UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXÁMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

TEMA:

NIVEL DE EFICIENCIA DE LOS LECTORES BIOMETRICOS DE LOS DEPARTAMENTOS DEL GAD MUNICIPAL DEL CANTON BABA

EGRESADO:

JHONN ALBERTO ZURITA BAJAÑA

TUTOR: Ing. NARCISA MARIA CRESPO TORRES, MSc

AÑO - 2019

Introducción

La gestión administrativa del cantón Baba se rige por las disposiciones emanadas por el Código de Organización Territorial, Autonomía y Descentralización COOTAD, y en lo que respecta al personal que labora el artículo 354 indica: Los servidores públicos de cada gobierno autónomo descentralizado se regirán por el marco general que establezca la ley que regule el servicio público y su propia normativa. En ejercicio de su autonomía administrativa, los gobiernos autónomos descentralizados mediante ordenanzas. Podrán regular la administración del talento humano y establecer planes de carrera aplicado a sus propios y particulares realidades locales y financieras.

En lo que respecta de manera específica al talento humano, este se encuentra organizado por categorías de acuerdo a la Ley Orgánica de Servicio Público y su control se realiza por medio de equipos biométricos, este es el mecanismo de seguridad que comprueba el ingreso y salida del personal que labora en las diferentes áreas del Gad Municipal. En el Municipio existen cuatro equipos biométricos dactilares, los cuales no están prestando un servicio eficiente, a pesar de ser un sistema de control del personal que labora, este busca mecanismos para que los mismos no funciones de manera eficiente.

Dentro de los problemas que se detecta por el uso de Biométricos en el Gad de Baba, es que este solo cubre un esquema de integración por medio de la replicación entre las bases de datos, no existe la integración de la información entre los diferentes biométricos que existen en la institución, debido a que su software de control no maneja un API (Interface de Programación de Aplicación) para Java. Requiere de gran cantidad de espacio físico en disco, porque la plantilla que usa para capturar el patrón biométrico tiene gran cantidad de bits.

También presenta dificultades en la portabilidad del dispositivo, debido a que las dimensiones del dispositivo dificultan su transporte (dimensión promedio de 20 x 25 cm). Además, es difícil integración del software con el dispositivo, debido a su complejo manejo de patrones biométricos.

Es compleja la modificación del software para la realización de cambios a nuevos requerimientos, debido a que usa su propio software y no se tiene acceso al código de manera libre. Además existe la dificultad en la transferencia de la información biométrica de la base propia del dispositivo a la base del sistema, debido al tamaño de su plantilla.

También se ha determinado que existen problemas en infraestructura, esto es cableado, socker, los lectores de huellas fallan, no identifican fácilmente, los UPS fallan, siendo uno de motivos las fallas de energía.

Entre otros, estos son los problemas más comunes que se están suscitando en el Gad en lo que respecto a los biométricos, y que amerita la presente investigación.

DESARROLLO

Los sistemas biométricos en la actualidad cumplen una función muy importante en el control del personal y en el proceso de reconocimiento de personas, sobre los cuales se basan las políticas públicas de seguridad. Las autoridades del Municipio del cantón Baba consideran que la biometría es el medio idóneo para identificar a las personas, y por este motivo lo implementaron.

En este estudio se detallan los estándares vigentes de información biométrica, considerando los problemas que se presentan en el Gad Municipal del cantón Baba, También se realiza un estudio de campo sobre un organismo de la administración pública que requiere o debería requerir procesos de identificación seguros.

Considerando que en nuestro medio existen diversas instituciones públicas disponen de sistemas biométricos, es necesario realizar el estudio de análisis de vulnerabilidades y guías de buenas prácticas para minimizar posibles impactos, pérdidas y manipulación de información

Peralta et al., (2014) señalan que la biometría es un sistema de tecnología, basada en reconocimientos de huellas digitales, reconocimientos a través de óptica y en sistema de reconocimiento de voz, que se ha visto implementado en los últimos tiempos como medida de seguridad y a su vez como registro óptimo de personas, animales y objetos. (Rosado Cusme).

Borghello en una investigación indica que: La utilización de la huella dactilar como mecanismo de identificación de las personas, es el método biométrico más utilizado en nuestro medio como forma de controlar en las organizaciones los ingresos y egresos del personal que labora.

