MONOGRAFÍA DE ESTUDIO SOBRE LA APLICACIÓN DE SEGURIDAD BIOMÉTRICA PARA LA IDENTIFICACIÓN DE USUARIOS EN ENTORNOS WEB

NEVARDO ALONSO AYALA ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TUNJA

2015

MONOGRAFÍA DE ESTUDIO SOBRE LA APLICACIÓN DE SEGURIDAD BIOMÉTRICA PARA LA IDENTIFICACIÓN DE USUARIOS EN ENTORNOS WEB

NEVARDO ALONSO AYALA ROJAS

Trabajo monográfico

Presentado como requisito para Optar el Titulo

Especialista en Seguridad Informática

Ing. HENRY FERNANDO RODRÍGUEZ HERNÁNDEZ

Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TUNJA

2015

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

Tunja, xx de Junio del 2015

DEDICATORIA

El presente documento del trabajo realizado se lo dedico a mi Dios todo poderoso quien me ha dado la fortaleza física, mental y espiritual para desarrollar y culminar de forma satisfactoria esta etapa de superación personal y formación académica.

AGRADECIMIENTOS

Agradezco a mi Dios por permitirme culminar esta nueva experiencia en mi formación académica y profesional, por darme las facilidades y la satisfacción de culminarla, porque me ayude a lograr el buen aprovechamiento de lo adquirido en la especialización y por sus bendiciones que nunca me ha abandonado.

Sinceros agradecimientos a mis padres José Miguel Ayala Parada (Q.E.P.D.) y Berenice Rojas de Ayala (Q.E.P.D.), por brindarme la vida, inculcarme la responsabilidad y el compromiso de finalizarlo lo iniciado; a mi esposa Martha Liliana Pinto Malaver, por apoyarme y darme la fuerza necesaria para no desfallecer y lograr alcanzar éste triunfo.

Completo agradecimiento al Ing. Henry Fernando Rodríguez Hernández por su guía, asesoramiento y paciencia; a los docentes y tutores, Inmensamente agradecido con el Líder del programa de Especialización en Seguridad Informática el Ing. José Miguel Herrán Suárez, quienes me brindaron su apoyo incondicional, asesoría, acompañamiento y empuje, para llevar a cabo la culminación del presente trabajo.

Ing. Nevardo Alonso Ayala Rojas

CONTENIDO

CONTENIDO DE IMÁGENES

CONTENIDO DE TABLAS

CONTENIDO DE ANEXOS

RESUMEN

Se analizará información sobre los diferentes sistemas de medición biométrica, como uno de los elementos tenidos en cuenta para la creación de aplicaciones en seguridad informática. Abordando el concepto de biometría, que proviene de la raíz griega *“bios”* que significa vida y *“metron”* que significa medida; se estudian los métodos para el reconocimiento de humanos basados en uno o más rasgos físicos intrínsecos.

La UNAD siendo una de las primeras instituciones educativas en ofrecer aprendizaje virtual a nivel nacional, cuenta con un sistema de identificación poco seguro para el ingreso al campus de aprendizaje. La autenticación de acceso a la plataforma de estudio que se utiliza, es la digitación de usuario y contraseña, método que no garantiza la seguridad, facilitando la suplantación en el desarrollo de las actividades académicas propuestas, por lo tanto se sugiere la conveniencia de implementar otro método de seguridad para acceder a la plataforma, procurando de esta manera, mejor eficacia en la identificación de los estudiantes y generando una mayor responsabilidad, ofreciendo como resultado un mejor y más notable rendimiento académico.

La actual propuesta se centra en plantear un modelo de seguridad de acceso a la plataforma, basado en la biometría, que le permita evaluar con certeza la autenticación del aprendiz. Esta tecnología biométrica brinda herramientas eficientes para instaurar diferentes niveles de seguridad, ya sea en la industria, comercio o en la informática.

SUMMARY

Effective biometric information measuring human as considered for creating applications in security elements are analyzed. Addressing the concept of biometrics, it comes from the Greek root "bios" meaning life and "metron" meaning measure; thus we study of automated methods for recognizing humans based on one or more intrinsic physical features.

The UNAD being first educational institutions to offer online learning nationally, has little effective identification system for entrance to campus learning. Entrance authentication platform is fingering study uses username and password, which method does not guarantee security, facilitating impersonation in development of academic activities proposed, so the convenience of implementing other security method is suggested to access platform, thus ensuring better efficiency in identifying students and creating greater accountability, offering best result and remarkable achievement.

The current proposal focuses on raising security model of access platform, based on biometrics, to assess with certainty authentication apprentice. This biometric technology provides efficient tools to establish different levels of security, whether in industry, commerce or in informatics.

INTRODUCCIÓN

El uso de las características físicas y conductuales como herramientas de identificación de individuos, ya se llevaba a cabo en tiempos antiguos. Los egipcios verificaban la identidad de las personas que participaban en las diferentes operaciones comerciales y judiciales. Se sabe que en el siglo XIV en China, los mercaderes estampaban las huellas de la palma de la mano y los pies de los niños en un papel con tinta para distinguir a los unos de los otros.

En el siglo XIX investigadores en criminología intentaron relacionar las características físicas de los individuos con tendencias criminales, por ejemplo, Alphonse Bertillon desarrolló el sistema "Bertillonaje"[1] o antropometría descriptiva, como un método para identificar individuos basado en registros detallados de medidas de su cuerpo. Sin embargo los resultados no eran lo suficientemente confiables, pero aun así la idea de medir las características físicas de un individuo parecía efectiva. De manera paralela comenzó el desarrollo de la identificación por huellas dactilares que muy pronto se convirtió en la metodología internacional para la identificación, debido a que éstas son un rasgo distintivo entre los seres humanos. En 1856, sir William Herschel fue el primero en implantar la huella dactilar como método de identificación en documentos para personas analfabetas.

Ya en el siglo XX de acuerdo a la creciente necesidad de identificación de los individuos el avance se hizo permanente en cuanto al aprovechamiento de las características únicas e irrepetibles de los seres humanos. Es así como en el año 1935 se comenzaron a utilizar otras características físicas como variantes de identificación, por ejemplo el iris del ojo; en este sentido, los oftalmólogos Carleton

[1] http://www.oocities.org/cjr212criminologia/bertillon.htm

Simon e Isodore Goldstein plantearon que los patrones vasculares de la retina son únicos en cada individuo. Después en el año de 1941, Murray Hill de los Laboratorios Bell inició el estudio de la identificación por voz, sus trabajos fueron redefinidos por L.G. Kersta. Más adelante Durante los años 1964 y 1965 Woodrow Wilson Bledsoe, Helen Chan Wolf y Charles Bisson trabajaron en el reconocimiento facial humano haciendo uso de la computadora y desarrollaron el primer sistema semi-automático de reconocimiento.

En los setentas A.J. Goldstein, L.D. Harmon, y A.B. Lesk usaron 22 marcas específicas subjetivas como el color de cabello y grosor de labios para automatizar el reconocimiento facial.

El 25 de Mayo de 1971 se patenta en Estados Unidos un sistema de identificación de la palma de la mano por parte de Norman G. Altman.

Durante la última década la industria de la biometría ha madurado y la investigación de las tecnologías biométricas orientadas al mercado empresarial y de la seguridad comienza a tener un crecimiento aún más significativo. En la actualidad comienzan a aparecer en el mercado aplicaciones a gran escala que serán cada vez más accesibles para empresas y particulares.

Son imperantes las necesidades en cuanto a veracidad de la identificación y el desarrollo de sistemas de seguridad cada vez más incorruptibles, que también resultan en un problema ético en cuanto a la seguridad de la privacidad del individuo, por lo que Ricardo Llopis Nebot anota en su documento ***Sistemas de Autenticación Biométricos***: "*El problema básico en la implantación de los*

métodos biométricos es la aceptación del usuario", ya que para desarrollar las diferentes tecnologías biométricas es necesario reconocer las anormalidades físicas del ser humano y almacenar información personal que evidentemente se hace susceptible de ser mal utilizada.

En Universidad Nacional Abierta y a Distancia – UNAD, por tener la modalidad de aprendizaje virtual, es necesaria la identificación de los miembros de la comunidad como forma de reconocimiento para acceder al campus de estudio. En la actualidad los estudiantes ingresan al sistema con el método tradicional de autenticación, consistente en la digitación de usuario y contraseña asignados a cada uno de ellos, admitiendo que esta información sea entregada a personas que lo suplanten. Estos sistemas tradicionales por su poca efectividad y bajo nivel de seguridad, crean conflictos en protección, control y seguridad informática, debido a su vulnerabilidad de cifrado y por falta de confidencialidad. Debido a esto, se evidencia la necesidad de implementar un nuevo método de protección, evitando que tales situaciones de riesgo se presenten. La tecnología actual brinda herramientas eficientes y efectivas, para instaurar diferentes niveles de seguridad en el acceso o autenticación del personal, con autorización del administrador del sistema.

Por tanto, la propuesta de investigación documental que se entrega, evidencia la necesidad de implementar un modelo de seguridad de acceso diferente al existente en la plataforma académica de la UNAD, basado en los aportes tecnológicos de la biometría, para llevar a cabo la identificación de individuos según sus características físicas, logrando mayor certeza y efectividad en la autenticación; evaluando y evidenciando sus fortalezas y debilidades, evitando de esta forma la suplantación del estudiante.

1. DEFINICIÓN DEL PROBLEMA

1.1. DESCRIPCIÓN

Al indagar sobre la seguridad del acceso a la plataforma, se encuentra que para verificar la identidad de la persona que accede, la única forma de reconocimiento, es la digitación de usuario y contraseña, información que es suministrada por el administrador del sistema una vez matriculado el estudiante; datos que cualquier persona puede conocer; lo que conlleva a que se presente en ocasiones suplantaciones por personas ajenas, quienes ingresan para dar desarrollo a las actividades académicas propuestas en los cursos virtuales, situación que repercute en la calidad de aprendizaje de los estudiantes, en la eficacia de sus profesionales y obviamente en el buen nombre de la universidad. Esta situación permite que se presente un estudio de seguridad, proponiendo la aplicación y descripción de una nueva forma de identificación, obteniendo un mejor control y resultado en cuanto a la autenticación de acceso a las actividades académicas virtuales.

1.2. FORMULACIÓN

¿Las acciones realizadas para fortalecer la seguridad de acceso de personas a la plataforma en la UNAD son suficientes y se cumplen satisfactoriamente?

1.3. JUSTIFICACIÓN

La Universidad Nacional Abierta y a Distancia por tener la modalidad de aprendizaje virtual, ha generado un reglamento de seguridad de acceso a la plataforma, y a las actividades impuestas, como a la información contenida en ella. Inicialmente se ha determinado que para evitar el ingreso al campus desde dos puntos distintos geográficamente, sea corroborada la dirección IP de los equipos

que ingresan y se encuentren conectados a la red para el desarrollo de actividades en línea que debe entregar el estudiante, en cuanto a la seguridad y privacidad de la información se utiliza el reglamento vigente.

La institución como ente de aprendizaje autónomo y consciente del riesgo que significa manejar la información en la nube generó un reglamento, donde se dan a conocer sus artículos más pertinentes en cuanto a las políticas de seguridad instauradas en la universidad.

Estos son:

Articulo 1. *"Política General de Seguridad de la Información. Proteger, preservar y administrar, la confidencialidad e integridad de la información de la Universidad Nacional Abierta y a Distancia - UNAD, salvaguardando la precisión y la completitud de la misma, minimizando los riesgos asociados de daño y asegurando el eficiente cumplimiento de las funciones sustantivas de la entidad apoyada en la confidencialidad, integridad y disponibilidad de la información*.[2]

Articulo 2. *Ámbito de Aplicación. Esta política aplica a todos los procesos y procedimientos que conforma el Sistema de Gestión de la Calidad de la Universidad, así como a todas las actuaciones administrativas que desarrollen sus distintas unidades, por intermedio de sus funcionarios administrativos, cuerpo docente o contratistas.*

Articulo 3. *Definiciones. Para efectos de la aplicación de la siguiente resolución, se adoptan las siguientes definiciones:*

> *a. Activos de Información: Cualquier componente (humano, tecnológico, software, manuales, documentación, entre otras) que tiene Valor para la organización y signifique riesgo si llega a manos de personas externas.*

[2] Resolución N° 004793 del 22 de Agosto del 2013 - Por la cual se crea la Política de Seguridad de la Información para la Universidad Nacional Abierta y a Distancia - WAD

b. Activo tecnológico: Equipo, maquinaria, herramienta o software, necesario para realizar las actividades productivas especificas de una organización.

c. Base de Datos: Conjunto de datos almacenados y organizados con el fin de facilitar su acceso y recuperación mediante un computador

d. Código fuente: Conjunto de instrucciones escritas en algún lenguaje de programación de computadoras, hechas para ser leídas y transformadas por alguna herramienta de software (compilador, intérprete, ensamblador) en lenguaje de máquina o instrucciones ejecutables en el computador.

e. Correo Electrónico Institucional. Recurso de la institución a disposición de los funcionarios, contratistas, docentes, estudiantes y egresados, el cual permite el envío y recibo de información institucional.

f. Credenciales de usuario: Privilegios de seguridad agrupados bajo un nombre y contraseña, que permiten acceso a los sistemas de información.

g. Custodio: Grupo de funcionarios o unidades organizacionales, designado por los propietarios de la información, los cuales se encargan de mantener las medidas de protección establecidas por los responsables sobre los activos de información. En ocasiones el responsable y el custodio son la misma persona.

h. Data-center o CPD (Centro de Procesamiento de Datos): Edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

i. Dispositivo biométrico: Dispositivo de seguridad utilizada, en sistemas computarizados que sirve para identificar atributos físicos como rasgos faciales, patrones oculares, huellas digitales, la voz y la escritura,

j. información sensible o vulnerable: También llamado activo sensible, es el nombre que recibe la información personal o institucional (datos personales, información financiera, contraseñas de correo electrónico, domicilia, datos de investigaciones), la cual puede ser alterada, descompuesta, mal utilizada, divulgada y/o eliminada, causando graves daños a la organización propietaria.

k. Plan de continuidad del negocio (Business Continuity Plan, BCP): Documento de estudio y aplicación que incluye la identificación y protección de los procesos y recursos del negocio considerados crítico paca sostener un desempeño aceptable, mediante la identificación de potenciales amenazas, la definición de estrategias para su eliminación, minimización o delegación y la preparación de procedimientos para asegurar la subsistencia de los mismos al momento de concretarse dichas amenazas.

l, Redes de Computadores: También llamada red de ordenadores, red de comunicaciones de datos o red informática, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos el6ctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

m. Seguridad física: Todos aquellos mecanismos (generalmente de prevención y detección) destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de copia de seguridad con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.

n. SAN (Storage Area Network) o Red de Área de Almacenamiento: Red de almacenamiento integral. Se trata de una arquitectura completa~ que agrupa los siguientes elementos:

Una red de alta velocidad de canal de fibra o SCSI.

- *Un equipo de interconexión dedicado (conmutadores, puentes, etc.).*

- *Elementos de almacenamiento de red (discos duros).*

o. SGS1 (Sistema de Gestión de Seguridad de la Información) Conjunto de políticas de administración de la información. El término es utilizado principalmente por la ISO/IEC 27001.

p. Seguridad Informática: Proceso de prevenir y detectar el uso no autorizado de los medios informáticos. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar tos posibles riesgos a la infraestructura o a la información.

q. Seguridad de la Información: Son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de tos sistemas tecnológicos que permiten resguardar y proteger la información.

r. Seguridad Perimetral: Corresponde a la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión en instalaciones especialmente sensibles.

Articulo 4. *La política para el manejo de la información tiene como propósito definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida y para asegurar el cumplimiento de regulaciones y leyes aplicables a la Universidad Nacional Abierta y a Distancia.*

Artículo 5. *Esta política aplica a funcionarios administrativos, cuerpo docente, contratistas directos o indirectos y estudiantes de la institución.*

Queda claro que las políticas de seguridad instauradas por la universidad para la protección de la información, activos y bases de datos, es amplia y suficiente, ya que por medio de ellas se está garantizando la confidencialidad, disponibilidad e integridad de la misma.

