado en comparación a otros

a otros sistemas que cumplen la misma gestión, esta tecnología conserva una constante evolución y se ha mantenido por su confiabilidad en la lectura de información por ser precisa y rápida.

Es decir la tecnología RFID es un avance tecnológico de mucha ayuda para los humanos ya que permite la rápida y eficiente identificación por medio de radiofrecuencias utilizando códigos únicos y auténticos.

También es un optimizador de recursos económicos y humanos ya que reemplaza a las personas que de ellos se encargaban y los precios son muy bajos en comparación de otros sistemas.

El empleo de las llamadas tecnologías emergentes dentro del espectro de la informática y la ingeniería de software, permite con la ayuda de las normativas proporcionadas por la ingeniería de software diseñar y construir soluciones cuyo impacto y valor agregado redundan en todos los escenarios de la llamada economía naranja o economía de conocimiento; la apropiación de los desarrollos inherentes a la tecnología RFID para su utilización en la definición y estructuración de modelos de identificación y seguridad, permiten al programa de Ingeniería de Sistemas de la Universidad Libre, participar como referente y consultor en el diseño de soluciones especializadas con alta calidad. (Angamarca, 2009).

Son tecnologías innovadoras, versión actualizada de tecnologías ya existentes tradicionales, convencionales que surgen de la necesidad de convertir, almacenar, ordenar, relatar tramitar o circular filiaciones ineludibles para cualquier diligencia humana que tenga que ver con el usos de computadoras y más aparatos electrónicos que estén relacionados a el internet la información, comunicación y robótica.

La tecnología de RFID es un sistema de auto identificación inalámbrico, el cual consiste de etiquetas que almacenan información y lectores que pueden leer a estas etiquetas a distancia. La tecnología RFID está siendo adoptada cada vez por más industrias debido a que su costo es cada vez menor y sus capacidades son mayores. Esto permite genera grandes beneficios como incrementos en la productividad y administración principalmente en los sectores de cadenas de suministro, transporte, seguridad y control de inventarios. (Sanchez, 2008).

Se impone cada vez más el uso de la tecnología biométrica en los sistemas de control de acceso, la tecnología de radiofrecuencia (RFID) en tarjetas, ya sean éstas con etiquetas (tags) pasivas o activas, continúa siendo un instrumento muy extendido. (CUCORENT, 2009).

Existen diferentes expectativas donde la tecnología rfid es aplicable, por ser de fácil ejecución, aplicación y adquisición.

Tags, son comandos o conjuntos de palabras claves que los programas cibernéticos o aplicaciones descifran para formar páginas, también conocidas como etiquetas de Wordpress y sirven para agrupar publicaciones dentro de un blog.

Sistemas autónomos: Analizan una sola entrada y son los acertados para un control de acceso básico. Con un único lector se puede dar de alta a muchos usuarios. Son sencillos de instalar y gestionar. (CUCORENT, 2009).

Sistemas centralizados: Se supervisan múltiples accesos a través de un sistema centralizado que lleva el control, compilando información de entradas, salidas e incidencias y posibilitando generar informes. (CUCORENT, 2009).

Sistemas distribuidos: Controlan varios ingresos en un mismo puesto mediante tecnología de radiofrecuencia. No necesitan cableado y son apropiados para un recinto con múltiples entradas. (CUCORENT, 2009).

Sistemas inalámbricos: De disposición inmediata, se adaptan a cualquier sistema. Al no necesitar cable, no requieren obra y su gran variedad permite encontrar una salida para cualquier problema o sistema de control de acceso. (CUCORENT, 2009).

Control de accesos en la nube: La nueva tecnología posibilita tener el control de los accesos de una empresa o negocio en el dispositivo móvil, ordenador o Tablet, manejando un control total de lo que ocurre en estos espacios, pudiendo abrir o bloquear entradas y conocer cualquier situación al instante. Se pueden administrar los permisos desde la web o desde una aplicación en tiempo real con un panel de control sencillo e intuitivo. (CUCORENT, 2009).

Evolución de la tecnología RFID

Entre las opciones RFID, los códigos de barra y las cintas magnéticas dependen de la relación directa con los beneficiarios. Además los códigos de barra solamente puede ser utilizados una vez y la información contenida en ellos no puede ser mejorada. (CUCORENT, 2009).

El acceso que se ejecuta es un método confiable dirigido al control en el ingreso y egreso del personal administrativo de la universidad técnica de Babahoyo.