Así mismo, aclara que este mecanismo tiene una utilización de más de un siglo, primeramente de manera manual y en la actualidad de forma automatizada (biometría) . Este sistema de control lo utilizan las instituciones públicas y también las organizaciones privadas, es una forma cómoda para el personal de registrar

sus ingresos y egresos a sus actividades laborales, además es el sistema más económico, por la tecnología que utiliza.

El conocimiento de uso de los dispositivos y su configuración es una parte fundamental para un buen funcionamiento de los sistemas biométricos, los mismos que disponen de procesos complejos en el cual se relacionan los mecanismos psicofisiológicos con el aspecto intelectual de la comprensión, puesto que se trata del reconocimiento de características.

Los relojes biométricos a nivel mundial cada día van adquiriendo nuevas tecnologías como el reconocimiento de voz y rasgos faciales, por este motivo las empresas deberán estar preparadas y predispuestas a la utilización de estos dispositivos para el control de personal.

Algunos de los principales problemas de los relojes biométricos es la incertidumbre de vulnerabilidades, la disponibilidad de la información de las marcaciones, la falta de seguridad de acceso con los relojes, entre otros por lo que existe la necesidad de disponer de una guía para la utilización correcta del software del reloj y la manipulación de la información, él mismo que ayudará a realizar un estudio exhaustivo de las políticas de seguridad así como mejorara los procesos y por ende la calidad de servicios.

El fácil acceso a los relojes biométricos puede provocar alteraciones, manipulaciones y daños, los mismos como pueden ser lógicos y físicos causando incertidumbre a los administradores y a los empleados por no contar con una información adecuada de los registros y disponibilidad del reloj biométrico.

Considerando que el reloj biométrico almacena temporalmente los registros, la mayoría de los sistemas biométricos disponen de una base de datos centralizada en un computador personal, que puede ser manipulada fácilmente si no se cuenta con un adecuado control de acceso.

La falencia del análisis de vulnerabilidades de los relojes biométricos podría provocar la manipulación de los registros y presentar datos falsos en los ingresos

y salidas del personal, causando molestias ante el personal y posibles pérdidas económicas.

La nueva tecnología que se utiliza en el reconocimiento de características de las personas denominado biometría, se ha realizado en base a una comprobación científica de que una persona tiene características distintas a otras. Esta identificación biométrica mide a una persona digitalmente sus rasgos.

La tecnología biométrica en la actualidad se utiliza como una medida de ciberseguridad, esta gestión es automatizada y tienen procesos de reconocimientos variados, pero en el caso de esta investigación esta aplicada al control de persona de una institución pública, que brinda servicio a la comunidad.

Los aspectos básicos que protege la biometría son:

- Secreto de la información
- Protección de bienes
- Proceso de identificación
- Medidas de prevención
- Identificación de individuos
- Reducción de costos

En el Gad Municipal de Baba existen cuatro biométricos, los cuales están situados en el Edificio de la administración municipal, en el Auditorio, la Biblioteca, Biblioteca y campamento, los mayores problemas que presentan estos equipos, tiene que ver con el cableado y con los sockets, los cuales se encuentran en malas condiciones por falta de mantenimiento, esto está provocando datos erróneos sobre la hora de marcada de ingresos y egresos del personal.

Foto 1: Biométrico Gad Baba
Tomada por: Jhonn Zurita

Estos biométricos se encuentran a la intemperie, además al tener problemas de socket están inestables, a esto hay que agregar la luz y la vibración produce errores en el control del personal. Los terminales biométricos que se utilizan en el Gad de Baba con compatibles y por este hecho usan el software Bio Time 7.0.

Dentro de las causas del deterioro de los equipos, también se debe indicar que la energía eléctrica no está fija, esta tiene constantes variaciones, y los equipos no están protegidos con UPS, además hay problemas con los enlaces entre las diferentes unidades de biométricos con el computador central que genera la información de control del personal que labora en esta institución pública.

La conectividad de los equipos es una de las causas que originan los problemas de conectividad, esto se origina por la mala calidad de las instalaciones y porque las mismas están en lugares no adecuadas.

Foto 2: Red conexión biométrico Gad Baba y cableado sobre un techo
Tomada por. Jhonn Zurita

Como se puede observar la red está a la intemperie en un techo, al estar la conectividad sin protección alguna, la misma se deteriora y produce fallas en la información recabada por los biométricos.

Los sistemas biométricos en el Gad Municipal de Baba, está permitiendo corregir deficiencias que se tienen en los registros de información de cada empleado, de manera específica como auxiliar en el control de entrada y salida del personal que labora en esta institución.