Al ser aplicadas, cubren en su totalidad los rangos de seguridad de la información, por consiguiente, no se observa la necesidad de la modificación o adición de alguna de éstas, por considerar que la propuesta del nuevo sistema de autenticación ya está siendo amparada bajo dichas políticas.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Analizar y proponer un modelo de seguridad para el acceso a la plataforma virtual de aprendizaje de la UNAD, basados en la biometría, que le permita evaluar la certeza y efectividad de acciones en seguridad de autenticación.

2.2. OBJETIVOS ESPECÍFICOS

Indagar sobre diferentes fuentes de información acerca de la medición biométrica y sus posibles usos, ventajas, desventajas y reconocer las aplicaciones que se han desarrollado para su aplicación.

Presentar un análisis de las posibilidades de implementar ésta seguridad en un entorno de aprendizaje virtual, asegurando la presencia asertiva del auténtico estudiante.

Proponer del estudio realizado, el sistema de seguridad biométrico más adecuado en cuanto a costos y aplicabilidad en plataforma para el reconocimiento del estudiante.

3. MARCO REFERENCIAL

3.1 ANTECEDENTES

Basados en el tema de seguridad biométrica, se encontraron teorías, documentos, aplicaciones y trabajos desarrollados e implementados en diferentes lugares, organizaciones y países, los cuales sientan un precedente del conocimiento en la aplicación de la biometría en lo que tiene que ver con la seguridad, control y riesgos informáticos que brinda una base más efectiva para la presente propuesta, definiendo características propias de lo requerido para su implementación.

Estas son:

3.1.1 SERVICIO DE VERIFICACIÓN BIOMÉTRICA – SVB[3]

En este ejemplo se puede observar que en el Perú se creó una Agenda Digital denominada RENIEC, con el objetivo de permitir que la sociedad peruana pueda acceder a beneficios que brinda el desarrollo de las tecnologías de la información y comunicación, de esta forma, RENIEC se viene desarrollando para el fortalecimiento del Gobierno Electrónico en el Perú, de esta forma se ha implementado el "Servicio de Verificación Biométrica – SVB, de la información, así como proveer una herramienta accesible que garantice la identidad de las personas que realizan transacciones económicas.

El SVB, ha permitido la reducción de los actos delictivos al momento de realizar dichas transacciones lo que brinda un mejor apoyo al Sistema Automático de Identificación de Impresiones Dactilares – AFIS. Hoy en día, el robo de identidad, es el delito con mayor crecimiento mundial. Esto se debe al valor que esa información puede tener, debido al vertiginoso crecimiento del mercado electrónico y las redes sociales.

[3] SERVICIO DE VERIFICACIÓN BIOMÉTRICA – SVB http://www.reniec.gob.pe/portal/pdf/05_svb.pdf

A propósito de esta información podemos encontrar que a pesar de ser una de las últimas técnicas de protección e identificación, la aplicación expuesta cumple con algunas de las necesidades que busca fortalecer y mejorar su seguridad, en lo relacionado con el acceso e identificación de las personas, pero únicamente fue desarrollada e instaurada para la parte gubernamental del Perú, lo que hace que no sea una de las más factibles para el propósito de lo que se desea proponer, para el beneficio en una institución educativa, que garantice la identificación de sus verdaderos estudiantes, encontrándose completamente limitada en su uso.

Otra de las propuestas encontrada es:

3.1.2. SISTEMA BIOMETRICO DE RECONOCIMIENTO DE HUELLAS DIGITALES - SISBIORHED[4]

"*En el sistema "SISBIORHED",* el ingreso de huellas digitales se realizará de forma manual (huellas estáticas), por medio un scanner o dependiendo de la aplicación y recursos de la empresa u organización donde se aplique el sistema con un mouse biométrico.

Mediante comparaciones de patrones de huellas digitales el sistema determinará la identidad de una persona y su información personal básica como nombre, edad, género, mismas que se encontrarán almacenadas en una base de datos.

Los patrones de huellas digitales ingresados se encontrarán en formato .bmp o .jpg y por su tamaño la cantidad ingresada será dependiente de la memoria y recursos del computador donde se pruebe y utilice el sistema, ya que el almacenamiento de imágenes sin un adecuado formato comprimido genera demasiado espacio utilizado. Limitado por no existir en el mercado dispositivos biométricos de bajo costo y con características que permitan una adecuada

[4] SISTEMA BIOMETRICO DE RECONOCIMIENTO DE HUELLAS DIGITALES – SISBIORHED, Autor: María Augusta Melo Sánchez http://repositorio.ute.edu.ec/bitstream/123456789/5673/1/34215_1.pdf

manipulación de las imágenes digitales no se ha podido implementar esta funcionalidad."

En el ejemplo anterior se hace referencia a la identificación por huella dactilar, tema tradicional cuando se trata de la seguridad biométrica, describiendo las dificultades que se presentan en lo relacionado al reconocimiento de las personas en el momento de una transacción bancaria o para la identificación de difuntos, cuando no se ha logrado el adecuado registro. Este sistema les ha aportado la mayor cantidad de información, brindando el nivel de seguridad esperado, lo que hace que se demuestre una vez más, en la necesidad de instaurar un método como la biometría de huellas en algunos sistemas de información. Sin embargo esta aplicación que tampoco ofrece lo deseado para satisfacer las necesidades referidas en una plataforma de aprendizaje, por lo que se continúa con otro ejemplo de aplicaciones que describe estudios que se han desarrollado respecto a la seguridad biométrica.

3.1.3. ESTUDIO SOBRE LAS TECNOLOGÍAS BIOMÉTRICAS APLICADAS A LA SEGURIDAD[5]

"*El estudio es realizado por el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO), la cual es una sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. INTECO es un centro de desarrollo de carácter innovador y de interés público de ámbito nacional que se orienta a la aportación de valor, a la industria y a los usuarios, y a la difusión de las nuevas tecnologías de la información y la comunicación (TIC) en España, su misión consiste en aportar valor e innovación a los ciudadanos, a las PYMES, a las Administraciones Públicas y al sector de las tecnologías de la información, a*

[5] OBSERVATORIO – INTECO – OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN
file:///C:/Users/Nevardo/Downloads/informe_biometria_final.pdf

través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad promoviendo una línea de participación internacional.

El presente estudio surge de la necesidad de conocer el nivel de desarrollo y confianza de las tecnologías biométricas así como su capacidad para afrontar los riesgos existentes y sus futuras líneas de desarrollo. Dentro de este plan de acción se realizan labores de investigación, análisis, estudio, asesoramiento y divulgación que atenderán, entre otras, a las siguientes estrategias:

- *Elaboración de estudios e informes propios en materia de seguridad de las Tecnologías de la Información y la Comunicación, con especial énfasis en la Seguridad en Internet.*
- *Seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la confianza en el ámbito nacional e internacional.*
- *Generación de una base de datos que permita el análisis y evaluación de la seguridad y la confianza con una perspectiva temporal.*
- *Impulso de proyectos de investigación en materia de seguridad TIC.*
- *Difusión de estudios e informes publicados por otras entidades y organismos nacionales e internacionales, así como de información sobre la actualidad nacional y europea en materia de la seguridad y confianza en la Sociedad de la Información.*
- *Asesoramiento a las Administraciones Públicas en materia de seguridad de la información y confianza, así como el apoyo a la elaboración, seguimiento y evaluación de políticas públicas en este ámbito.*"

En este caso se observa una propuesta de estudio del análisis de las diferentes técnicas biométricas existentes en el mercado, sus diversos usos y aplicaciones

desarrolladas. Trata de las posibles amenazas y vulnerabilidades a las que están expuestas. Demostrando que existen formas de ser instaurados para el mejoramiento de seguridad en las instituciones gubernamentales de España, por lo que no es posible ser instaurado en instituciones educativas, pero si como fuente de información en el reconocimiento de lugares donde se han desarrollado estudios de aplicabilidad de sistemas biométricos en sectores públicos como gubernamentales. Situación que enlaza con el siguiente documento indicando como es desarrollado en un país diferente y donde es aplicada la técnica de la biometría para casos judiciales como el siguiente.

3.1.4. RED DE JUSTICIA DE PENNSYLVANIA TENDRÁ TECNOLOGÍA DE RECONOCIMIENTO FACIAL[6]

"La Red de Justicia de Pennsylvania (JNET) junto con su asociado DataWorks implantó un nuevo programa de biometría facial denominado ForensicaGPS, esta servirá de apoyo a las fuerzas policiales para identificar sospechosos o testigos en base a las fotos y videos tomados por cámaras de vigilancia.

El programa ForensicaGPS de Animetrics será incorporado al sistema de reconocimiento facial (JFRS) de JNET, logrando que este sea más ágil y preciso en las investigaciones policiales. Esta aplicación toma imágenes 2D de vigilancia por video o fotografía y las convierte a 3D mediante software de reconocimiento facial patentado por Animetrics. De esa imagen tridimensional, se puede construir una imagen facial de identificación, lo que hace más fácil la confirmación de la identidad cuando se compara con casi tres millones de imágenes que se han acumulado desde 1998 en la base de datos de Pennsylvania", al crear y analizar aún cuando la imagen original esté borrosa o distorsionada hasta cinco imágenes diferentes de un marco bidimensional con mayor precisión en las coincidencias faciales. Actualmente más de 40,000 agentes del orden de Pennsylvania utilizan

[6] http://www.sistemasbiometricos.cl/web/ - agosto 27, último artículo.

JNET para acceder a las bases de datos locales, estatales y federales. Además, 800 agentes de más de 500 departamentos han sido o serán entrenados en el empleo del nuevo JFRS."

Para el caso del artículo anterior, se puede encontrar que el sistema de reconocimiento facial está siendo utilizado por la justicia de Pennsylvania, ya que ha proporcionado la identificación asertiva de diversos sospechosos, lo que permite que la labor policial sea mucho más eficiente y efectiva, demostrando que con la aplicación de estos métodos y técnicas de identificación facial, se logra una mejor capacidad del reconocimiento de individuos en cualquier ámbito, ya sea de tipo judicial, gubernamental o académico, presentando la confianza adecuada en tales procedimientos. Ya sean por distorsión de la imagen que dificulta su identificación, esta es procesada en imágenes fácilmente reconocidas por el sistema demostrando su aplicabilidad, siendo ésta una de las que más se asemeja a la recomendación ideal.

3.1.5. DISEÑO DE UN SISTEMA BIOMÉTRICO DE IDENTIFICACIÓN USANDO SENSORES CAPACITIVOS PARA HUELLAS DACTILARES[7]

"El sistema de reconocimiento biométrico está basado en el procesamiento digital de una imagen de una huella dactilar de 256 x 300 píxeles, la cual se toma por medio de un sensor capacitivo, luego se transmite a un computador (PC) por una interfaz de comunicación obteniendo la imagen para ser almacenada y posteriormente utilizada.

El procesamiento de la huella es realizado por medio de algoritmos de filtrado de imágenes; el primero resalta los valles y crestas de la huella, y se aplica a la imagen por regiones, el siguiente algoritmo se encarga de filtrar la imagen para extraer las características más importantes, luego se lleva la imagen a sólo dos

[7] Diseño de un Sistema Biométrico de identificación usando sensores capacitivos para huellas dactilares - http://www.scielo.org.co/pdf/rfiua/n39/n39a02

niveles de gris, las crestas a un ancho de un solo píxel, y por último el reconocimiento, se hace hallando la ubicación de las características o minucias de cada huella y las distancias entre ellas, generando vectores de información.

Los sistemas de análisis de huellas dactilares pueden ser clasificados en dos categorías:

- *Verificación o autenticación: (Automatic Fingerprint Authentication System - AFAS), consiste en obtener la imagen de la huella dactilar de una persona, de la cual se conoce su identidad, para compararla con la que está almacenada en la base de datos y verificar si la huella dactilar pertenece a esa persona.*
- *Identificación: (Automatic Fingerprint Identification System - AFIS), consiste en conocer solo la imagen de la huella dactilar y compararla con las existentes en la base de datos para hallar la identidad de la persona a la que pertenece esa huella dactilar quien está conformada por crestas y valles, que forman figuras dentro de la imagen de la huella.*

Con el sistema diseñado se pretende desarrollar un sistema de identificación de personas, confiable y seguro, que permita controlar el acceso a lugares restringidos y permita crear la base para el desarrollo de un sistema embebido de identificación portátil y de bajo consumo de energía para su comercialización, la gran importancia y el valor agregado de este diseño radica en el control que se tiene sobre cada una de las etapas del sistema; en los algoritmos propios y mejorados de procesado, análisis y aplicación, lo que posibilita en gran medida futuras modificaciones del sistema."

En el artículo anterior, es posible observar, que la aplicación de esta tecnología se basa gracias a los sensores capacitivos que son los encargados de capturar la imagen de la huella digital, haciendo que se desarrolle esta tecnología para el uso y comercialización, con el fin de popularizarla en sectores que puedan incluirla a sus sistemas de seguridad. Ya sea para el acceso a instalaciones o simplemente para la identificación del personal, o en diversos asuntos que consideren necesarios. Esta situación hace ver, el cómo se viene aplicando la técnica,

apoyándose en los dispositivos como el hardware; el cual está siendo creado por empresas que lo colocan a disposición comercial para su utilización y aprovechamiento. Pero para la recomendación de la técnica pensada, la descrita en el anterior artículo no se ajusta a lo que se pretende presentar, como se describe en el siguiente artículo de la implementación de reconocimiento por captura de imágenes en una plataforma pero por video.

3.1.6. DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA DE SOFTWARE PARA RECONOCIMIENTO FACIAL EN VIDEO[8]

"Este trabajo aborda el reconocimiento facial en video, cuya problemática se ha convertido en los últimos años en un tema altamente recurrente en diversos ámbitos tales como sistemas de seguridad, plataformas de redes sociales, aplicaciones de marketing, etc. También se abordan los avances actuales en reconocimiento de rostro en video, detallando iniciativas privadas y de comunidades abiertas.

El objetivo general planteado corresponde al diseño, implementación y validación de una plataforma de software para el reconocimiento facial en un archivo de video, utilizando métodos ya establecidos y validados en el campo de la biometría, como lo son el algoritmo Haar para detección de rostros y el algoritmo PCA Eigenface para el reconocimiento facial. La problemática de fondo tiene que ver con la utilización de estos algoritmos en un escenario como el de un video, en el cual no necesariamente existe una actitud colaborativa de parte de las personas, aportando gestos, poses y luminosidad muy cambiantes, lo cual dificulta la comparación entre los rostros detectados y el rostro objetivo que se desea identificar.

[8] Diseño e implementación de una plataforma de software para reconocimiento facial en video - Villalon de la Vega, Dario Eduardo - http://repositorio.uchile.cl/handle/2250/112271

El sistema desarrollado se compone principalmente de 4 módulos funcionales: módulo de ingreso de imágenes del rostro objetivo para el entrenamiento del sistema; módulo de ingreso del video a procesar; módulo del proceso de reconocimiento y módulo de entrega de resultados. Adicionalmente se desarrolló un módulo con una herramienta que facilita la generación de la referencia de verdad o Ground Truth para el rostro objetivo en el video de interés, con el fin de evaluar de la efectividad del sistema.

Para la ejecución de pruebas, se seleccionaron tres rostros objetivo a partir de los cuales se construyó una base de imágenes con 100 fotografías por cada rostro las que fueron recolectadas desde Internet. También se seleccionó desde Internet un video de alta resolución para cada rostro. Los resultados de las pruebas son presentados mediante el análisis de curvas ROC y cálculo del índice AUC para cada curva. Las conclusiones obtenidas apuntan a una alta dependencia de la calidad de la información de entrenamiento del sistema para lograr una aceptable capacidad de reconocimiento, que en este caso alcanzo a un 73% en el caso más favorable."

Al realizar el análisis detallado de la lectura anterior, podemos concluir que se han diseñado diversas versiones de las aplicaciones de reconocimiento facial, encontrando la creación de una aplicación basada en video, describiendo la toma de unas 100 imágenes de la misma persona, para ser almacenadas en sus bases de datos, que serán utilizadas en la identificación de ésta misma, comparándola con cualquiera de las posiciones almacenadas en las imágenes que componen el video, demandando un mayor tiempo de respuesta, de almacenamiento por individuo, lo que hace que sea uno de las aplicaciones más dispendiosas y pesadas para el sector de la seguridad informática, debido al tamaño de almacenamiento demandado por las imágenes de cada individuo. Con lo que podemos concluir a manera general que las técnicas de reconocimiento facial desarrolladas en los diferentes sectores, para diferentes tareas, han logrado cumplir y satisfacer algunos de las requerimientos solicitados por el cliente que lo

utiliza, pero no significa que es posible que cumplan con lo que demanda al ser aplicada en una plataforma de aprendizaje, ya que fueron desarrolladas para una tarea específica, en un lugar específico, con restricciones para cada ambiente, situación totalmente diferente a la que se encontrará en un ambiente de aprendizaje virtual, donde debe ser efectiva, eficiente, liviana, aplicable, que se pueda incorporar en una página web, siendo provechada a nivel nacional e internacional sin ocasionar inconvenientes ni traumas en su ejecución, garantizando el libre y seguro acceso del estudiante desde cualquier lugar del mundo a cualquier hora, tal y como se utiliza la autenticación empleada hoy en día en el sistema.