La tecnología **RFID** en las tarjetas de acceso es un paso adelante en relación con las de banda magnética que exigen recorrer el lector manualmente por el lado de la banda. Por eso las tarjetas que incluyen tags (etiquetas) RFID se llaman «de proximidad», y basta con acercarlas al lector para que identifiquen al usuario. (CUCORENT, 2009).

Es interesante analizar la evolución de las etiquetas en el mundo RFID, ya que progresivamente iremos viendo cómo las etiquetas «activas» cobran protagonismo y comienzan a implementarse en sistemas de controles de accesos de personal. (CUCORENT, 2009).

Etiquetas rfid activas y semipasivas

Las etiquetas RFID pueden ser activas, semipasivas (o alimentadas por batería) o pasivas. El pasivo no requiere alimentación interna y solo se activa cuando el lector está cerca, proporcionándole la energía necesaria. La mayoría de las etiquetas RFID son etiquetas pasivas porque son mucho más baratas de fabricar y no requieren baterías. (CUCORENT, 2009).

Estas cartas pasivas no tienen poder. La señal proveniente del lector genera una pequeña corriente, suficiente para operar el chip de la tarjeta, el cual genera y transmite su respuesta, que

puede ser cualquier tipo de información, no solo un código de identificación. Su distancia utilizable real oscila entre 10 cm y varios metros, dependiendo de la frecuencia de funcionamiento, así como del diseño y tamaño de la antena. (CUCORENT, 2009).

Nuevas etiquetas (*tags*) RFID activas para los sistemas de controles de acceso

A pesar de ser más caras, el uso de etiquetas activas es cada vez más común. A diferencia de las pasivas, poseen su propia fuente autónoma de energía, gracias a la que son capaces de transmitir señales más potentes que las pasivas, por lo que son más eficientes en entornos dificultosos para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua) o el metal (contenedores, vehículos). Los datos de estos *tags* pueden leerse desde larga distancia transmitiendo en frecuencias de microondas (2,45 GHz). (CUCORENT, 2009).

Se ve una formación creciente de las etiquetas activas en sistemas de control de acceso, ya que no dependen de la intermediación directa con los usufructuarios ni de colocar las identificaciones cerca del lector como los códigos de barra, cintas magnéticas y lectores de proximidad y superan limitaciones engorrosas que generan desgastes de tiempo. (CUCORENT, 2009).

El sistema de control de acceso es un sistema técnico que inhabilita o permite el acceso a los administradores de la Universidad Técnica de Babahoyo, ubicado en la matriz de la organización y reporta el trabajo realizado para identificar la información aprobada y certificada. Permite el acceso a datos, personas o recursos utilizados para diferentes aplicaciones o plataformas.

Sistemas de Control de Acceso Autónomos.

Estas son tecnologías para controlar el acceso a uno o más puertos sin conectarse a una PC o sistema central, por lo que no guardan registros de eventos.

Si bien esta es una limitación importante, es posible que algunos controles de acceso discrecional no restrinjan el acceso programado o grupal a la puerta, según la calidad de la marca. En otras palabras, la forma más sencilla es simplemente utilizar un método de identificación (ya sea clave, proximidad o biométrico) como una "llave" electrónica. (CHESKYW).

Según (Pastorino, 2018) Las **cerraduras electromagnéticas** y las **cerraduras electrónicas** no son exactamente lo mismo.

Cuando hablamos de cerradura electrónica, nos referimos a un mecanismo que impide el acceso (como un picaporte en una cerradura tradicional), y cuando hablamos de cerradura electromagnética, nos referimos a un dispositivo magnetizador que utiliza una corriente eléctrica para forzar la puerta. Abierto. Cerrar La cerradura electromagnética consta de dos partes: un lado es un electroimán colocado dentro del marco, el otro lado es una placa de metal llamada parte móvil que se coloca en la puerta. Cuando la corriente fluye, creará un campo magnético que conecta las dos partes, cuando la corriente deja de funcionar, el campo magnético desaparece para ayudar a que las partes se separen y abran la puerta.

Diferencia entre cerradura electrónica y cerradura electromagnética

La diferencia principal entre las cerraduras electrónicas y las electromagnéticas responde a la pregunta: ¿qué pasa cuando se corta la energía?