Se ha determinado que el patrón biométrico de las personas que trabajan en el Gad Municipal se almacena en tarjetas magnéticas, no existe una base de datos centralizada, es decir no hay conectividad entre los cuatro biométricos existentes.

Los biométricos se sincronizan entre sí en la función de introducción de texto y símbolos, pero es necesario un servidor que pueda sincronizar hasta con 500

dispositivos para que sea eficiente, esto no está sucediendo en el Gad de Baba, por lo cual la migración de datos no es efectiva, cada biométrico tiene conexión a una computadora, pero estos no están conectados entre sí.

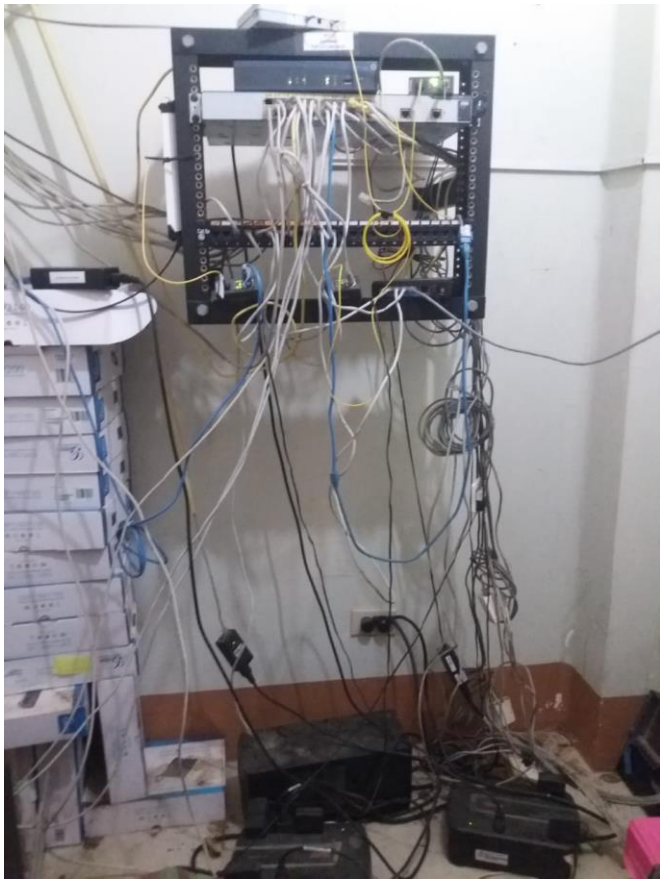

Foto 3: Socket de Red Biométrico Gad Baba ubicado en administración central
Tomada por. Jhonn Zurita

Además, la fibra óptica se encuentra sin seguridad alguna, la misma no está fijada a la pared, lo cual trae un deterioro a corto plazo, y problemas de conectividad.

También una problemática no tecnológica que se está originando en esta institución pública con el uso de los biométricos, es la manipulación manual, donde se considera:

1. No están los empleados registrados adecuadamente, esto es la asistencia en base a un calendario de labores prediseñado.

2. Muchas veces los empleados no tienen asignado un calendario temporal, el biométrico aquí calcula de forma diferente, esto provoca información no real.

3. En ocasiones el horario asignado a un empleado, no tiene rangos de tiempo válidos para la entrada y salida.

Al no estar conectados los computadores de cada uno de los biométricos, no existe eficiencia en el control; esto no lo hacen porque la señal de internet contratada por el Gad no es buena, presenta muchas fallas.

También se indicó que no existe estabilidad en el servicio de energía eléctrica, siempre hay apagones lo cual provoca errores, ya que “después de un apagón eléctrico los dispositivos no se conectan a Biotime 7.0 automáticamente” (Evangelista, 2018). Este error se produce porque muchas veces esta activada la función DHCP en las configuraciones de Ethernet, porque el lector biométrico asigna de manera automática una IP del router, antes de que se reanude la conexión a internet, en este caso necesariamente debe reiniciarse el equipo.

En ocasiones el sistema deja de funcionar, en estos casos se procede de la siguiente manera:

1. Se revisa que los servicios se encuentren activos y corriendo en la herramienta Bio Time 7.0

2. Se revisa la conexión de la base de datos

3. Se verifica si ha ocurrido un cambio en la autenticación, ubicación o puerto de la base de datos, si esto ocurre hay que actualizar los datos.