3.2. MARCO CONTEXTUAL

Para comprender un poco mejor el desarrollo del proyecto, en el marco contextual, se nombra algunas de las principales características influyentes en la toma de la decisión para la creación y análisis de la propuesta.

Estas son:

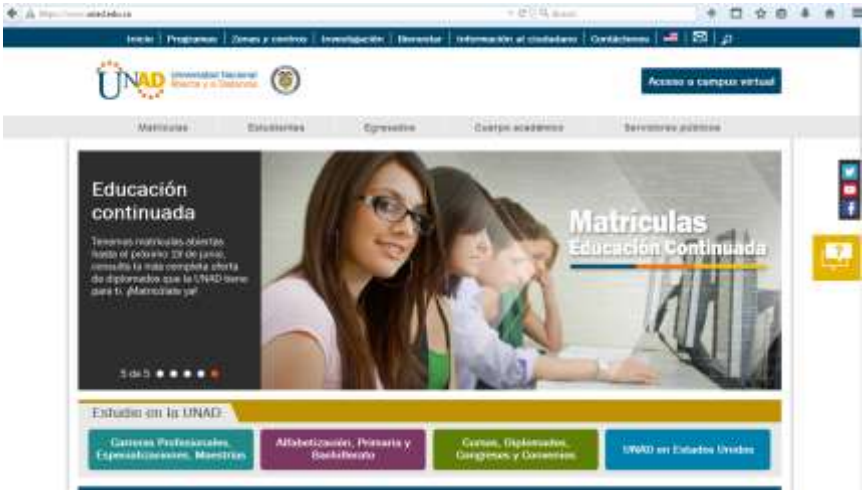
3.2.1. COMPONENTE ORGANIZACIONAL - UNAD[9]

"La institución que hoy se conoce como Universidad Nacional Abierta y a Distancia (UNAD) fue creada mediante la Ley 52 del 7 de julio de 1981 por el Congreso de la República como la Unidad Universitaria del Sur de Bogotá (UNISUR) con el carácter de establecimiento público adscrito al Ministerio de Educación Nacional, con el fin de «Orientar todos sus esfuerzos para responder a las necesidades, intereses y problemas reales del país, especialmente de aquellos que afectan a los sectores populares, marginados de la ciencia, la técnica y la

[9] Proyecto Académico Pedagógico Solidario Versión 3.0, página 22

cultura, lo cual constituye un principio de realidad». (UNISUR, 1983).

Imagen 1: Página principal de la UNAD



Fuente: https://www.unad.edu.co

En el año de 1982 se dispuso que los programas de UNISUR se ofrecieran exclusivamente bajo la modalidad a distancia, lo cual significó para la época una innovación educativa y, a la vez, el cambio de paradigma en algunas instituciones de educación superior, con relación a la orientación de sus esfuerzos hacia la producción de mediaciones pedagógicas y la formación de mediadores, para acompañar el aprendizaje significativo, auto-dirigido, autónomo y colaborativo de los estudiantes en la nueva modalidad. De igual manera, significó la promoción y organización de las comunidades regionales, las cuales entraron en diálogo e interacción dinámica con la nueva institución educativa denominada UNISUR.

3.2.1.1. MISIÓN DE LA UNAD[10]

"La Universidad Nacional Abierta y a Distancia (UNAD) tiene como misión contribuir a la educación para todos a través de la modalidad abierta y a distancia, mediante la investigación, la acción pedagógica, la proyección social y las innovaciones metodológicas y didácticas, con la utilización de las tecnologías de la

[10] Proyecto Académico Pedagógico Solidario Versión 3.0, página 24

información y de la comunicación, para fomentar y acompañar el aprendizaje autónomo, generador de cultura y espíritu emprendedor que en el marco de la sociedad global y del conocimiento propicie el desarrollo económico, social y humano sostenible de las comunidades locales, regionales y globales con calidad, eficiencia y equidad social. (UNAD, Estatuto General. Capítulo 1. Artículo 2)"

3.2.1.2. VISIÓN DE LA UNAD[11]

"La UNAD se proyecta como una Mega universidad líder en Educación Abierta y a Distancia, reconocida a nivel nacional e internacional por la calidad innovadora y pertinencia de sus ofertas y por el compromiso y aporte de su comunidad académica al desarrollo humano sostenible de las comunidades locales y globales, con calidad, eficiencia y equidad social."

3.2.1.3. MODALIDAD DE EDUCACIÓN ABIERTA Y A DISTANCIA[12]

"Para el cumplimiento de sus responsabilidades sustantivas, la Universidad facilitará la utilización de las tecnologías de la información y comunicación en los modelos pedagógicos, adecuadas a las características propias de la Educación Abierta y a Distancia."

3.2.1.4. MODELO PEDAGÓGICO UNADISTA APOYADO EN E-LEARNING[13]

"*El Modelo Pedagógico de la UNAD, (MPU), se fundamenta en unas concepciones específicas de universidad, educación, formación, aprendizaje, currículo, didáctica, contexto de aprendizaje, evaluación, entre otras. En este sentido, incorpora*

[11] Proyecto Académico Pedagógico Solidario Versión 3.0, página 24
[12] Ibid, página 33
[13] Ibid, página 34

elementos propios de los ambientes de aprendizaje y particularmente de los ambientes virtuales de aprendizaje, que reconocen cinco dimensiones estructurarte que viabilizan el proceso educativo del sujeto, lo cual posibilita y favorece la construcción de conocimiento. Así mismo, el MPU se fundamenta en tres tipos de aprendizaje que interactúan y se realimentan con cada una de las actividades académicas que se proponen."

3.2.1.4.1. APRENDIZAJE AUTÓNOMO[14]

"En la modalidad a distancia el aprendizaje autónomo es un elemento clave que determina el alcance del objetivo primordial: aprender a aprender, en este tipo de aprendizaje el estudiante regula, dirige y evalúa su forma de aprender, utilizando estrategias que le permitan no solo aprobar sino contextualizar el conocimiento.

El estudio independiente y autónomo es el fundamento de la formación y del aprendizaje desarrollado con base en el trabajo personal y en pequeños grupos colaborativos. Desde la perspectiva de la EAD que se caracteriza por procesos de aprendizaje individual y grupal, donde el estudiante se convierte en el actor principal de la construcción de su conocimiento y de su progreso, es de vital importancia el aprendizaje autónomo en el sentido de que es el medio para que el individuo logre sus objetivos y metas."

3.2.1.4.2. APRENDIZAJE COLABORATIVO[15]

"El aprendizaje construido desde la perspectiva de lo autónomo, tratado en el aparte anterior, posibilita al estudiante contar con herramientas de toda clase para interactuar con otros en torno a lo construido hasta el momento. Afirmamos que el conocimiento se construye en la interacción y que este es un consenso entre

[14] http://estudios.unad.edu.co/especializacion-en-nutricion-animal-sostenible/metodologia
[15] Opcit, página 40

comunidades, de manera que ningún saber se consolida como tal en un único interlocutor, lo cual abre espacio para una perspectiva dialógica del proceso educativo en el contexto colaborativo."

3.2.1.4.3. APRENDIZAJE SIGNIFICATIVO[16]

"El saber construido debe tener una relación directa con el sujeto, lo cual quiere decir que el aprendizaje debe darse en un contexto de significados para el estudiante, y que el saber que se construya será particularmente reconstruido en la memoria y en la aplicación si se ha acompañado de experiencias que lo recrean y que son parte del entorno individual de quien lo construye.

3.2.1.5. CAMPUS VIRTUAL[17]

"El aprendizaje es un proceso que se da de manera personal, es una construcción propia que incorporamos a nuestra vida, este proceso no es observable de manera directa, si no que se percibe a través de nuestras conductas. También es un proceso social de interacción que gira alrededor de un propósito particular, por ejemplo: en la interacción entre un docente y un estudiante, ambos aprenden conjuntamente, de esta manera se da un intercambio de saberes específicos que permite la construcción de un nuevo conocimiento.

Para esta modalidad, el acceso a los contenidos didácticos, los procesos de aprendizaje y el acompañamiento tutorial se realizan en el Campus Virtual. Los contenidos didácticos con estándares internacionales, que opcionalmente pueden descargarse en formato HTML y PDF para su tratamiento off line o sin conexión a Internet."

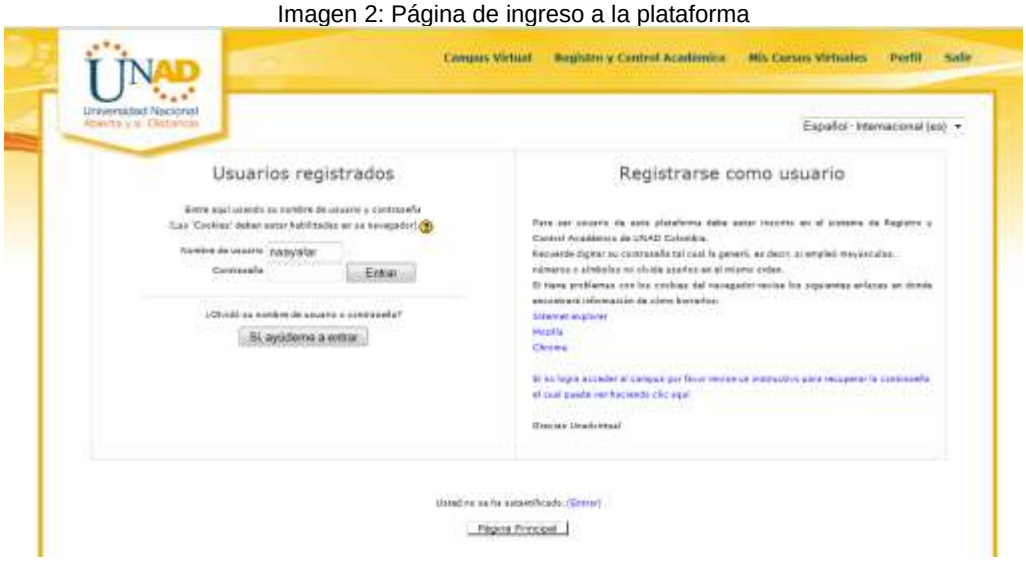
[16] Ibit, página 41
[17] http://estudios.unad.edu.co/especializacion-en-nutricion-animal-sostenible/metodologia

3.2.1.6. PROCESO DE AUTENTICACIÓN AL CAMPUS VIRTUAL

Para la propuesta el proyecto de actualización, cambio o sugerencia de la forma de autenticación, se inicia con la realización del respectivo seguimiento y observación al proceso de autenticación de las personas que laboran en la institución (administrativos), así como a los educandos y al cuerpo docente. Identificando que el único método de acceso utilizado para el ingreso a la plataforma, desde que se instauró el sistema virtual en 2004 al 2011, y que se sigue utilizando en la actualidad, como es la digitación de usuario (login) y contraseña (password) del aprendiz, suministrados por los administradores del sistema. Las contraseñas se encuentran debidamente codificadas y encriptados de tal forma que se evita el hackeo por parte de personas inescrupulosas e interesadas en ocasionar traumas al sistema de aprendizaje. Situación que en muchos de los casos, los mismos estudiantes se encargan de facilitar tales identificaciones a personas extrañas, solicitando la colaboración para el desarrollo de las actividades académicas que se encuentran implantadas en el campus virtual de los diferentes programas académicos de la universidad.

En la imagen 2, se ilustra la página principal del acceso a la plataforma donde ingresa el Nombre de Usuario y su Contraseña, para la intrusión a los curos.

Imagen 2: Página de ingreso a la plataforma



Fuente: https://campus0a.unadvirtual.org/campus0/login/index.php

Se han encontrado algunas dificultades e inconvenientes de acceso, debido a que los aprendices se encargan de cambiar estas contraseñas; acción que se les sugiere no realizar desde el inicio de su proceso de matrícula, llamado que no es atendido por ellos, ocasionando traumatismos e impidiendo su acceso al campus, debido a que la nueva contraseña por ser diseñada y modificada con caracteres especiales que posteriormente se vuelven olvidadizos, por los estudiantes, éstas no son reconocidas por su complejidad lo que causa que no le sea permitido el ingreso al estudiante.

Otro caso que se presenta con las contraseñas es de aquellos estudiantes que solicitan aplazamiento o después de un tiempo al no matricularse; en el momento de retomar sus estudios, e intentar autenticarse para el ingreso a la plataforma, encuentran que tal contraseña ya no es válida o se ha olvidado por el cambio que realizaron a ésta, cuando se encontraba como estudiante activo, situación que es muy frecuente en casos descritos impidiendo su intrusión.

3.2.2. ¿QUÉ ES UNA PLATAFORMA MOODLE?[18]

"Moodle es una plataforma de aprendizaje a distancia (e-learning) basada en software libre que cuenta con una grande y creciente base de usuarios.

Imagen 3. Aplicación en la que se creó la plataforma

Fuente: imágenes google

Moodle es un sistema de gestión avanzada (también denominado "Entorno Virtual de Enseñanza-Aprendizaje (EVEA)"; es decir, una aplicación diseñada para

[18] Centro de Profesorados de Alcalá – Moodle - http://www.redes-cepalcala.org/plataforma/file.php/1/manual_plataforma_cep_alcala.pdf

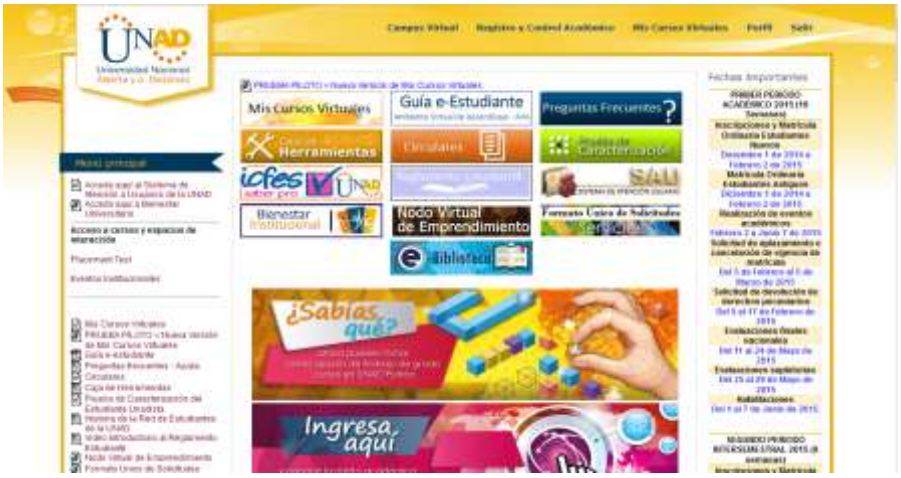
ayudar a los educadores a crear cursos de calidad en línea. Estos tipos de sistema de aprendizaje a distancia a veces son también llamados Ambientes de Aprendizaje Virtual o Educación en Línea.

Moodle fue creado por el australiano Martin Dougiamas. Esta herramienta ha venido evolucionando desde 1999, produciéndose nuevas versiones del producto, extendiéndose por más de 100 países y siendo traducida a más de 50 idiomas."

"La palabra Moodle era al principio un acrónimo de Modular Object-Oriented Dynamic Learning Environment (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular), muy útil para programadores y teóricos de la educación."

En la imagen 4, se ilustra cómo se encuentran distribuidas las actividades dentro del campus virtual; y que encontrará el estudiante en el momento de acceso a ella, ya sea para una actividad en particular o para el ingreso a los cursos que tiene inscritos.