Las cerraduras electromagnéticas son de tipo “Fail Safe” (si falla, estoy a salvo) lo que significa que se conservan cerradas mientras exista corriente eléctrica, pero ante un corte en el suministro la cerradura se libera y la puerta queda abierta. En cambio, las cerraduras electrónicas trabajan del modo “Fail Secure” (si falla, estoy asegurado) y operan de modo contrario: cuando no hay electricidad se mantienen cerradas. (Pastorino, 2018).

Es paradójico que la prioridad en caso de corte de energía, como en un failsafe fallido, dé prioridad a los que pueden salir ya que puede tratarse como un evento. En una situación de "emergencia", la prioridad es mantener la instalación cerrada y segura a pesar de un corte de energía. (Pastorino, 2018).

La primera gran desventaja de las cerraduras electromagnéticas es que, en caso de corte de corriente, ya no garantizan el acceso al mecanismo. La mayoría de las marcas solucionan este problema utilizando baterías o un SAI para mantener la cerradura encendida durante un tiempo. Sin embargo, en lugares donde a menudo ocurren cortes de energía, definitivamente es un problema a considerar. (Pastorino, 2018).

Independientemente de si son electromagnéticos o electrónicos, hay varias prioridades que debemos tener en cuenta cuando se trata de este tipo de cerraduras. La conclusión es que las llaves perdidas o robadas se pueden cancelar fácilmente. Dado que cada clave es única y tiene una identidad, basta con eliminar del sistema las claves perdidas o todas las claves pertenecientes a un vecino que ya no existen y nunca se han devuelto. (Pastorino, 2018).

Llaves RFID para cerraduras electrónicas y electromagnéticas: ¿cómo funcionan?

Las llaves que se utilizan en las cerraduras electrónicas y electromagnéticas no son como las tradicionales llaves de cobre, sino más bien como llaves o tarjetas. Estas claves utilizan diferentes variaciones del protocolo RFID para identificar al usuario y obtener acceso. (Pastorino, 2018)

La tecnología RFID se deriva del inglés Radio Frequency IDentification, que en español significa identificación por radiofrecuencia y su propósito debe ser utilizar ondas de radio para autenticar objetos. Para ello suele utilizarse un chip, que contiene datos de identificación y es leído por un lector sin contacto ya largas distancias. Los rituales más comunes de esta tecnología son: lectura de información de vehículos en movimiento, manejo de inventario de productos, identificación de titulares de pasaportes y documentos, pagos electrónicos y llaves electrónicas para control de entrada y salida de edificios u oficinas. (Pastorino, 2018).

Para leer correctamente la información registrada en una etiqueta RFID, el lector necesita saber cómo se registra la información y qué protocolo se utiliza para extraer la información.. (Pastorino, 2018).

Según (Pastorino, 2018) En cuanto a cómo leerlos, existen principalmente dos tipos de chips RFID, clasificados por la antena que tiene y la radiofrecuencia utilizada:

Los primeros chips de baja frecuencia del mercado (normalmente 125Khz) tenían un alcance menor de 2 a 30 cm, dependiendo del lector RFID. Leen más lento que las frecuencias altas, pero son menos sensibles al ruido. Pueden almacenar hasta 1 KB de información y son los más

económicos y fáciles de implementar. Si bien la corta distancia hace que leer (o copiar) una clave sea casi necesario para leer (o copiar) una clave, estas claves generalmente son menos seguras porque la información no se puede cifrar. Algunos de los protocolos más comunes utilizados para estas llaves incluyen: EM4100, HID Proximity e Indala, entre otros.

Las **frecuencias** de funcionamiento típicas son 125 kHz y 132 KHz. Las etiquetas de **baja frecuencia** son generalmente etiquetas pasivas que obtienen energía de la radiación cerca del campo de la bobina de acoplamiento del lector mediante acoplamiento inductivo. (Mora, 2020).

Por otro lado, los chips de alta frecuencia (normalmente 13,56 Mhz) son más flexibles y tienen un rango más amplio, de 10 cm a 1 m, aunque esto los hace más sensibles al ruido. También pueden almacenar más información, como huellas dactilares o datos para diferentes aplicaciones, y enviarla más rápido. Esto significa que la etiqueta puede contener datos encriptados que solo pueden interpretarse cuando se conoce la clave. Como resultado, estas etiquetas son más seguras y más difíciles de copiar. Algunas de las marcas más populares son Mifare, Mifare Plus, Classic o Desfire, etc.