Cuando los equipos biométricos están sin conexión no envían la información adecuada al equipo informático (marcaciones, información de usuarios y/o huellas), esta información permanece en el reloj biométrico, siempre y cuando su memoria interna lo permita, caso contrario se está perdiendo información, en este caso la información guardada se la importante por medio de USB.

Los problemas indicados, se presentan en el siguiente mapa de problemas:

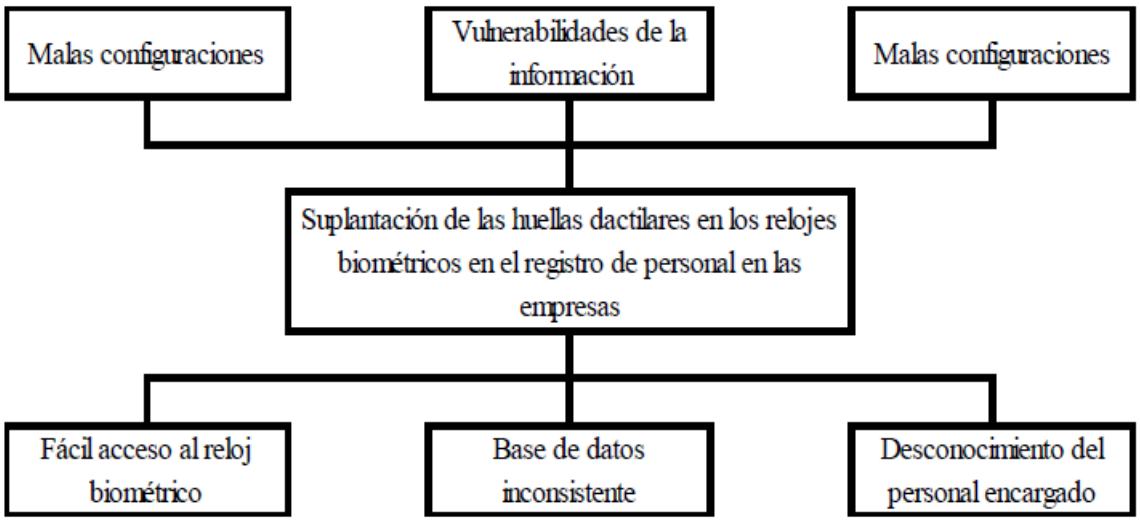

Grafico 1: Guía de problema central y derivados

Realizado por. Jhonn Zurita

Cuando el equipo deja de funcionar por problemas de electricidad, lo cual ocurre a menudo, se realiza la reconexión de la plataforma del equipo, el cual funciona con la versión ZEM, con una pantalla inicial fácilmente identificable por su interfaz. (Anexo 1)

Por lo general el proceso para reconectar el equipo biométrico lo único que se hace es reiniciarlo, para lo cual se procede de la siguiente manera:

El equipo biométrico del Gad municipal es el modelo LP400, que para prenderlo solo se debe hacer presión sobre el botón “0” (Anexo 2), para lo cual debe presionarse este botón por un lapso de cinco segundos.

Cuando el equipo no quiere reiniciarse, significa que se ha bloqueado, en este caso debe ingresarse como administrador al menú del biométrico para cambiar la configuración. Este es un problema que siempre se origina cuando existen apagones, sobre todo esto ocurre en la etapa invernal.

Por medio de la investigación se determina que existen falencias en el uso de los biométricos, se está manipulando los registros y se presenta información falsa a la autoridad para evitar ser sancionado por los egresos tardíos o las tempranas salidas del personal.

En lo que respecta a la seguridad informática vinculado a los biométricos, existe deficiencia en los protocolos, reglas, métodos y herramientas para evitar los riesgos de producir una información falsa, como está ocurriendo en la actualidad. Por este motivo no hay una seguridad informática adecuada sobre el software, base de datos, metadatos y archivos.

“Los sistemas biométricos, a pesar de su aparente alto nivel de seguridad para los usuarios, presentan un elevado número de puntos en los que pueden ser atacados. Recientemente, ante la proliferación de los sistemas de reconocimiento biométrico en aplicaciones de autenticación para dispositivos electrónicos y control de acceso, su seguridad ha cobrado gran relevancia” (Fonseca, 2013)

Además de los problemas de conectividad, de los biométricos que son objeto de estudio son vulnerables, presumiéndose por medio de falsificación de huellas dactilares de los usuarios de este equipo, esto se cree que está ocurriendo porque no existe medidas de precaución, como la utilización de cámaras de seguridad que permita vigilar los registros de la huella digital por parte de los empleados, dentro de las consideraciones para no utilizar esta medida de control es el aumento de costos parta la institución, la cual tiene un presupuesto reducido, donde el 80% va destinado a gastos corrientes (Sueldos, suministros).