Imagen 4. Página inicial de la plataforma de la UNAD



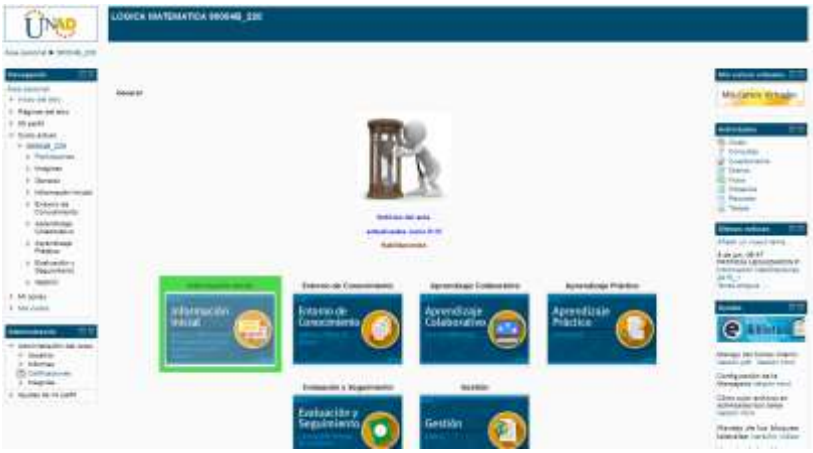
Fuente: http://campus0a.unadvirtual.org/campus0/

"Técnicamente, Moodle es una aplicación que pertenece al grupo de los Gestores de Contenidos Educativos (LMS, Learning Management Systems), también

conocidos como Entornos de Aprendizaje Virtuales (VLE, Virtual Learning Manage-ments), un subgrupo de los Gestores de Contenidos (CMS, Content Management Systems). De una manera más coloquial, podemos decir que Moodle es una aplicación para crear y gestionar plataformas educativas, es decir, espacios donde un centro educativo, institución o empresa, gestiona recursos educativos proporcionados por unos docentes y organiza el acceso a esos recursos por los estudiantes, y además permite la comunicación entre todos los implicados."

En la imagen 5 se observa la distribución de las actividades de un curso específico dentro del campus virtual, donde el estudiante debe identificar cada uno de los enlaces que encuentra, explorar su utilidad, para así poderse desenvolver activamente dentro del curso, solucionando sus posibles inconvenientes de ubicación en el campus creado bajo la modalidad de aprendizaje virtual.

Imagen 5. Campus virtual de un curso de la UNAD



Fuente: http://152.186.37.83/ecbti01/course/view.php?id=12

3.2.3. ANÁLISIS DE AVANCES DE TÉCNICAS BIOMÉTRICAS

Desde el componente investigativo de la UNAD, lo que se pretende con este proyecto es indagar sobre otras fuentes de información acerca de la medición biométrica y sus posibles usos, dentro de las cuales encontramos:

*"Los "**Sistemas de Autenticación Biométricos**"[19], donde expresa que, desde el principio de los tiempos, la búsqueda de un medio de identificación no ambiguo ha sido uno de los objetivos de la humanidad. En la vida cotidiana como en el mundo tecnológico, la importancia de la privacidad y la seguridad de los datos obligan a establecer medidas de identificación y autentificación con el fin de asegurar que ninguna otra persona accede a datos ajenos o servicios privados.*

En la llamada era de la tecnología, cada vez mas actividades que hasta entonces se realizaban en papel han pasado a realizarse mediante aplicaciones informáticas, como el comercio electrónico, o el acceso a datos bancarios, operaciones en las que se necesita garantizar la confidencialidad y seguridad.

Hasta ahora se observan continuamente métodos sencillos para resolver estos problemas como, por ejemplo, el uso de las tarjetas plásticas de identificación, en las que incluso se solía incorporar una foto o una firma a modo de identificación entre personas. En el mundo de la tecnología de la información este planteamiento debe ser modificado ya que no existe una persona que te identifique. Es por ello que se requieren otras técnicas que resuelvan dicho problema, como el uso de password o diferentes protocolos de seguridad que existen."

Con el anterior texto podemos corroborar que a través del inicio de los tiempos, siempre se ha buscado una forma eficiente que se utilice como método efectivo para la identificación del ser humano en los diferentes lugares que han requerido un mayor grado de seguridad, valiéndose de nuevas tecnologías, dándole la respectiva importancia a la privacidad y la seguridad de los datos como personales, empresariales, industriales y comerciales, los cuales exigen el establecimiento de nuevas formas de autentificación garantizando el acceso autorizado únicamente a personas que sean identificables por el sistema, evitando la suplantación de personal que se pueda dedicar a la sustracción o robo de datos ajenos o información relevante de una organización.

[19] Sistemas de Autenticación Biométricos – Seguridad y protección de la información - http://spi1.nisu.org/recop/al01/llopis/Biometricos.PDF

Por ende, proponer del estudio realizado, el sistema de seguridad biométrico más adecuado en cuanto a costos y aplicabilidad tanto en plataforma como para el usuario, optimizando el reconocimiento asertivo del estudiante virtual, siendo de conocimiento general que la aplicación de nuevas tecnologías o sistemas de seguridad, implican un alto costo tanto para los estudiantes como para la universidad misma, pero al observar la documentación anterior, podemos encontrar diferentes tipos de medición biométrica la actual permitiría una verdadera autenticación del usuario final en un entorno web, ya sea para la plataforma de estudio que proporciona la universidad o para el acceso a cualquier entorno que se encuentre en la nube, comprobando y realizando el respectivo filtro de autorizaciones en cuanto acceso se refiere.

El objetivo de este proyecto ha sido proponer un nuevo sistema de seguridad de acceso a las actividades académicas virtuales en la plataforma de la UNAD, que permita tanto para los empleados como a los estudiantes, la reactivación automática de su clave de acceso por medio del reconocimiento facial, siendo la utilización de la cámara interna de los computadores u ordenadores que dispone cada uno de ellos, y que por ser un hardware que se encuentra disponible en cada uno de éstos equipos o puestos de trabajo, lo que facilita reducir que por costos se reduce en su mínimo valor, ya que los usuarios no tienen la necesidad de adquirir ni de invertir en esta clase de tecnología o de aparatos que se requieren para la implementación de este sistema debido a los grandes costos que puede acarrear la compra de los aparatos nombrados.

En cuanto al software a utilizar en la implementación, debe ser instalado, y acondicionado a la misma aplicación base donde se encuentra programada la plataforma de aprendizaje de la universidad, ya que es directamente a ésta, donde el estudiante debe autenticarse para su ingreso y posterior trabajo, desarrollo y entrega de las actividades académicas de sus cursos virtuales.

Dentro del software comercial que se encuentra en el mercado para ser utilizado por la institución encontramos las siguientes aplicaciones[20]:

- FaceComponent: Se encarga de capturar automáticamente asegurando la calidad en la abstracción de imágenes faciales biométricas.
- IrisComponent: se encarga de la captura y procesamiento por lotes de la calidad, abstracción de la cámara de imágenes del iris.
- FormScanner: aplicaciones de escaneo de fichas de huellas dactilares.

Con las aplicaciones descritas, es posible implementar un sistema de identificación o autenticación biométrica, acoplándola con la plataforma de aprendizaje de la institución, garantizando que el estudiante es quien en realidad está desarrollando las actividades, evitando la suplantación del individuo.

3.3. MARCO CONCEPTUAL

3.3.1. EL CONCEPTO DE LA BIOMETRÍA

Uno de los términos más relevantes y del cual será el más tratado en el desarrollo del presente trabajo, es denominado como la "biometría", que en términos más sencillos significa como la medida de un patrón humano en cada persona, para el caso en éste documento, se está tratando con la biometría facial.

En los casos que tienen referencia con la seguridad informática, el tema que más se ha utilizado es el de la criptografía, que fue el método más empleado y utilizado para proteger y ocultar dentro de unos párrafos sin sentido la información relevante, de posibles personas inescrupulosas que se encargaban de interceptar los mensajes y sustraer la información o los datos que solamente determinados grupos de personas podrían tener acceso a tal información.

[20] Software Biométrico- http://www.aware.com/es/biometrics/index.html?gclid=CNrooqLd0cUCFQgRHwodpp8AGg

Cuando hablamos de seguridad biométrica podemos expresar que la persona es “la llave” única para tener acceso físico o lógico en una organización o sistema, donde la combinación de la electrónica y la tecnología con los últimos adelantos en éstos, han arrojado excelentes resultados en el desarrollado de nuevas técnicas para la solución y fortalecimiento en materia de la seguridad informática.

La inclusión de todas estas técnicas, tecnologías y métodos de detección ha generado grandes cambios en cuestiones de seguridad tanto informático como físico en instituciones, entidades y organizaciones, cohibiendo el ingreso no autorizado de personas a dichas corporaciones, sin antes realizar la plena verificación de su identidad, corroborando que dicho individuo sea plenamente reconocido y autorizado para su intrusión.

Haciendo referencia al hardware que es la parte física de un sistema informático como son los elementos electrónicos o dispositivos que utilizan para la capturar las imágenes del individuo, siendo la base primordial para la propuesta del proyecto. Estos dispositivos serán los encargados de realizar dicha captura facial del usuario, enviando sus imágenes, convertidas en datos, para realizar la comparación de estas, validando su autenticidad y permitiendo su acceso. Es importante destacar que el software del prototipo debe contener una pequeña muestra de información en su base de datos, con imágenes faciales de algunos de los usuarios; de forma tal que sea posible la realización de las pruebas pertinentes y lograr obtener los resultados esperados en el posible uso e implementación en el sistema de autenticación.

Un criterio que se debe tener en cuenta dentro de los sistemas de seguridad basados en identificación biométrica en el momento de su ejecución, son los mensajes visuales y auditivos que se generarán al errar o al encontrar que la imagen capturada presenta discrepancia entre la almacenada en la base de datos y la recibida por el dispositivo, indicando que el usuario que intenta ingresar su validación no fue exitosa en el momento de acceso.

Es bien sabido que tanto el software como el hardware estarán directamente relacionados, que cuando uno falle, el otro por obvias razones dejara de funcionar por lo que el sistema implantado en la plataforma no permitirá su correcto funcionamiento.

La biometría tiene como apoyo para su utilización, dispositivos de captura y almacenamiento, siendo este último capaz de contener un determinado número de patrones de datos e imágenes de usuarios a los que se les debe llevar el control de la información. De estos datos biométricos, es posible la captura gracias a dispositivos electrónicos que facilitan el almacenamiento en bases de datos para posteriormente compararlos con una referencia específica entre lo capturado y lo almacenado. Una vez capturada la imagen y creado el patrón de compatibilidad, esta es analizada hasta en cinco (5) posiciones y perspectivas diferentes, entregando un cuadro bidimensional, que indicará si el usuario es el verdadero, proporcionando un mayor grado de precisión entre las coincidencias faciales, así la imagen original se encuentre distorsionada o ligeramente borrosa.

Si estos eventos coinciden o sucede lo contrario, el sistema concederá o negará el libre acceso del usuario al sistema deseado, dependiendo de la respuesta obtenida.

En cuanto a los sistemas de seguridad biométricos, éstos están basados en el almacenamiento de registros de información relacionada con las características propias de cada individuo, estableciendo patrones estrictamente necesarios para su correcto funcionamiento de la técnica. Hoy en día el bum de la nueva tecnología junto con los actuales métodos de identificación biométrica que se encuentran en uso dentro de diversos ámbitos empresariales como sociales, están remplazando a los ya existentes, pasando de lo tradicional como los passwords, claves de las tarjetas de crédito, tarjetas magnéticas de identificación con códigos de barras y otros sistemas conocidos por la sociedad, hasta la era digital, finalizando en la técnica de la biométrica.

Con el valioso apoyo de estos métodos de seguridad, no será fácil olvidar la clave de acceso que era asignada a una determinada labor; dificultad que será superada a medida que avance la tecnología, lo que impedirá que no se presente nuevamente ni con mucha frecuencia, los casos mencionados de pérdida de la información.

Los sistemas de autenticación biométrica más conocidos en el mundo de la seguridad, quienes han establecido fortalezas y debilidades, al ser aplicadas en diversos campos y actividades cotidianas, especialmente en el resguardo de la información, podemos nombrar los siguientes casos:

3.3.2. RECONOCIMIENTO DE HUELLA DACTILAR [21]

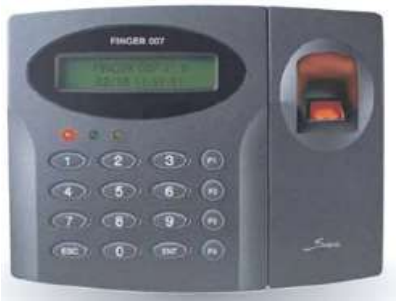
Acerca del reconocimiento por medio de la huella dactilar se tendrá en cuenta la descripción presentada por la empresa ICE SEGURIDAD S.L.

"Es el sistema biométrico más antiguo y más económico. Plantea además la ventaja de ser muy cómodo de utilizar. El problema de higiene al existir contacto, problema de lectura con manos sucias, es relativamente fácil de copiar una huella y por tanto engañar al sistema, también puede generar cierto recelo en los usuarios por asociarse al entorno policial, son algunas de las dificultades que se presenta. Pese a estos problemas es el sistema ideal para instalaciones sin una elevada necesidad de seguridad."

El Reconocimiento dactilar se basa en la extracción de características especiales de la huella dactilar de la persona.

[21] ICE SEGURIDAD S.L. - Productos y servicios http://www.iceseguridad.com/sis_biom.htm

Imagen 6. ICE SEGURIDAD S.L.



Fuente: http://www.iceseguridad.com/sis_biom.htm

Ventajas:

- ✓ Cómodo de utilizar.
- ✓ Pequeña variabilidad en el tiempo.
- ✓ Buena precisión, tiene una Fiabilidad de 1 en 64.000 millones son iguales.

Desventajas:

- ✓ Problema de higiene.
- ✓ Asociado con temas penales.
- ✓ Problema de lectura con manos sucias.
- ✓ Fácil de copiar una huella.

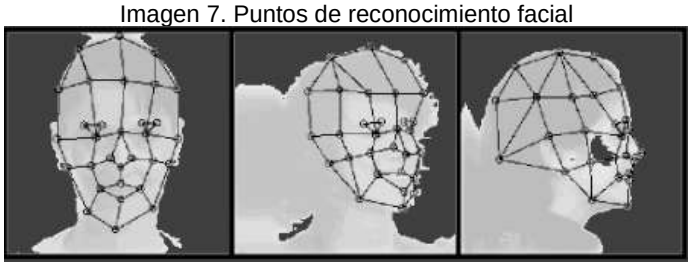
3.3.3. RECONOCIMIENTO FACIAL[22]

"Una cámara toma la imagen de una cara, y mide las distancias y proporciones entre los puntos que separan la parte interior y exterior de los ojos, de la nariz, y la boca principalmente. Aunque reporta la ventaja de poder archivar una foto o secuencia de vídeo junto con el fichaje del acceso realizado, es un sistema con

[22] ICE SEGURIDAD S.L. - Productos y servicios - http://www.iceseguridad.com/sis_biom.htm

una tasa demasiado elevada de fallo (cicatrices, gafas, gorra, barba, etc.) en el momento del escaneo, este se realiza analizando el rostro en función de ciertos puntos claves, se obtiene una plantilla única que permite autentificar a una persona de forma precisa y este análisis se puede hacer, geométrico e información de textura y forma."

Imagen 7. Puntos de reconocimiento facial



Fuente: http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Ventajas:

- ✓ Permite captación única del rostro del individuo.
- ✓ La información adicional se expresa según el estado de ánimo.
- ✓ Es fácilmente comprobable por un operador humano.

Desventajas:

- ✓ Presenta un alto grado de fallo.
- ✓ La iluminación es prioritaria.
- ✓ Es fácilmente engañable con imágenes impresas.

3.3.4. RECONOCIMIENTO IRIS [23]

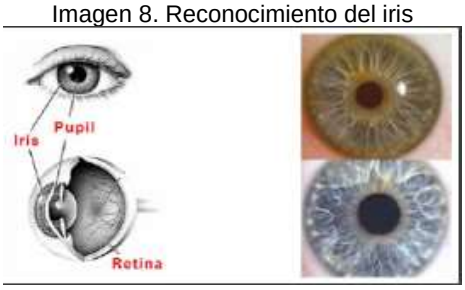
"Es la extracción de características de la textura del iris, la lectura con un alto nivel

[23] https://cienciasetecnologia.com/biometria-leitura-iris-retina/?lang=es; http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

de fiabilidad y seguridad, el único inconveniente que plantea es ser un tanto intrusiva al tener que realizarse un escáner del ojo, el cual tiene en 11 milímetros de diámetro cada iris donde se concentra más de 400 características. Rasgos, surcos radiales, Zona pupilar, borde pigmentado, zona Ciliar, collarete y criptas.