Posibilidad de clonar una llave electrónica

Cuando se trata de seguridad, nada es 100% seguro y las posibilidades de vacilación siempre son escasas. La dificultad es el tipo de protocolo que implementa la clave, el método de cifrado y, por supuesto, si la clave tiene algún mecanismo anti-intrusión. Fuerza bruta. Esta combinación de

características es muy importante a la hora de elegir una cerradura electrónica o electromagnética con cerradura RFID. (Pastorino, 2018).

Si desea ver qué tan transparente es su llave electrónica, ya sea un pase de casa, un casillero de gimnasio o un pase de tránsito, necesitará una tarjeta Proxmark III. Este dispositivo de código abierto basado en un chip Arduino y dos antenas (alta y baja frecuencia) se considera la navaja suiza para pruebas de chips y lectores RFID. Además, puede leer, copiar, clonar y emular casi cualquier etiqueta RFID. Además, al ser de código abierto, podemos encontrar diferentes módulos y versiones para cada situación y preferencia. (Pastorino, 2018).

Un chips arduino, no es más que una placa de micro controlador basada en múltiples microchips que almacena datos o historia relativas a las conversiones de códigos descifrados.

MARCO METODOLOGICO

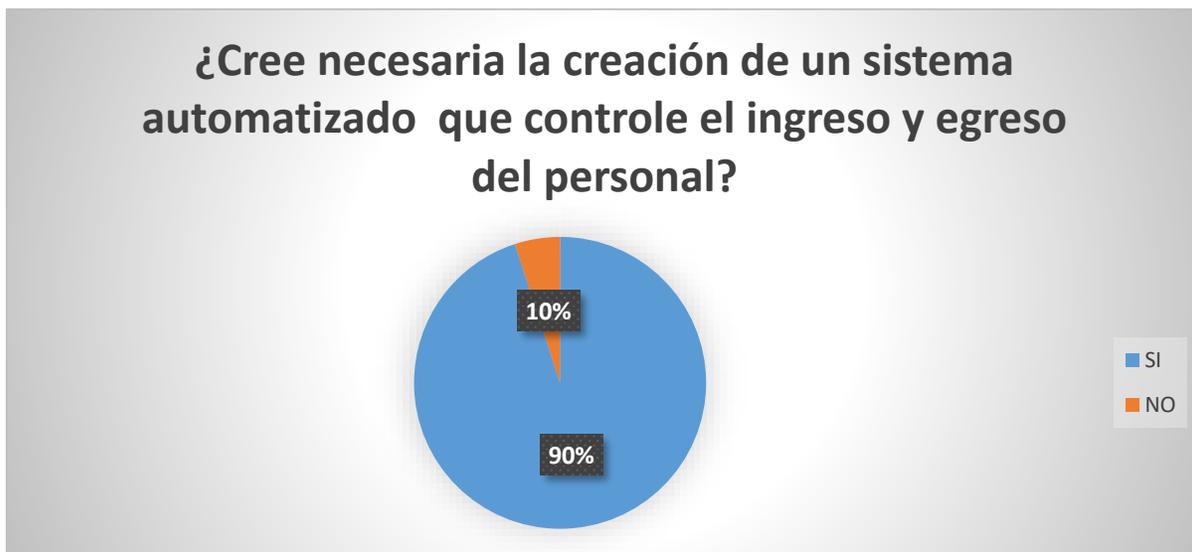
En este caso de estudio se ha utilizado el método analítico ya que se analiza la forma de implementar un sistema de acceso al personal administrativo de la universidad técnica de Babahoyo utilizando muchos sitios web, libros, revistas etc.

También se emplea el método investigativo porque para realizar el proyecto de investigación se necesita descubrir más a fondo la situación del lugar donde se aplica el sistema y más allá de las nuevas tecnologías para plasmar en nuestro sistema de acceso.