También se ha considerado que muchas personas que manejan estos equipos de control pueden borrar la información que guarda la memoria interna del biométrico, esto se lo puede hacer por medio de la utilización del software Attendance Management, lo cual es de uso popular, porque en esta ciudad hay muchas personas que tienen conocimientos avanzados de informático. Cuando está

instalada esta aplicación se puede determinar por medio de la pantalla principal, así:

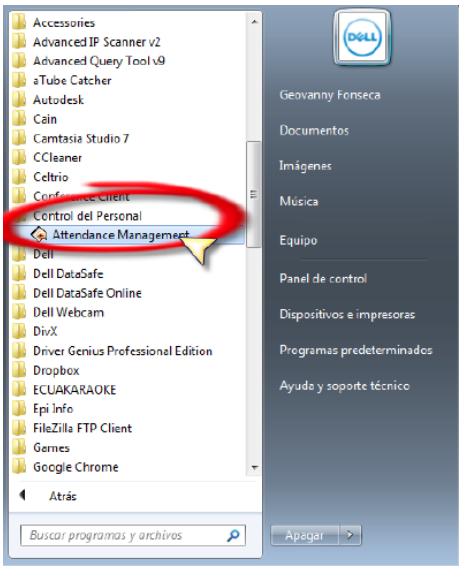

Foto 4: Pantalla Computador Gad Baba
Tomada por. Jhonn Zurita

Con esto:

“1. Restaurar el dispositivo. - Existe la disponibilidad del sistema para restaurar al punto de partida del biométrico, esto es reiniciar el equipo como cuando se lo fabrico, dejar su memoria en blanco lista para iniciar como la primera vez.

2. Modificar firmware. - Existe la libertad de modificar el firmware, o también de cambiarlo, configurando el dispositivo dentro de esta opción.

3. Dispositivo inicial.- Como existe la posibilidad de configurar el reloj biométrico, esta opción deja en libertad de borra toda la información y reprogramas con nuevos usuarios, huellas dactilares y se reinicia como si recién se lo va a utilizar después de fábrica.

4. Capturar imagen. - En el caso del biométrico del Gad de Baba, no tiene la opción de capturar una imagen vinculando al computador.

5. Dispositivo apagado. - En esta opción el software da una orden de apagado al reloj biométrico.

6. Limpiar privilegios de administradores. - Antes de dar clic en limpiar privilegios del administrador revisamos el reloj biométrico lo que está bloqueado y solo el administrador del dispositivo puede acceder a la información" (Fonseca, 2013).

El sistema biométrico es un sistema repetible, es decir que tiene una característica de captar una información y que a futuro puede identificar la misma cada vez que el individuo registre en el equipo biométrico una característica que puede ser la huella digital el iris de la vista o el rostro de una persona.

Es importante indicar que a pesar de las personas tener características aparentemente iguales, existen ciertas diferencias entre los individuos, estas diferencias son captadas de manera exacta por los equipos biométricos, el medio de captar son sensores que identifican un componente especifico del comportamiento físico del ser humano.

2. Transmisión

"Algunos, pero no todos, los sistemas biométricos recogen datos en una localización, pero se almacenan y/o procesan en otra. Tales sistemas requieren la transmisión de datos. Si está implicada una gran cantidad de datos, la compresión es fundamental, a fin de requerir poco ancho de banda y poco espacio para su almacenamiento" (Fonseca, 2013).

La transmisión de los datos que identifica el equipo biométrico es comprimida en una base de datos y su capacidad de memoria es la que permite almacenar la información del número de usuarios para realizar un registro adecuado en base al reconocimiento de características especiales que diferencian a una persona de otra.

3. Procesado de la señal

La señal captada por el biométrico es transmitida a la memoria, este proceso se realiza en base a las tareas automatizadas de extracción de la información. Control de la calidad de la misma y relación o concordancia de la identificación del individuo.

Es importante que el biométrico sea ubicado en una parte donde no haya interferencia de la señal, donde el sensor pueda captar de manera eficiente y real la información del usuario del equipo, muchas veces se pierde la señal por ruido o problemas en la trasmisión, como cableado en malas condiciones o suciedad en el equipo.

La finalidad del proceso de relación y concordancia en el desarrollo de modelos, es que actualmente el sistema envía de manera cuantitativa la información para un proceso de comparación y presentación de informes de manera concreta.