Para obtener estas características una cámara escanea el iris y genera una imagen que es analizada por medio de los algoritmos de Daugman para obtener el código del iris (IrisCode). Éste código ocupa solo 256 bytes, luego es buscada en una base de datos donde encuentra un código homólogo."

Imagen 8. Reconocimiento del iris



Fuente: http://www.biometria.gov.ar/metodos-biometricos/iris.aspx

Ventajas:

- ✓ No se conoce ningún reporte falso de aceptación.
- ✓ Puede entregar información adicional del individuo.
- ✓ Puede ser aplicado para alta seguridad.

Desventajas:

- ✓ Es Intrusivo, es decir, puede causar problemas de violencia.
- ✓ Es dependiente de la calidad con la que se capture la imagen del iris.
- ✓ Se requiere que el usuario entregue su mejor disponibilidad para capturar una imagen del iris de buena calidad.
- ✓ Ligeramente costoso.

3.3.5. RECONOCIMIENTO DE LAS CARACTERÍSTICAS DE LA PALMA DE LA MANO [24]

"Esta tecnología se aplica a la lectura de pliegues, huellas, arrugas midiendo las características físicas de la mano y dedos desde una perspectiva 3D, este procedimiento se transforma en una serie de patrones numéricos de la mano convirtiendo el grosor y localización de las venas, de la longitud de los dedos además del acho y altura, luego estos patrones se comparan en una base de datos y demás características únicas en cada ser humano en la palma de la mano. Sistema similar a la lectura de huella dactilar con la importante ventaja de poder realizar el escaneado sin contacto físico."

Imagen 9. Reconocimiento puntos de la mano

Fuente: Computer Visión http://www.computervisionbytecnalia.com/portfolio/sistema-de-reconocimiento-biometrico-de-la-palma-de-la-mano/

Ventajas:

- ✓ Permite la agilidad de acceso y reconocimiento.
- ✓ Procesamiento muy rápido en la identificación.

Desventajas:

- ✓ Dispositivos de lectura de tamaño medio.
- ✓ Poco confiable en áreas de alto grado de suciedad.

[24] http://www.computervisionbytecnalia.com/portfolio/sistema-de-reconocimiento-biometrico-de-la-palma-de-la-mano/

3.3.6. RECONOCIMIENTO POR TONOS DE VOZ [25]

"A diferencia con la anteriores medidas de seguridad biométrica, el reconocimiento por voz reside en la necesidad de tomar varias muestras diferentes, ya que la voz varía dependiendo de la situación sentimental de la persona, se obtiene un espectrograma que puede verse influenciado por una congestión nasal, por ejemplo. Es susceptible al engaño si se producen grabaciones. Su fiabilidad se encuentra por debajo de otros sistemas biométricos."

Imagen 10. Reconocimiento del tono de voz

Fuente: Sistemas Biométricos

En éste proceso se estudia el timbre, intensidad, tono y frecuencia, acumulando esta medición con la situación en la que se toma la muestra nos referimos a que puede ser difusa en el sentido de que debemos evaluar el estado de ánimo de la persona, ya sea alegre, triste, con un tono sensual o simplemente de enojo.

Ventajas:

- ✓ Permite que sea utilizado vía telefónica.
- ✓ Procesamiento rápido y fácil de aplicar.
- ✓ No es fácil duplicable con exactitud.

Desventajas:

- ✓ Fácilmente engañarle con dispositivos de captura de voz.

[25] Sistemas Biométricos - http://sistemasbiometricos.over-blog.com/article-reconocimiento-de-voz-62568598.html

3.3.7. RECONOCIMIENTO POR LECTURA DE VENAS [26]

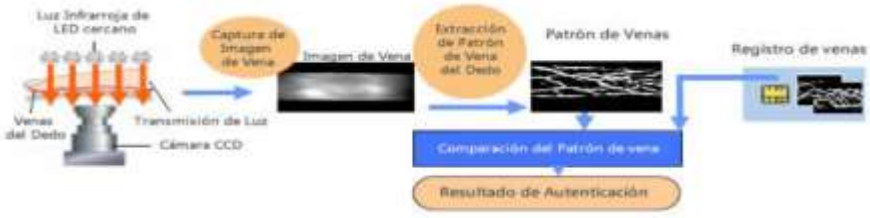
"El reconocimiento de las venas de los dedos, es un método de autenticación biométrica que utiliza técnicas de reconocimiento basados en imágenes de los patrones de las venas que están debajo de la piel de los dedos humanos. El reconocimiento de las venas del dedo es una de las muchas formas de biometría que se utilizan para identificar a las personas y verificar su identidad.

La identificación de la vena del dedo, es un sistema de autenticación biométrica que compara el patrón vascular en el dedo de un individuo, con los datos obtenidos previamente. Hitachi desarrollo y patento un sistema de identificación de venas de los dedos en el año 2005. Esta tecnología está actualmente en uso y se está desarrollando en una amplia variedad de aplicaciones, incluyendo la autenticación de las tarjetas de crédito, la seguridad de los automóviles, sistemas de tiempo y asistencia de los empleados, la autenticación del computador y de red, y cajeros automáticos.

Los patrones de los vasos sanguíneos son únicos para cada individuo, así como otros datos biométricos como las huellas digitales o los patrones del iris. A diferencia de otros sistemas biométricos, los patrones de los vasos sanguíneos son casi imposibles de falsificar, ya que se encuentran debajo de la superficie de la piel. Los sistemas biométricos basados en huellas digitales pueden ser engañados con un dedo falso dotado de una huella digital copiada, los sistemas basados en voz y características faciales pueden ser engañados por las grabaciones e imágenes de alta resolución. El sistema de identificación de venas de los dedos es mucho más difícil de engañar, ya que sólo se puede autenticar el dedo de una persona viva."

[26] http://www.tecnoseguro.com/analisis/cctv/reconocimiento-de-venas-la-nueva-tecnologia-en-biometria.html

Imagen 11. Ampliación diagrama venas.



Fuente: RISCO GROUOP.- http://www.tecnoseguro.com/analisis/cctv/reconocimiento-de-venas-la-nueva-tecnologia-en-biometria.html

"Científicos de la Universidad Carlos III de Madrid (UC3M) [27], evalúan una técnica que aumenta la eficacia y usabilidad de la identificación biométrica vascular. Utilizando la información ofrecida por las venas de la mano, consiguen entre un 99,5 y un 99,8 por ciento de éxito, realizando la identificación de la persona en cuestión en apenas dos segundos.

Las venas del cuerpo humano presentan una distribución geométrica única para cada persona y que es invariable con el paso del tiempo. Su distribución aleatoria permite que un sensor - similar al de una cámara de fotos - capte mediante luz infrarroja las venas superficiales de la mano, de manera que se obtiene un patrón exclusivo de cada individuo.

Para medir la eficacia de este modelo biométrico, Raúl Sánchez-Reillo, investigador del Grupo Universitario de Tecnologías de Identificación de la Universidad Carlos III de Madrid (UC3M), ha probado el sistema en condiciones extremas, tanto de humedad con diferentes luces ambientales.

3.3.8. IDENTIFICACIÓN MÁS RÁPIDA Y SEGURA[28]

"*Las conclusiones obtenidas en su estudio, publicado en la International Carnahan*

[27] http://portal.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/biometria_vascular

[28] Tomado literalmente de: Un estudio analiza la eficacia de la identificación biométrica por las venas de las manos - http://portal.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/biometria_vascular

Conference on Security Technology (IEEE), demuestra que no se produjeron resultados de 'falsa aceptación', por lo que las probabilidades de que el sistema se equivoque frente a usos fraudulentos son prácticamente nulas. En lo que respecta a la humedad, el investigador afirma que el sistema es más seguro que las huellas dactilares; mientras que en el caso de la luz ambiental, es necesario optimizar el escenario donde se ubicará el sensor, puesto que las imágenes se velan con altas concentraciones de luz solar. En general, las tasas de error son bajas y fluctúan entre el 0,5 y el 0,2 por ciento. Sánchez-Reillo explica que en la mayoría de los casos "el falso rechazo se produce fundamentalmente cuando las personas no colocan la mano correctamente en el sensor".

En la actualidad, los sistemas de seguridad biométricos están siendo progresivamente utilizados tanto en aplicaciones bancarias como comerciales. El uso de esta técnica biométrica se está implementando también en hospitales, donde podrían sustituir a las tarjetas inteligentes o a la huella dactilar. En la práctica, "analizar la estructura de las venas es más cómodo y rápido a la hora de acceder a los registros, a los laboratorios de análisis clínicos o para entrar al quirófano, ya que no es necesario que los médicos y las enfermeras se quiten los guantes de látex para que el sensor los identifique", explica el profesor del Departamento de Tecnología Electrónica de la UC3M."

3.3.9. BENEFICIOS DE LA BIOMETRÍA

Ya hemos hablado de los diferentes tipos de mediciones biométricas más reconocidos en el mundo de la seguridad, ahora se hablará de los beneficios que ofrece esta nueva tecnología para ser aplicada, evitando las diversas situaciones que se encuentran y que se describen a continuación: una de las más utilizadas; consistente en la memorización una contraseña, que no habría necesidad de tenerla, ya que generalmente para evitar su olvido por parte de los usuarios, se diseñan con palabras fáciles de recordar, como lo es la fecha de un cumpleaños,

el número del teléfono, el nombre del hijo/a etc. O como el portar una tarjeta o llave en lugares poco recomendados y de fácil alcance de personas inescrupulosas, con el fin de sustraerlas logrando el acceso a un sistema, a una institución o, a un espacio específico que requiere de la verificación de la identificación, autenticando la veracidad del usuario. Gracias a la aplicación de los métodos de medición biométrica, es posible evadir estos inconvenientes, por estar directamente relacionados con el usuario mismo y por la exactitud que presenta en sus métodos permitiendo un alto grado de seguridad.

Por otra parte la adquisición y posterior utilización de estos dispositivos de medición biométrica, permitirá a las organizaciones una disminución en costos de la administración de sus sistemas de seguridad, debido a que sólo se estaría realizando el mantenimiento respectivo al elemento lector seleccionado, al almacenamiento de la información capturada, contando desde luego con el talento humano, el cual se encargará de manipular, actualizar, y disponer de la base de datos y del control de acceso.

Las características biométricas propias del ser humano, permiten crear patrones únicos e irrepetibles que sean aprovechadas en la utilización de esta metodología y tecnología para la identificación y autenticación del hombre, debido a que son particularidades específicas e intransferibles del individuo, lo que impediría la suplantación, adulteración y duplicidad de esta información genética.

3.3.10. APLICACIONES DE LA BIOMETRÍA

Esta modalidad se está aplicando hoy en día en diferentes lugares y zonas que requieren de un mayor rango de seguridad como son:

1. Seguridad en la movilidad y de accesos, como lo son los Aeropuertos, instalaciones industriales, instituciones públicas, centros hospitalarios de especial cuidado.

2. Seguridad en transacciones electrónicas como lo son los cajeros automáticos, uso de tarjetas de crédito.
3. Seguridad de acceso por medio de la validación de la firma electrónica en documentos enviados por web, sistemas electrónicos por votación.
4. Maquinaria de manejo especial o sectores de instalaciones exclusivas de personal autorizados para su acceso.

3.4. MARCO LEGAL

Dentro del marco legal que rige la seguridad de la información y las leyes que lo actúan en cuanto a su protección intelectual, derechos de autor, propiedad industrial, firmas electrónicas y comercio electrónico, se reunieron las siguientes leyes que consideran lo anteriormente dicho en la normatividad Colombiana.

TIPO DE DOCUMENTO	NÚMERO DE NORMA	FECHA	ENTIDAD	DESCRIPCIÓN
LEY	**603**	**2000**	Unidad Administrativa Especial Dirección Nacional de Derecho Autor.	Esta ley hace referencia a la protección de los derechos de autor en Colombia. **"Por la cual se modifica el artículo 47 de la Ley 222 de 1995". El Congreso de Colombia.** Tomado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960
LEY	**1273**	**2009**	El Congreso de Colombia	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" Tomado de : http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
PROYECTO DE LEY	**016**	**2014**	El Congreso de Colombia	Por la cual se implementa el Sistema de Identificación Biométrico en los aeropuertos, terminales de transporte terrestre y marítimo a nivel nacional y se dictan otras disposiciones. Tomado de: http://190.26.211.102/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2014%20-%202015/PL%20016-14%20BIOMETRIA.pdf
NORMA INTERNACIONAL	**ISO/IEC 24745**	**2011**	ISO e IEC	Tecnología de la información – Técnicas de seguridad – Protección de la información biométrica.
DECRETO	**1766**	**2011**	Sistema Federal de Identificación Biométrica para la Seguridad (SIBIOS)	Tiene por objeto prestar un servicio centralizado de información respecto de los registros patronímicos y biológicos individuales, a los fines de contribuir a la comprobación idónea y oportuna en materia de identificación de personas y rastros, en procura de optimizar la investigación científica de delitos y el apoyo a la función preventiva de seguridad.
LEY ESTATUTARIA	**1266**	**2008**	El Congreso de Colombia	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Tabla 1. Leyes reguladoras, Fuente autor

4. DISEÑO METODOLÓGICO

4.1. ALCANCES DEL PROYECTO

La Universidad Nacional Abierta y a Distancia por ser una de las instituciones más importantes en el sector educativo a nivel nacional e internacional, en su incorporación a la parte virtual y el uso del internet con apoyo de las TIC´s, como forma de comunicación directa con sus estudiantes desde el año 2004, siempre ha empleado una única forma de autenticación de los usuarios a la plataforma de aprendizaje, lo que ha demostrado ser el método tradicional para el ingreso de los estudiantes al campus virtual, por lo que la propuesta busca innovar en la implementación de una técnica de autenticación de acceso a esta, ya que se ha observado en algunas oportunidades, la suplantación del estudiante en sus cursos, situación que ha afectado directamente la calidad en el aprendizaje y por ende una preocupante realidad, ya que el buen nombre de la institución se ve afectado directamente, por la baja calidad de egresados que entrega la universidad a la sociedad, algo que es posible frenar o controlar con la aplicación de una nueva técnica que demuestre que es el estudiante real quien ingresa para la presentación de sus actividades académicas, lo que hará que la calidad y el nivel educativo de la institución supere las estadísticas tanto de deserción como de suplantación de estudiantes en los periodos académicos.

La Universidad por disponer de una buena infraestructura tecnológica, muy bien configurada y adecuada en cada uno de sus Centros, hace que se brinde la mejor y mayor comodidad, en el aprovechamiento de los recursos informáticos con que cuenta para el beneficio de sus estudiantes, garantizando un buen desempeño de éstos en el desarrollo de sus actividades académicas, optimizando los recursos físicos y lógicos que se encuentran incorporados a la tecnología actual, en disposición de los educandos sin costo alguno para ellos, contando con una

conexión a internet de banda ancha de 10 Mb, programas ofimáticos y aplicaciones en línea dentro del campus virtual, con los controles máximos y específicos para reducir los riesgos a un nivel mínimo de afectación en su seguridad informática.

4.2. MÉTODOS PARA LA BÚSQUEDA DE INFORMACIÓN

En el proceso de búsqueda para la elaboración y presentación del proyecto, se pretende encontrar la mayor cantidad de información referente al tema planteado, como lo es el la Biometría; en especial la técnica de Reconocimiento Facial, ya que es a la que se desea llegar con la actual propuesta, dando cumplimiento a los objetivos propuestos.

Se tendrán acciones como:

4.2.1. OBSERVACIÓN DIRECTA

Mediante esta acción se logrará evidenciar la forma de autenticación e ingreso que tienen los usuarios a la plataforma de aprendizaje de la universidad y sus diversas dificultades que presentan con la técnica actual de identificación.

4.2.2. ENTREVISTA

A través de una serie de preguntas al administrador del sistema se logrará identificar en que aplicación está creada o montada la plataforma de aprendizaje, si acepta o permite la inclusión de aplicaciones y bajo qué tipo de programación o bajo que formatos permite su acoplamiento, de esta forma se podrá encontrar lo mejor y más acorde a lo que se puede sugerir en el presente proyecto.