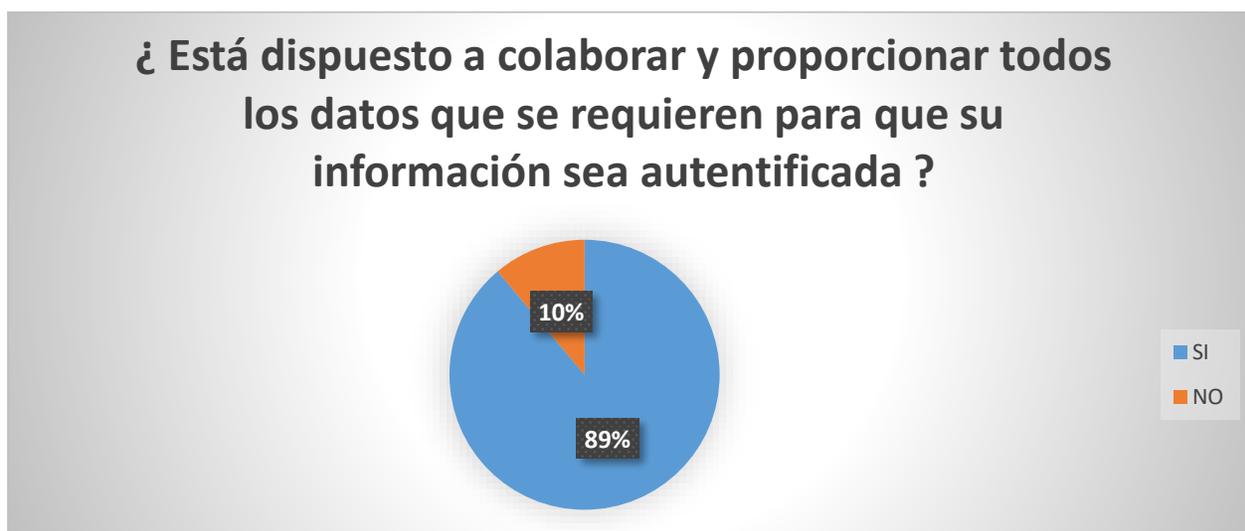
Fue realizada la técnica del muestreo, tomando el 100% del personal administrativo y sacando el 30% para realizar varias preguntas

Realizamos una básica y ligera encuesta a una muestra del personal administrativo que está ubicado en la matriz de la Universidad Técnica de Babahoyo.

Encuesta



De acuerdo a la encuesta realizada se obtuvo que un 90% considera que es necesario crear un sistema automatizado que controle el ingreso y egreso del personal, mientras que un 10% considera que no es necesario.



De acuerdo a la encuesta realizada se obtuvo que un 89% está dispuesto a colaborar y proporcionar todos los datos que se requieren para la información sea autenticada, mientras que un 10 % considera que no es necesario

¿Está usted de acuerdo con la aplicación de un nuevo sistema de control de acceso?



De acuerdo a la encuesta realizada se obtuvo que un 89% está de acuerdo con la aplicación de un nuevo sistema de control de acceso, mientras que el 10% considera que no es necesario.

¿Se debería crear un programa informático donde los guardias puedan corroborar la información del personal que ingresa?



De acuerdo a la encuesta realizada se obtuvo que un 89% está de que se debería crear un programa informático donde los guardias puedan corroborar la información del personal que ingresa, mientras que un 10% considera que no es necesario.

RESULTADOS

En este caso de estudio ANALISIS Y DISEÑO DE UN SISTEMA QUE PERMITA EL CONTROL DE ACCESO AL PERSONAL ADMINISTRATIVO UBICADO EN LA MATRIZ DE LA UNIVERSIDAD TECNICA DE BABAHOYO, UTILIZANDO TECNOLOGIA RFID.

Se ha obtenido considerable información sobre la Universidad Técnica de Babahoyo como institución, sobre su personal y formas o técnicas de llevar el control utilizando una encuesta muy básica que se realizó al 100% del personal administrativo de la institución. Por medio de los resultados de dicha encuesta e incluyendo varias consideraciones de estudiantes al azar se logra implementar dicho sistema de control de acceso utilizando reconocimiento biométrico con tecnología rfid.

DISCUSIÓN DE RESULTADOS

La universidad técnica de Babahoyo en el área de la matriz, donde está ubicado el personal administrativo contaba con un convencional y obsoleto control manual de acceso, con el cual no se lograba el control total de ingreso y egreso de personas y se infiltraban personas no autorizadas en dicha área.

Es de mucho beneficio para la institución la adquisición de este moderno y automático sistema ya que facilita controlar de manera muy estricta el acceso solamente de personas autorizadas evitando la mala manipulación de documentos muy importantes que reposan en el lugar. Utilizando un reloj biométrico que realiza reconocimiento facial, de huellas dactilares, iris de los ojos y también tiene acceso mediante un tag o un chip arduino, ya que, el aparato es completo y cuenta con todas las funciones mencionadas según su configuración.