Dentro de este proceso las distancias se fijan en cero, siempre se van a producir diferencias que se tiene relación directa con el sensor o esta relacionada en el proceso de transmisión de datos, muchas veces originadas por el propio usuario del biométrico.

Como se ha descrito anteriormente, el biométrico en los actuales momentos es una auxiliar indispensable en las organizaciones modernas. Este sistema es la aplicación de métodos matemáticos y estadísticos que permiten identificar los rasgos físicos de las personas, es decir verifican la identidad de los individuos en base a características diferenciadas.

El proceso de autentificación de identidad de una persona se sustenta en un patrón guardado en una base de datos, a esto se denomina como uno-para-uno. La autentificación biométrica es más veloz que la de identificación biométrica,

cuando la base de datos es pequeña, cuando la base de datos es grande demora mucho más este proceso.

Los sensores son los que permiten recolectar la información, los datos biométricos son medibles considerando que esta información no puede cambiarse, porque ya se indicó anteriormente que todas las personas tienen características individuales, que no se repiten en otras personas.

CONCLUSIONES

De la descripción de los problemas tecnológicos que se origina por el mal uso de los biométricos en el Gad del cantón Baba, se concluye:

Que la utilización de cuatro biométricos en el Gad municipal, no ha traído eficiencia y eficacia en el control del personal que labora en esta institución, porque los mismos se encuentran en condiciones no adecuadas,

No se ha dado el mantenimiento adecuado, esto está originando problemas de conectividad con el equipo informático, además se ha determinado que existen fallas en el sistema eléctrico y que los equipos biométricos no están conectados a UPS, esto no permite registrar de manera exacta los ingresos y egresos del personal. El internet es de mala calidad, esto provoca que no se produzca la conectividad adecuada.

Por la investigación se determina que el manejo de los dispositivos no es adecuado, incluso el soporte tecnológico del software no se aplica de acuerdo a las recomendaciones tecnológicas.

La base de datos del sistema biométrico no cuenta con la seguridad necesaria, esto produce perdida de información de las marcaciones, también se determinar que los equipos no están en red, funcionan de manera independiente.

Los archivos de ejecución del software no tienen seguridad, esto permite manipular las configuraciones internas del programa.

Bibliografía

Aguilar, E; Dávila, D.2013. Análisis, diseño e implementación de la aplicación web para el manejo del distributivo de la facultad de ingeniería. Tesis. Ing. Sistemas. Universidad de Cuenca. Cuenca,

Cedeño Juan (2017). Sistema biométrico de control de acceso para el laboratorio de cómputo de la unidad educativa Francisco González Álava.

Cacuango, W; Arteaga, M; Guzmán, S. 2014. Lector de huellas digitales. En línea. Formato HTML. Consultado el 22 de noviembre de 2015. Disponible en: https://prezi.com/y6-bsfoforef/lector-de-huellas-digitales/

Evangelista, A. (2018). *tecnosinergia.zendesk.com.* Recuperado el 2019

Fonseca, G. (2013). *VULNERABILIDADES DE LOS RELOJES BIOMÉTRICOS.* Ambato: Universidad Tecnica de Ambato.

Hernández, A. 2016. Reconocimiento facial y dactilar. En línea. Formato HTML. Consultado el 22 de noviembre de 2016. Disponible en: https://prezi.com/ohnjexvdppb4/reconocimiento-facial-y-dactilar/

Lugo, O; Villavicencio, G; Díaz, S. 2014. Paquete tecnológico para el monitoreo ambiental en invernaderos con el uso de hardware y software libre. Chapingo, MX. Revista Terra Latinoamericana. Vol. 32. Núm. 1. p 77-84

Rosado Cusme. (s.f.).

Tolosa, C. (2017). *https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia%20/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf.* Recuperado el 2019

Ventura, J. (2015). Introducción al concepto de seguridad. . En línea. Formato HTML. Consultado el 21 de noviembre de 2015. Disponible en http://elordenmundial.com/seguridad/introduccion-al-concepto-de-seguridad/

Anexo 1

Pantalla principal software Biotime 7.0

Equipo del Gad de Vinces

Anexo 2

Pantalla principal software Biotime 7.0

Equipo del Gad de Vinces

Anexo 3

Fotos de Cables de conexión biométrico Gad baba

Tomada por: Jhonn Zurita

Fotos de Cables de conexión biométrico Gad baba

Tomada por: Jhonn Zurita