Aplicando esta misma técnica y por medio de llamada telefónica a las empresas que ofrecen productos relacionados y en particular al que se desea tener en

cuenta para su recomendación, se espera obtener los costos y características especiales que necesita o requiere la aplicación, para ser incorporada a la plataforma como innovación en su utilización a nivel educativo.

4.3. TIPO DE INVESTIGACIÓN

4.3.1. INVESTIGACIÓN DOCUMENTAL

Este tipo de investigación es empleado en el momento de iniciar la búsqueda de antecedentes y hace referencia al tema seleccionado como objeto de exploración de la información relacionada, básicamente, en documentos fundamentados del eje tratado, así como trabajos de investigación realizados a dicho tema seleccionado, relacionando los ensayos, artículos, documentos publicados en revistas especializadas que cumplan con las características demarcadas.

Gracias a la investigación documental, nos brinda un modo ordenado del proceder para llegar a un fin determinado, especialmente en el momento del procesamiento de la información recopilada como un camino para llegar a un resultado, esto es la separación de sus partes y se procede a revisar ordenadamente y por separado cada uno de ellos que apoye mediante la descomposición de sus elementos llegando a una conclusión efectiva.

5. ANÁLISIS DE VIABILIDAD EN LA IMPLEMENTACIÓN DE SISTEMAS BIOMÉTRICOS PARA LA AUTENTICACIÓN DE USUARIOS EN LAS PLATAFORMAS WEB

5.1. TABLA DE COMPARACIÓN ENTRE MÉTODOS BIOMÉTRICOS

MÉTODO DE SISTEMAS BIOMÉTRICOS	FORTALEZAS	DEBILIDADES
RECONOCIMIENTO DE HUELLA DACTILAR	Fácil de utilizar, conocido mundialmente, rapidez en su uso, fácil mantenimiento, apropiado con bajo nivel de seguridad.	Delicado con su higiene, fácil de engañar, dispositivos un tanto costosos, asociado con antecedentes judiciales.
RECONOCIMIENTO FACIAL	Sistema económico en uso e implementación, reconocimiento por rostro de más de una imagen, se debe mantener actualizado, facilidad en su mantenimiento, dispositivos económicos.	Fácil de engañar, pero seguro, actualización constante por cambios faciales.
RECONOCIMIENTO IRIS	Alto nivel de fiabilidad y seguridad, económico en dispositivos.	Fallo por cambios en el ojo, actualización contante de la imagen, no aplicable a toda persona, posible riesgo de daño en el ojo, costoso en su aplicabilidad y dispositivos.
RECONOCIMIENTO POR TONOS DE VOZ	Basado en los decibeles de la voz, dispositivos económicos.	Se deben capturar varias muestras, ocasiona un alto volumen de almacenamiento en archivo, puede ser influenciado por congestión nasal o problemas de otorrinolaringología, dependiente de la situación sentimental o emocional de la persona, facilidad de ser engañado,

Tabla 2. Comparación entre métodos biométricos, Fuente autor

Con el análisis realizado anteriormente a los diferentes métodos aplicados en los sistemas para reforzar su seguridad de acceso, encontramos que se cuenta con muchas fortalezas y debilidades, donde cada uno de ellos aporta características específicas y especiales para su utilización, ya que son técnicas donde algunos de ellos emplean costosos dispositivos, donde la practicidad no es la más recomendada y su utilización no es muy adecuada, así como su mantenimiento, adquisición e implantación no es la más económica del mercado.

En cuanto a la adquisición y posterior utilización de estos dispositivos de medición biométrica, permitirá a las organizaciones una disminución en costos de la administración de sus sistemas de seguridad, pero no en cuanto a su mantenimiento y continuidad de uso, ya que es muy difícil el conservar algunos de ellos por su alto costo, por lo que se expone, con esta reflexión se proponga un método efectivo que brinde los mejores resultados en cuanto a practicidad, economía, facilidad de instalación, de adquisición, de implantación y de uso, por lo que se propone que el método que brinda todas estas ventajas sea el de **Reconocimiento Facial**, debido a que a pesar de sus pocas deficiencias que presenta, brinda la calidad y efectividad requerida en lo que hace referencia al acceso de un usuario en un entorno, ya sea de aprendizaje o de ingreso físico en un establecimiento u organización. Para el caso específico en que se basa el presente trabajo en nuestra universidad, éste método y técnica facilita su aplicación en la plataforma, que por ser actividades en línea y de carácter individual en un ambiente virtual, donde el estudiante para su ingreso ya no requeriría de la digitación del usuario y contraseña, sino consistiría en ubicarse o sentarse frente a la cámara de su computador, donde la aplicación instalada en la plataforma académica identificará y reconocerá al educando, garantizando de esta forma que sea el aprendiz correcto, logrando diferenciar entre una fotografía y el ser humano propiamente dicho sin riesgo al engaño del sistema.

A continuación se enumeran algunas de las empresas desarrolladoras del software y aplicaciones creadas de acuerdo a las necesidades de las mismas.

5.2. APLICACIONES CONOCIDAS PARA EL RECONOCIMIENTO FACIAL

5.2.1. NUEVO SOFTWARE DE RECONOCIMIENTO FACIAL "*CARA*" [29]

Esta aplicación llamada **Cara**, desarrollada por **IMRSV**. De acuerdo a lo que explica el CEO de la empresa, Jason Sosa, Cara es un equivalente a una plataforma de datos estadísticos de páginas web, pero aplicado al **reconocimiento facial**.

De la misma forma en que la publicidad de la Web se adapta a los gustos de los usuarios, Cara tiene la capacidad de brindar el material suficiente para alcanzar ese mismo nivel de personalización en la publicidad convencional. **Cara** puede detectar múltiples rostros a una distancia máxima de 7,5 metros, reconocer el género, establecer si son niños, adultos, o mayores. Otro aspecto importante de su detección es el *"nivel de atención"* que las personas le dan a la cámara.

Básicamente, lo que se busca es obtener la *"respuesta humana"* a cada producto, y **Cara** se perfila como la herramienta ideal para ello. Como era de esperarse, ***la privacidad*** es un tema muy delicado en el ámbito del **reconocimiento facial**, pero Cara lo resuelve de forma relativamente sencilla: Si bien conserva los datos estadísticos, nunca almacena las imágenes.

El software está disponible para Windows y Linux, a un precio de 39.95 dólares por cada cámara que se quiera utilizar. Sin embargo, los requerimientos de Cara son relativamente bajos, y en el futuro podrá operar en plataformas móviles como iOS y Android.

[29] http://www.neoteo.com/cara-nuevo-software-de-reconocimiento-facial/

5.2.2. SISTEMAS DE GESTIÓN DE VÍDEO "*VMS- Video Management Systems*"[30]

A través del modelo VMS de IProNet, se puede disponer de la instalación para cualquier número de cámaras, desde una hasta miles, todo ello gestionado por un software e-netcamCLIENT junto a nuestros grabadores e-netcamRMS, a los que a su vez, se les pueden añadir las aplicaciones desarrolladas por IProNet entre ellas: el reconocimiento y lectura de matrículas, conteo de personas/objetos, reconocimiento facial, analítica, etc.

Los sistemas de Gestión de Vídeo de IProNet Sistemas podrían resolver las necesidades de visualización, grabación, alarmas y tele actuación con cámaras y codecs de vídeo IP. Su capacitación técnica es garantía de prestaciones, fiabilidad y confiabilidad para dar respuesta tanto en situaciones de alta disponibilidad como en pequeñas instalaciones.

5.2.3. RECONOCIMIENTO BIOMÉTRICO FACIAL "*SmartFACE*" [31]

Este sistema especialmente indicado para control de accesos. SmartFACE es otra posible solución de reconocimiento facial de IProNet sistemas, consistente en identificar a las personas que aparecen en la imagen a partir de una base de datos creada previamente.

El SmartFACE permite dar de alta personas en listas a través de imágenes capturadas desde las propias cámaras o importadas desde ficheros, creándose así un perfil de la persona.

[30] http://www.ipronet.es/productos/vms.php
[31] SmartFACE - http://www.ipronet.es/productos/vms.php

5.2.4. ALGORITMOS INTELIGENTES "*FACECHECK*"[32]

Con sus algoritmos inteligentes de reconocimiento facial, FaceCheck analiza la entrada de numerosas cámaras de CCTV (Circuito Cerrado de Televisión), y compara las imágenes capturadas con las plantillas y perfiles almacenados en la base de datos. El sistema anuncia instantáneamente la presencia de individuos sospechosos, alertando en forma inmediata a los operadores.

FaceCheck se ha desarrollado para evitar posibles amenazas y riesgos en diversos establecimientos y asimismo es de gran ayuda en las investigaciones policiales, es compatible con sistemas CCTV ya instalados, que tengan cámaras de transmisión análoga, con una resolución mínima de 420 líneas o superior en la norma NTCS o PAL.

5.2.5. MIB – TECHNOLOGY SOLUTIONS - RECONOCIMIENTO FACIAL[33]

Tecnología de última generación, no intrusiva, que utiliza el software propietario FaceRecognition, para generar un código único asociado con el rostro de una persona.

La aplicación FacePhi de reconocimiento facial nos permite determinar la identidad de una persona analizando características físicas únicas e intransferibles de su rostro, que son tomadas por una tecnología utilizando varios algoritmos propios del software FaceRecognition.

Dicha tecnología no es intrusiva y no necesita de colaboración por parte del usuario, sólo es necesario que su rostro sea capturado por una cámara web.

[32] FaceCheck - http://trebax.net/pdf/FaceCheck+Verify_Spanish.pdf
[33] MIB- Technology Solutions - http://mibtechsolution.com/reconocimiento.html

SISTEMA DE IDENTIFICACIÓN FACIAL – "FaceRecognition" Es aplicable en video vigilancia, detección de sospechosos, control de acceso, cajeros automáticos, banca online, vip y fidelización, banca móvil, verificación de firmas, login de empleados, gestión de perfiles online, aplicaciones móviles y sector automotriz.

Como conclusión luego de haber analizado las tecnologías que se ofrecen en el mercado a cerca del reconocimiento facial, se puede exponer que, una de las ventajas de esta tecnología es que no requiere la colaboración por parte del usuario en este caso el estudiante, que por diferentes razones podría estar poco interesado en la implementación de este tipo de aplicaciones. Por el contrario sólo es necesario que su rostro sea captado por una cámara para garantizar la concordancia de la persona que aparece en el sistema y la que está frente al equipo de cómputo.

6. PROPUESTA DE IMPLEMENTACIÓN DE SISTEMAS BIOMÉTRICOS PARA LA AUTENTICACIÓN DE USUARIOS EN LAS PLATAFORMAS WEB

A continuación se hace la descripción de la propuesta con lo requerido y recomendado para la implementación el software MIB – TECHNOLOGY SOLUTIONS - RECONOCIMIENTO FACIAL - **FacePhi** en la plataforma web de aprendizaje.

6.1. REFERENCIA DE LA APLICACIÓN.

Cuando se pretende implementar un software dentro de una plataforma en una institución educativa, es necesario cambiar algunas normas, políticas de seguridad y asumir los costos que se acarrean, procurando mantener absoluta confidencialidad, privacidad, integridad y disponibilidad la información recolectada e informar las modificaciones a los usuarios, los cuales encontrarán en el momento que deseen autenticarse para el ingreso a la plataforma.

La aplicación facial FacePhi recomendada se encuentra en SDK un producto framework de desarrollo que posibilita la integración en diferentes tipos de plataformas, lo que permite que se facilite la implementación con la utilizada en este momento por la institución.

FacePhi, garantiza el uso para un número indeterminado de usuarios y de igual forma un número indefinido de ingresos a la plataforma, lo que hace que sea una de las aplicaciones más indicadas ya que los estudiantes ingresan a los cursos en cualquier momento o lugar para el desarrollo de las diferentes actividades académicas, esto permitirá que se convierta en una de las formas más precisas de autenticación garantizando su ingreso por medio de la biometría capaz de operar en tiempo real.

La aplicación FacePhi permite almacenar las imágenes capturadas de los usuarios en formatos como JPG, BMG, JPEG, PNG y otras conocidas en el ámbito

de la multimedia facilitando su almacenamiento y comparación de los usuarios auténticos, su fuente de captura se puede realizar desde archivos, dispositivos de captura compatibles con DirectShow y dispositivos integrados en móviles Android.

6.2. CARACTERÍSTICAS DEL PRODUCTO

La aplicación de reconocimiento facial "FacePhi SDK" consta de:

- Librerías C++ para integrar la tecnología en aplicaciones nativas de Windows.
- Librerías .Net para integrar la tecnología en aplicaciones Windows de escritorio (WinForms, WPF) o en aplicaciones Web mediante Silverlight.
- Librerías para integrar el reconocimiento facial en aplicaciones iOS.
- Librerías para integrar el reconocimiento facial en aplicaciones Java.
- Librerías para integrar el reconocimiento facial en aplicaciones móviles Android.
- Controles de usuario que posibilitan abstraer al programador de la gestión de cámaras y extracción de características faciales, permitiendo la integración en tiempo récord de la tecnología (WF, WPF, Silverlight, Android, C++, iOS, HTML5).
- Aplicación de activación de licencias de la tecnología.
- Documentación completa de todo el producto.

6.3. TECNOLOGÍA DEL PRODUCTO[34]

La tecnología de reconocimiento facial de **FacePhi** es un sistema altamente tolerante a las siguientes situaciones:

- La tolerancia en la posición del modelo es +/- 15˚ en cada dirección.
- La Identificación Es Posible Aun Cuando Se Presente La Oclusión parcial del rostro.
- El sistema es a los cambios faciales normales en la presentación personal del modelo ejemplo: crecimiento de la barba o cambio de estilo de peinado.
- La Tecnología FacePhi no se ve afectada uso de gafas (excepto gafas de sol).
- El reconocimiento se lleva a cabo aun con Cambios moderados de luz.

La tecnología **FacePhi** emplea algoritmos de última generación relacionados con la localización de rostros y ojos y la codificación de características únicas e intransferibles del rostro.

Los requerimientos mínimos de calidad e imagen para reconocimiento facial son:

- El rostro debe ser completamente visible en la imagen
- Distancia mínima entre iris de 40 píxeles (recomendado 70 píxeles)
- La resolución de cámara recomendada es de 640x480 @ 30 fps (VGA)
- La resolución mínima es de 640 x 480 @ 24 fps
- Se recomienda usar cámaras con enfoque y/o iris automático, así como con compensación de contraluces.