Gran parte del personal administrativo consideran de vital importancia el diseño e implementación de este sistema que permite restringir el acceso a las personas que no cumplen ninguna función dentro de las instalaciones donde desempeña el área administrativa de la matriz de la universidad técnica de Babahoyo.

El sistema actual o herramienta manual no cuenta con la seguridad necesaria respecto a la autenticidad de las personas que ingresan o egresan del lugar al momento de registrarse, lo cual causa duda en la veracidad y molestias al momento de la intrusión de sujetos que se incluyen con fines diferentes a laborar en el lugar.

Es necesario utilizar nuevas tecnologías para cumplir con los objetivos propuestos en este caso la muy avanzada y eficiente tecnología rfid basada en el reconocimiento por radio frecuencias donde podemos utilizar varios códigos que es capaz de descifrar sin ningún inconveniente.

De manera verbal el personal administrativo que se encuentra ubicado en la matriz de la universidad técnica de Babahoyo ha corroborado que es de mucha importancia contar con un sistema como el antes expuesto.

Por último y no menos importante la implementación del sistema que hemos analizado y diseñado llevara a un gran nivel de prestigio tecnológico a la entidad que lo ha tomado como recurso de control de acceso al personal.

COSTO VARIABLE UNITARIO POR PRODUCTO	
DESCRIPCION	VALOR
Tag	\$ 1,00
chip arduino	\$ 4,50
tecnologia Rfid	\$ 25,00
lector de codigo de barra	\$ 20,00
cintas maganeticas	\$ 18,00
arduino pic Avr ky-037	\$ 2,39
sensor de presión	\$ 55,00
COSTO TOTAL	\$ 125,89

TABLA 1. COSTO VARIABLE UNITARIO

PRODUCCIÓN SEMANAL	Semana
biometricos de seguridad	50

TABLA 2. PRODUCCION SEMANAL

PRODUCCIÓN MENSUAL	Mes
biometricos de seguridad	200

TABLA 3. PRODUCCION MENSUAL

PRODUCCIÓN ANUAL	2022	2023	2024
biometricos de seguridad	2.400,00	2.760,00	3.312,00

TABLA 4. PRODUCCION ANUAL

		2022	2023	2024
COSTO DE PRODUCCIÓN EN DOLARES	COSTO UNITARIO	COSTO VARIABLE	COSTO VARIABLE	COSTO VARIABLE
biometricos de seguridad	125,890	302.136	347.456	416.948

TABLA 5. COSTO DE PRODUCCION

$$\text{RELACION BENEFICIO COSTO} = \frac{125,89}{302,136}$$

$$\text{RELACION BENEFICIO COSTO} = \frac{12.125,89}{26.282,50}$$

RELACION BENEFICIO COSTO =	0,46
-----------------------------------	-------------

CONCLUSIONES

- Se pudo detectar el método que lleva a tomar el control del ingreso al personal administrativo en la organización, el cual no ofrece la estabilidad elemental del caso.
- Se identificó la incidencia entre el sistema manual y el automatizado mediante la tecnología rfid.
- Se analizó un sistema automático que permite controlar el acceso de las personas autorizadas por medio de un aparato biométrico y con actuales tecnologías.

RECOMENDACIONES

- Ejecutar el sistema automático diseñado para el control de acceso del personal administrativo ubicado en la matriz de la universidad técnica de Babahoyo, ya que, será de gran ayuda para las autoridades de la entidad.
- Es preciso facultar e instruir al personal administrativo sobre el uso idóneo del sistema de control las veces que sea necesario para aportar facilidad a la manipulación, aplicación y registro del sistema.
- Aprovechar de manera óptima los recursos humanos, económicos y tecnológicos de la universidad utilizando la información recolectada para brindar un servicio de calidad a la comunidad.

REFERENCIAS

Angamarca, P. W. (julio de 2009). Ecuador: theme by cineca.

CARRION, N. A. (2016). Bogotá, Colombia.

CHAVEZ, W. M. (2018). JIPIJAPA &MANTA, MANABI, ECUADOR.

CHESKYW. (s.f.). empresa internacional: tecnoseguros.

CUCORENT. (2009). Madrid: empresa de soluciones informaticas.

Mora, J. A. (2020).

Paredes, W. C. (s.f.).

Pastorino, C. (mayo de 2018). iferencia entre cerradura electrónica y cerradura electromagnética.

QUIMIS, M. G. (2020). Jipijapa, Manabi, Ecuador.

region, r. i. (s.f.).

RODRIGUEZ, R. M. (2020). MADRID, ESPAÑA.

Sanchez, J. A. (2008). Perú: Revista de Investigación de Sistemas e Informática.

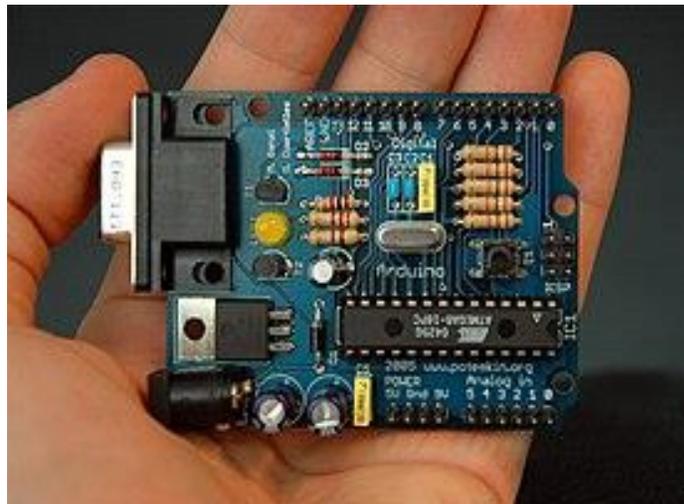
Veronica, V. V. (2013). GUAYAQUIL, GUAYAS, ECUADOR.

ANEXOS

Figura 1 Tags

Fuente: Open Tag Manager

Figura 2 Chips Arduino



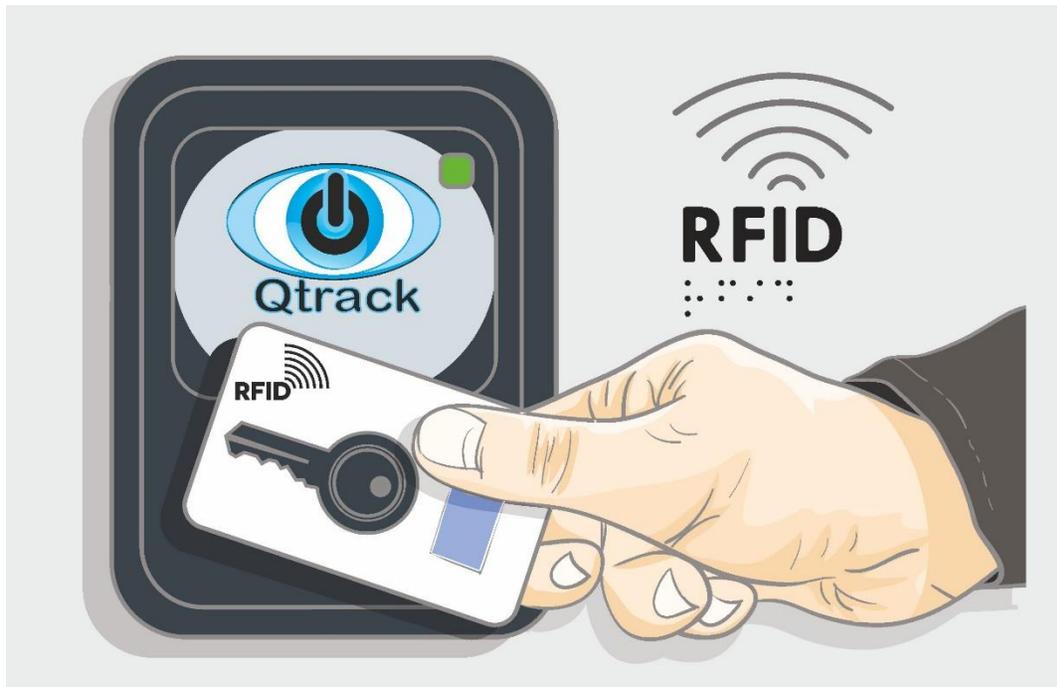
Fuente: arduino Uno Chips

Figura 3 Llave electrónica



Fuente: CALYPSOKEY

Figura 4 Tecnología Rfid



Fuente: Qtrack

Figura 5 Lector de código de barras



Fuente: sincable.sm

Figura 6 Cintas Mágneticas



Fuente: sites.google.com