[34] FacePhi - http://tech.facephi.com/es/content/especificaciones/

6.4. REQUISITOS NECESARIOS PARA LA IMPLEMENTACIÓN

6.4.1. Módulo extractor y matcher Windows

PLATAFORMA	WINDOWS
Requerimientos Hardware Desarrollo (SDK)	**Recomendado**: - Intel Core i3 @ 3,07GHz - 4 Gbyte RAM **Mínimo**: - Intel Core 2 Duo @ 2,5 GHz - 2 Gbyte RAM
Requerimientos Hardware Despliegue (Runtime)	**Recomendado**: (*) - Intel Core i3 @ 3,07GHz - 2 Gbyte RAM **Mínimo:** - Intel Core 2 Duo @ 2,5 GHz - 1 Gbyte RAM
Cámara	**Recomendado**: - Resolución VGA (640x480) / 30 FPS - Enfoque automático (autofocus) / Iris automático - Compensación de contraluces (WDR o similar) **Mínimo:** - Resolución VGA (640x480) / 24 FPS
Sistema Operativo	Windows XP Windows Vista Windows 7 Windows 8 Windows Server 2003 Windows Server 2008 Windows Server 2012
Software	NET Framework 4 Microsoft Visual C++ 2012 x86 Redistributable (ó x64) Silverlight 5
Herramientas Desarrollo	Microsoft Visual Studio .NET, MonoDevelop, SharpDevelop, etc.
Programación	CLS-Complaint .Net (C#, VB .NET, Java, J#, F#, Managed C++, etc.) Microsoft Visual C++ Compiler 2012

Tabla 3. Requisitos del módulo extractor y del módulo matcher en Windows

6.4.2. Módulo extractor Android

PLATAFORMA	ANDROID
Requerimientos Hardware Desarrollo (SDK)	**Recomendado**: - Intel Core i3 @ 3,07GHz - 4 Gbyte RAM. **Mínimo**: - Intel Core 2 Duo @ 2,5 GHz. - 2 Gbyte RAM.
Requerimientos Hardware Despliegue (Runtime)	**Recomendado: (*)** - Arquitectura armeabi-v7 ó arquitectura x86 **Mínimo:** - Arquitectura armeabi-v7 ó arquitectura x86
Cámara	**Recomendado**: - Resolución VGA (640x480) / 30 FPS. - Enfoque automático (autofocus) / Iris automático. - Compensación de contraluces (WDR o similar). **Mínimo:** -Resolución VGA (640x480) / 24 FPS.
Sistema Operativo	Android (versión mínima API level 14, versión 4.0)
Software	Android SDK, Java SDK
Herramientas Desarrollo	Eclipse, IntelliJ
Programación	Java (Android)

Tabla 4. Requisitos del módulo de extracción en Android

6.4.3. Módulo extractor iOS

PLATAFORMA	iOS
Requerimientos Hardware Desarrollo (SDK)	**Recomendado**: - Intel Core i3 @ 3,07GHz - 4 Gbyte RAM. **Mínimo**: - Intel Core 2 Duo @ 2,5 GHz. - 2 Gbyte RAM.
Requerimientos Hardware Despliegue (Runtime)	- Arquitecturas arm64, armv7 o armv7s
Cámara	**Recomendado**: - Resolución VGA (640x480) / 30 FPS. - Enfoque automático (autofocus) / Iris automático. - Compensación de contraluces (WDR o similar). **Mínimo:** -Resolución VGA (640x480) / 24 FPS.
Sistema Operativo	iOS (versión mínima 7.1)
Software	-
Herramientas Desarrollo	XCode
Programación	Objective C

Tabla 5. Requisitos del módulo de extracción en iOS

6.5. COSTOS DE IMPLANTACIÓN Y MANTENIMIENTO DE LA APLICACIÓN

Los costos de implementación y mantenimiento para esta clase de aplicación, se pueden calcular entre el rango de 120.000 a 180.000 US anuales[35], en el caso particular de la UNAD la asociación con esta aplicación no presenta inconveniente alguno.

El administrador del sistema de la UNAD, indica que el software recomendado es muy compatible, y que permitiría con suma facilidad su incorporación sin presentar dificultad alguna.

Otra condición del costo emitido es que puede ser utilizada por un número indeterminado de usuarios a nivel nacional o internacional sin restricción de acceso, lo que hace que se convierta en una de las aplicaciones que ofrece las mejores condiciones facilitando el uso en todos los sentidos.

6.6. EFECTOS DE LA IMPLEMENTACIÓN DE LA APLICACIÓN

Es importante anotar que aun que la implantación de este sistema requiere de una inversión inicial la cual debe ser contemplada por la parte financiera de la institución, el beneficio que conlleva la implementación de este tipo de técnicas de autenticación para garantizar el usuario verdadero es principalmente académico, lo que hace pensar que la relación costo-beneficio sea apropiada y acorde con lo que se desea obtener a favor de los estudiantes y la universidad en su calidad de aprendizaje. Y por supuesto teniendo en cuenta otros puntos de vista estos procedimientos de actualización pueden ser interpretados como un incremento en el costo de mantenimiento de los sistemas de autenticación, pero se debe comprender que al innovar en un método diferente para el acceso de estudiantes, docentes y administrativos, se estará a la vanguardia de la seguridad, minimizando los riesgos y aumentando el control informático en la institución.

[35] Información recopilada en entrevista telefónica con el Ingeniero Mauricio Murcia representante de la empresa FacePhi MIB – Technology Solutions http://mibtechsolution.com/reconocimiento.html

6.6.1. ORGANIZACIONAL Y PERSONAL

Otra de las adecuaciones necesarias en el momento de implementar este tipo de tecnologías es el encargarse de realizar la respectiva captura de las imágenes de los estudiantes, docentes, administrativos y todo aquel personal que tendrá contacto directo con la plataforma ocasionando un aumento de la capacidad de almacenamiento en sus bases de datos, debido a que una imagen ocupa generalmente más de espacio de almacenamiento que una palabra.

Además es necesaria la capacitación y comunicación de los cambios que se presentaran en la nueva forma de ingreso a la plataforma, además de la capacitación a los encargados del manejo del sistema quienes estarán al frente de la información almacenada en las bases de datos y deben contar con la idoneidad para su manejo.

Para la instauración del nuevo sistema la universidad debe desarrollar, difundir y desplegar, toda la publicidad necesaria sobre la nueva técnica de ingreso tanto en su página de internet como en las inducciones que se realizan a los estudiantes, indicándoles la correcta forma de autenticarse, con las respectivas recomendaciones como evitar cambios físicos faciales ya que se tendría que realizar una nueva captura de la imagen del usuario por parte de la persona encargada de administrar el sistema matrículas en la universidad.

Por supuesto es importante aclarar que aun que este sistema es muy seguro y no afecta profundamente el desarrollo de las actividades en la plataforma si es un cambio que afecta a toda la comunidad universitaria, para evitar impactos negativos es necesario realizar inducciones y clarificar nuevas formas de acceso a la plataforma.

6.7. IMPLANTACIÓN DE LA APLICACIÓN EN LA PLATAFORMA.

6.7.1 REQUERIMIENTOS DEL SISTEMA PARA LA APLICACIÓN

Antes de realizar la compra e instalación de la aplicación FacePhi, al sistema de autenticación a la plataforma, se debe corroborar que los requerimientos tanto de software como de hardware que posee la universidad son los necesarios e indicados para lograr una efectividad en el momento de su implementación, ya que la falta de alguna de las especificaciones que se nombraron puede ocasionar un colapso en su aplicación y ejecución en el momento de ingresar al campus.

6.7.2. PRUEBA PILOTO DE EFECTIVIDAD Y EFICIENCIA

Una vez se haya verificado lo recomendado en el ítem anterior, se debe iniciar con una prueba piloto donde se corrobora en una plataforma alterna que despliegue todo lo que se encuentra en la original, verificando su correcto funcionamiento en el momento de la autenticación, iniciando con la captura de las imágenes de los usuarios y su asignación de login de acceso, siendo estas almacenadas en las bases de datos, de esta forma se podrá comprobar que la aplicación no presenta fallas para su uso e ingresando de forma aleatoria en diferentes ciudades de la ciudad o del país, comprobando su efectividad y eficiencia de autorización de acceso a la plataforma de aprendizaje.

6.7.3. PERIODO DE PRUEBA

Se considera un tiempo de prueba prudente de aproximadamente doce (12) meses para corroborar que la aplicación **FacePhi** no presenta fallas en su ejecución por medio de la web y el ancho de banda que internet requiere para ser utilizado en el momento de la comparación de las imágenes almacenadas con la del usuario final, lo que permitiría su acceso a la plataforma.

6.8. CONCLUSIÓN DE LA PROPUESTA

Luego del estudio cuidadoso y metódico de las opciones disponibles en el mercado, la aplicación FacePhi fue elegida como la más adecuada y recomendada, siendo la que cumple de la mejor manera con las necesidades evidenciadas en cuanto a la identificación de los miembros de la comunidad universitaria.

Se propone un plan de implantación de este sistema biométrico para mejorar sustancialmente la protección de acceso a la plataforma de aprendizaje, estableciéndolo definitivamente como un nuevo método de control de acceso pero teniendo en cuenta que por la variedad de usuarios y diferentes condiciones en que será utilizado el mismo requerirá de adecuaciones, ajustes y soporte técnico lo que será proveído por el fabricante de la aplicación.

CONCLUSIONES

El método actual de autenticación empleado en la universidad, no brinda la adecuada seguridad de acceso a la plataforma de aprendizaje, debido al escaso nivel de seguridad, lo que permite fácilmente la suplantación de los estudiantes, lo que conlleva, que el desarrollo académico de las actividades sea por parte de éstos y por ende se reflejará en el bajo nivel académico.

Con la aplicación de la técnica de biometría basada en las venas de la mano, ésta proporciona un mayor rango de seguridad tanto física como lógica, debido a que este patrón está basado en la huella de distribución de las venas que cada persona posee; esta tecnología consiste en ubicar la mano sobre el lector sin necesidad de tener el contacto físico, manteniendo en completa asepsia el dispositivo para el siguiente usuario, visualizando las venas en un color oscuro debido a que la hemoglobina contenida en la sangre, absorberá dicha luz. Atenidos a este principio, es muy sencillo indicar que será muy complicado el poder falsificar este patrón, debido a que muchos de los vasos sanguíneos que presenta cada individuo no es repetido en ningún otro.

El sistema biométrico recomendado es el FacePhi, una vez realizado su análisis de compatibilidad y descrito en el cuerpo del documento actual, se observa que cumple con los requerimientos indispensables para ser utilizado dentro de una plataforma de aprendizaje, debido a su eficiencia y efectividad, necesaria para elevar el nivel de seguridad de acceso del estudiante (a la plataforma) ya que se identificará al verdadero usuario en el momento de la captura de la imagen para la autenticación de acceso.

Llegar a contar con sistemas biométricos para control de entrada y salida o cualquier tipo de acceso, hoy en día es muy necesario, como se observó se encuentran muchos sistemas biométricos como el de huella dactilar, iris, voz, firma, geometría de las manos, y biometría de las venas, pero se escogió el de

reconocimiento facial o de rostro por ser uno de los que más está incursionando, fortaleciendo y avanzando su investigación de tal forma que esta técnica sea cada vez más efectiva.

Existen diversas técnicas de medición biométrica, que han sido utilizadas en el transcurso del tiempo, desde la impresión de huella dactilar en papel, empleada para las transacciones comerciales en la antigüedad, hasta la medición de las venas humanas para la seguridad de ingreso a lugares físicos, o protección de la información de hoy en día, y gracias a la aplicación de éstas técnicas es posible que no se presente las suplantaciones aumentando de esta forma la seguridad de acceso y garantizando un mejor nivel académico en los estudiantes de la universidad.

La seguridad física como lógica de la informática y la búsqueda de nuevos sistemas de seguridad que fortalezcan y prohíban el fácil ingreso a sistemas o instituciones a nivel mundial de individuos no deseables, se hace que con la aplicación de estas técnicas se logre evitar la suplantación de la identidad de las personas que puedan causar daños de cualquier tipo, que ha sido una de las prioridades por parte de las instituciones u organizaciones las que han visto que la biometría humana es considerada hoy en día como una solución factible a la difícil situación que se presenta frente al tema de seguridad, al ser considerada como de carácter natural y difícil de ser imitable por tratarse de características, rasgos y gestos propias que cada persona tiene en su anatomía.

El método de reconocimiento facial, es una de las técnicas que ofrece más y mejores garantías para su aplicación, siendo el más opcionado dentro de los recomendados para la implementación en la plataforma virtual de aprendizaje, debido a sus bajos costos de adquisición, mantenimiento, efectividad y garantía en seguridad de acceso permitida por la biométrica.

Después de pasar por la memorización de las contraseñas, el porte de tarjetas y otras que se ha recordado, hoy en día nos enfrentamos a uno de los mayores desafíos que la sistematización en línea ha creado, como lo es la autenticación FIDO (Fast Identification Online), que significa Estándar Abierto de Autenticación, este estándar fue creado para que cualquier dispositivo habilitado con FIDO, tenga una interfaz con una amplia de seguridad en línea", donde se ofrecerá una muy buena experiencia sin el uso de contraseñas o palabras claves, presentando una muy buena fortaleza ante el phishing.

CRONOGRAMA

	MES 1																				MES 2									
ACTIVIDADES A REALIZAR	**SEMANA 1**					**SEMANA 2**					**SEMANA 3**					**SEMANA 4**					**SEMANA 5**					**SEMANA 6**				
Lectura y observaciones por el director																														
Correcciones sugeridas por el director																														
Reestructuración del proyecto																														
Levantamiento de la información en el CEAD																														
Recopilación de la información para el análisis																														
Obtención de resultados																														
Presentación de resultados en el proyecto																														
Lectura del proyecto y posible aprobación - asesor																														
Culminación del proyecto																														

RECOMENDACIONES

Una vez implementado el sistema de reconocimiento facial implementar jornadas para capacitación a los usuarios del sistema para optimizar el manejo del mismo, de acuerdo a los cambios requeridos por esta tecnología y por supuesto a los cuidados necesarios para que el sistema mantenga las mejores condiciones.

Como ya se ha descrito las condiciones existentes en cuanto a la seguridad de la información son las adecuadas sin embargo al hacer el cambio tecnológico sería conveniente también revisar las circunstancias actuales, identificar y subsanar las debilidades que se puedan encontrar para así evitar el acceso a la información institucional de personal no autorizado.

En cuanto a la aplicación de este sistema de identificación lo más recomendable es que los usuarios del sistema cuenten con sus equipos de cómputo que cumplan con las siguientes especificaciones básicas: un procesador Intel Centrino, Core 2, o AMD CON 1GHz, Sistema Operativo Windows 8, 7, iOS, o, Linux, Cámara video resolución VGA 640x480 pixeles y compensación de contraluces.

Para los usuarios del sistema sería recomendable tener en cuenta que el dispositivo de captura, en este caso se habla de la cámara digital con que cuente el ordenador que esté empleando, se encuentre en óptimas condiciones de limpieza o para el caso de dispositivos externos tener en cuenta que tanto el cable como la conexión sea la indicada y se encuentre en perfectas condiciones físicas.

REFERENCIAS

AWARE. (2014). SOFTWARE BIOMÉTRICOS. Obtenido de http://www.aware.com/es/biometrics/index.html?gclid=CNrooqLd0cUCFQgRHwodpp8AGg

BORBÓN Sanabria, J. (2011). Buenas prácticas, estándares y normas. REVISTA .SEGURIDAD, DEFENSA DIGITAL, Obtenido de: http://revista.seguridad.unam.mx/numero-11/buenas-pr%C3%A1cticas-est%C3%A1ndares-y-normas.

Carreño, I. (27 de 11 de 2012). *METODOLOGÍA UNAD APRENDIZAJE AUTÓNOMO AUTOAPRENDIZAJE*. Obtenido de http://es.slideshare.net/ivon1980/metodologa-unad-aprendizaje-autnomo-autoaprendizaje

Cesar Tolosa Borja, Álvaro Giz Bueno, “Sistemas Biométricos”, Disponible en internet:http://www.dsi.uclm.es/asignaturas/42635/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

CSIRT. (21 de agosto de 2014). Centro de Seguridad TIC de la Comunitat Valenciana. Obtenido de NMAP 6: Listado de comandos: http://www.csirtcv.gva.es/sites/all/files/downloads/NMAP%206_%20Listado%20de%20comandos.pdf

Camelo, L. (23 de 02 de 2010). SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA. Obtenido de http://seguridadinformacioncolombia.blogspot.com/2010/02/marco-legal-de-seguridad-de-la.html

Carlos Andrés Madrigal González, J. L. (03 de 2007). DISEÑO DE UN SISTEMA BIOMÉTRICO DE IDENTIFICACIÓN USANDO SENSORES CAPACITIVOS PARA HUELLAS DACTILARES. Obtenido de http://www.scielo.org.co/pdf/rfiua/n39/n39a02

Casals, J. S. (01 de 07 de 2013). BIOMETRÍA APLICADA A LA SALUD Y A LA SEGURIDAD. Obtenido de http://www.investigacionyciencia.es/blogs/tecnologia/20/posts/biometra-aplicada-a-la-salud-y-a-la-seguridad-11242

César Tolosa Borja, Á. G. (s.f.). SISTEMAS BIOMÉTRICOS. Obtenido de http://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

Copyright. (2004). PLATAFORMA BIOMÉTRICA HOMINI. Obtenido de http://www.homini.com/new_page_5.htm

Copyright. (23 de 02 de 2009). BIENVENIDOS A BIOIDENTIDAD. Obtenido de http://www.bioidentidad.com/

Copyright. (06 de 2013). REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. Obtenido de NUESTRA HUELLA: http://www.registraduria.gov.co/rev_electro/2013/rev_elec_junio/revista_junio2013.html

COLCOB. (05 de 05 de 2015). ULTIMA HORA! ENTRO EN VIGENCIA LA NUEVA LEY DE PROTECCION DE DATOS PERSONALES. Obtenido de http://www.colcob.com/web1/servicios-a-la-industria/item/82-ultima-hora-entro-en-vigencia-la-nueva-ley-de-proteccion-de-datos-personales.html

Copyrigth, D. d. (15 de 12 de 2011). LEY ESTATUTARIA 1266 DE 2008 . Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

D.C, ©. P. (01 de 05 de 2009). Ley 1273 de 2009 Nivel Nacional . Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

D.C., ©. P. d. (27 de 07 de 2000). Ley 603 de 2000 Nivel Nacional. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960

D.C., ©. P. d. (30 de 07 de 2009). Ley 1341 de 2009 Nivel Nacional . Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3691

Distancia, U. N. (s.f.). *METODOLOGÍA DE ESTUDIO*. Obtenido de Campus Virtual: http://estudios.unad.edu.co/metodologia-de-estudio

DUCKTOOLKIT. (2015). Welcome to DuckTolkit. DURIVA. (1 de Marzo de 2015). Diplomado de Informatica Forense Duriva. Obtenido de Fuente: Penetration Test consultado de: https://www.duriva.com/wp-content/uploads/2011/07/Diplomado-de-Informatica-Forense-Duriva.pdf

ESPAÑOL, E. p. (2012). Gestión de Seguridad de la Información. Obtenido de ISO27000.es: http://www.iso27000.es/sgsi.html

Esteban Saavedra lopez, Ph.D, CEO Opentelematics Internacional Bolivia, biometría y patrones para la identificación humana, Disponible en internet: http://www.slideshare.net/estebansaavedra/biometria-y-atrones-para-laidentificacion-humana

Flores, M. E. (25 de 10 de 2010). METODOLOGÍA DE LA INVESTIGACIÓN. Obtenido de http://www.slideshare.net/eugeniarodriguezflores2/metodologa-de-la-investigacion-5550178

González, E. (07 de 2005). INTRODUCCIÓN A LOS BIOMÉTRICOS. Obtenido de http://www.tress.com.mx/boletin/julio2005/biometricos.htm

Globedia, Biometría por ADN "Huella Genética", Disponible en internet: http://co.globedia.com/biometria-adn-huella-genetica

Grupo Atenea, Biometría informe tecnológico sectorial,

Disponible en internet: http://www.ateneadigital.es/revistaatenea/revista/PDF/Documentos/Documento_650.pdf

Gross, M. (16 de 09 de 2010). PENSAMIENTO IMAGINATIVO. Obtenido de http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa

HEREDIA, M. S. (18 de 11 de 2009). METODOLOGÍA DE LA INVESTIGACIÓN. Obtenido de http://www.monografias.com/trabajos58/metodologia-investigacion/metodologia-investigacion2.shtml

Idatzia, E. M.-k. (27 de 03 de 2012). SISTEMAS FÍSICOS Y BIOMÉTRICOS DE SEGURIDAD. Obtenido de http://recursostic.educacion.es/observatorio/web/eu/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

IDENTIFICACIÓN BIOMÉTRICA LA CLAVE ES LA HUELLA . (03 de 02 de 2012). Obtenido de http://www.cyza.com.co/WebSite/Files/PUBLICACION%20CYZA%20VOLUMEN%201.pdf

Julián, G. (11 de 09 de 2013). TU HUELLA ES LA ENTRADA AL SMARTPHONE. Obtenido de http://www.xataka.com/moviles/tu-huella-es-la-entrada-al-smartphone-asi-funciona-el-sensor-biometrico-del-nuevo-iphone-5s

López, V. C. (12 de 05 de 2015). DERTAS DE LA HUELLA. Obtenido de http://bibliotk.gdl.up.mx/ceup/huella.pdf

Madrid, U. C. (s.f.). UN ESTUDIO ANALIZA LA EFICACIA DE LA IDENTIFICACIÓN BIOMÉTRICA POR LAS VENAS DE LAS MANOS. Obtenido de http://portal.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/biometria_vascular

Medina, M. C. (2010). TIPOS DE INVESTIGACIÓN. Obtenido de http://www.monografias.com/trabajos59/tipos-investigacion/tipos-investigacion.shtml

Meyer, D. B. (13 de 09 de 2006). LA INVESTIGACIÓN DESCRIPTIVA. Obtenido de http://noemagico.blogia.com/2006/091301-la-investigacion-descriptiva.php

Misfud, E. (27 de 04 de 2012). SISTEMAS FÍSICOS Y BIOMÉTRICOS DE SEGURIDAD. Obtenido de http://recursostic.educacion.es/observatorio/web/es/cajon-de-sastre/38-cajon-de-sastre/1045-sistemas-fisicos-y-biometricos-de-seguridad

NEO-SISTEM. (s.f.). CAMARAS DE SEGURIDAD. Obtenido de http://camarasdeseguridad.over-blog.net/pages/accesos-biometricos-definicion-5930945.html

Novenca Security Systems, Biométricos-Una Introducción, Disponible en internet:

http://www.novenca.com/site/index.php?option=com_content&view=article&id=165&Itemid=122

NICOLAS LOPEZ PEREZ, J. J. (2012). TECNICAS DE BIOMETRIA BASADAS EN PATRONES FACIALES DEL SER. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/11059/2738/1/0053682L864.pdf

Nicolás, J. M. (19 de 07 de 2011). SIR FRANCIS GALTON, EL HOMBRE CAPAZ DE MEDIRLO TODO. Obtenido de http://scientiablog.com/2011/07/19/sir-francis-galton-el-hombre-capaz-de-medirlo-todo/

Pablo Pérez, E. Á. (12 de 2011). ESTUDIO SOBRE LAS TECNOLOGÍAS BIOMÉTRICAS APLICADAS A LA SEGURIDAD. Obtenido de file:///C:/Users/Nevardo/Downloads/informe_biometria_final.pdf

Peña, J. J. (2009). DISEÑO METODOLÓGICO. Obtenido de http://virtual.funlam.edu.co/repositorio/sites/default/files/DisenoMetodologico.pdf

Peña, J. J. (s.f.). DISEÑO METODOLÓGICO PRELIMINAR. Obtenido de http://www.uniatlantico.edu.co/uatlantico/sites/default/files/docencia/facultades/pdf/ciencias-juridicas/guia%20_monografia_diseno_metodologico.pdf

RESERVADOS, D. (02 de 2010). BIOMETRÍAS Y NORMAS. Obtenido de https://www.itu.int/net/itunews/issues/2010/01/05-es.aspx

RESERVADOS, D. (2015). SOFTWARE RELOJ EN LÍNEA Y RELOJ BIOMÉTRICO. Obtenido de https://es.shiftplanning.com/timeclock/

RENIEC. (2012). SERVICIO DE VERIFICACIÓN BIOMÉTRICA - SVB. Obtenido de http://www.reniec.gob.pe/portal/pdf/05_svb.pdf

Rios, M. C. (28 de 04 de 2013). SISTEMAS BIOMÉTRICOS. Obtenido de http://es.slideshare.net/matutexmat/trabajo-biometria

R., M. A. (01 de 2013). *TUTORIAL EDUCACIÓN A DISTANCIA EN LA UNAD* . Obtenido de -APRENDIZAJE-AUTÓNOMO Y AUTOAPRENDIZAJE: http://es.slideshare.net/moiseschavezpsic/tutorial-educacin-a-distancia-en-la-unadaprendizajeautonomo-y-autoaprendizaje

Sánchez, M. A. (2008). SISTEMA BIOMETRICO DE RECONOCIMIENTO DE HUELLASDIGITALES. Obtenido de: http://webcache.googleusercontent.com/search?q=cache:http://repositorio.ute.edu.ec/bitstream/123456789/5634/1/34215_1.pdf

Sensores Ópticos, Disponible en internet:http://www.itescam.edu.mx/principal/sylabus/fpdb/recursos/r34716.PDF

SERNA, A. (25 de 08 de 2013). BIOMETRÍA, EL ARTE DE MEDIR AL SER HUMANO PARA IDENTIFICARLO . Obtenido de http://www.lapatria.com/en-domingo/biometria-el-arte-de-medir-al-ser-humano-para-identificarlo-41761

Tecnologías Biométricas Aplicadas a la Seguridad,

Disponible en internet: http://www.slideshare.net/serweb/biometria-desarrollo-practica

UMANICK TECHNOLOGIES, S. (10 de 07 de 2013). APLICACIONES Y USOS DE LAS TECNOLOGÍAS BIOMÉTRICAS. Obtenido de http://www.umanick.info/2013/07/aplicaciones-y-usos-de-las-tecnologias.html

UNAM. (2013). BIOMETRÍA INFORMÁTICA. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/clasificaciontipo.html

UNAM, Facultad de Ingeniera, Clasificación de los sistemas biométricos, Disponible en internet: http://redyseguridad.fip.unam.mx/proyectos/biometria/clasificacionsistemas/capturaretina.html

UNAM, Facultad de Ingeniera, Clasificación de los sistemas biométricos,Disponible en internet: http://redyseguridad.fip.unam.mx/proyectos/biometria/clasificacionsistemas/capturamano.html

UNAM, Ingeniería, U. -F. (s.f.). Biometría Informática . Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/biometria/fundamentos/antecedentes.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, Mirian del Carmen Benavides, Francisco Solarte. (2012). Módulo riesgos y control informático. Bogota: Datateca UNAD.

UNAD. GONZALEZ, Y. C. (2013). Fundamentos de seguridad de la información Bogota: datateca UNAD. Universidad de la República, facultad de Ingeniería, “Proyecto Aguará, reconocimiento de Caras”, Disponible en internet: http://iie.fing.edu.uy/investigacion/grupos/biometria/proyectos/aguara/descargas/documenta_aguara_v1.0.pdf

Verdugo, w. (05 de 10 de 2010). INVESTIGACION DESCRIPTIVA. Obtenido de http://www.slideshare.net/wenceslao/investigacion-descriptiva-5366924

Websites, G. (s.f.). BIOMETRÍA. Obtenido de http://www.goit.cl/biometria.html

Werner, S. D. (s.f.). APLICACIÓN DE NUEVAS TECNOLOGÍAS AL SISTEMA

ELECTORAL. Obtenido de BIOMETRÍA Y VOTO ELECTRÓNICO: http://www.monografias.com/trabajos82/biometria-y-voto-electronico/biometria-y-voto-electronico2.shtml

ANEXOS

ANEXO A.

1. CIRCULAR 01 de Diciembre 15 del 2000[36]

DERECHOS DE AUTOR

El derecho de autor es una forma de propiedad privada que reconoce una protección jurídica especial al autor como creador de una obra literaria o artística, entendida como tal, toda expresión personal de la inteligencia manifestada en forma perceptible y original.

A esos efectos, la Dirección Nacional de Derecho de Autor, Unidad Administrativa Especial adscrita al Ministerio del Interior, en desarrollo de su objeto de brindar asesoría general en materia de derecho de autor y derechos conexos o afines a éste; ejercer la inspección y vigilancia sobre las sociedades de gestión colectiva de los mencionados derechos; inscribir en el registro las obras literarias y artísticas, los contratos y actos vinculados con el derecho de autor y los derechos conexos; propender por la difusión y la promoción de esa rama de la propiedad intelectual; y fijar las políticas gubernamentales, que en torno a esa disciplina jurídica, requiere nuestro país, se permite ilustrar a las sociedades comerciales y civiles en el cumplimiento de la Ley 603 del 27 de julio de 2000, por la cual se modifica el artículo 47 de la Ley 222 de 1995, que establece como una de las obligaciones de los representantes legales de las sociedades, incluir dentro de su informe de gestión, el grado de cumplimiento de la legislación referente al derecho de autor, en los siguientes términos:

[36] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13959#0

"Artículo 1º. El artículo 47 de la Ley 222 de 1995, quedará así:

"Artículo 47. Informe de gestión. El informe de gestión deberá contener una exposición fiel sobre la evolución de los negocios y la situación económica, administrativa y jurídica de la sociedad.

"El informe deberá incluir igualmente indicaciones sobre:

1. Los acontecimientos importantes acaecidos después del ejercicio.
2. La evolución previsible de la sociedad.
3. Las operaciones celebradas con los socios y con los administradores.
4. El estado de cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la sociedad.

"El informe deberá ser aprobado por la mayoría de votos de quienes deban presentarlo. A él se adjuntarán las explicaciones o salvedades de quienes no lo compartieren.

"Artículo 2º. Las autoridades tributarias colombianas podrán verificar

El estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación también se evadan tributos."

Según la disposición legal, corresponde a los representantes de las sociedades comerciales o civiles elaborar dentro de su informe de gestión un panorama del cumplimiento de las normas de propiedad intelectual, específicamente, del derecho de autor.

En consideración a lo señalado por la Ley 603 de 2000, y de conformidad con el marco de protección cimentado por los acuerdos internacionales y la normatividad colombiana vigente en materia de derecho de autor, esta Dirección ha advertido la relevancia de emitir unas recomendaciones de orden práctico a fin de que sean tenidas en cuenta por parte de las sociedades, en los siguientes términos:

1. El principio fundamental del derecho de los creadores de obras literarias y artísticas, tales como programas de computador, bases de datos, libros, obras fotográficas, obras audiovisuales, obras musicales, etc., consiste en que toda utilización de aquellas requiere ser autorizada de manera previa y expresa por sus autores o legítimos titulares;

2. Las interpretaciones o ejecuciones de los artistas, las fijaciones sonoras de los productores fonográficos y las emisiones de los organismos de radiodifusión (radio y televisión) se encuentran protegidas como derechos conexos al derecho de autor. Tales prestaciones requieren de la respectiva autorización por parte de sus legítimos titulares para poder ser utilizadas;

3. Para hacer uso de obras protegidas por el derecho de autor o de las interpretaciones o ejecuciones de artistas intérpretes o ejecutantes, de las grabaciones fonográficas y de las emisiones de los organismos de radiodifusión, protegidas por los derechos conexos al derecho de autor, es necesario contar con las autorizaciones debidamente soportadas en contratos de licencia de uso, para así entender dichas utilizaciones como legales;

4. Para la adquisición de derechos de autor, de obras realizadas mediante encargo por parte de las sociedades, bien sea mediante contratos de prestación de servicios o bajo contratos laborales, es necesario que se observen las formalidades prescritas por el artículo 183 de la Ley 23 de 1982, que establece que la transferencia de los derechos, vía cesión, debe constar en escritura pública o en documento privado con diligencia de reconocimiento de firma y contenido ante notario (artículo 183 de la Ley 23 de 1982);

5. Para que los contratos, en virtud de los cuales se negocia la adquisición o uso de derechos de autor o de derechos conexos, tengan efectos ante terceros, deben ser inscritos en el Registro Nacional de Derecho de Autor

de la Unidad Administrativa Especial Dirección Nacional de Derecho de Autor; sin embargo, la omisión de este requisito no invalida la negociación entre las partes (artículo 183 Ley 23 de 1982 y artículo 6 de la Ley 44 de 1993);

6. la sociedad hace uso de obras musicales, aún en el ámbito privado, se encuentra obligada a cumplir con el pago por concepto de comunicación pública de la música ante las sociedades que administran, recaudan y distribuyen dichos derechos, como son la Sociedad de Autores y Compositores de Colombia, SAYCO, y la Asociación Colombiana de Intérpretes y Productores Fonográficos, ACINPRO;

7. En materia de utilización de programas de computador (software), las sociedades deben contar con las respectivas licencias de uso para el número de equipos de computador permitidos por la licencia. Los usos o explotación de los programas deben ser no más que los autorizados expresamente en el contrato de licencia de uso y la licencia debe estar vigente al momento de la utilización de los programas;

8. Si la sociedad ha adquirido legalmente los derechos patrimoniales de autor sobre una obra, no le es dable desconocer los créditos de quién la creó, puesto que debe mencionarse el nombre del creador con cada utilización (paternidad); tampoco es posible entrar a modificar, mutilar, deformar o alterar el contenido de la obra (integridad), conforme a los postulados del derecho moral de autor de la obra;

9. La responsabilidad en materia de violaciones al derecho de autor y derechos conexos, está regulada en su parte civil, por el artículo 242 y ss. de la Ley 23 de 1982, que remite a las disposiciones del Código Civil en lo atinente a la indemnización por daños y perjuicios dentro del régimen de responsabilidad civil extracontractual (artículo 2.341). En lo pertinente a la

responsabilidad penal, se encuentra determinada por el artículo 51 y ss. de la Ley 44 de 1993 que señala penas de prisión e imposición de multas.

Tales sanciones, así como los trámites procesales jurídicos, se encuentran igualmente contemplados en los nuevos Código Penal y Código de Procedimiento Penal (Ley 599 y 600 de 2000 respectivamente), los cuales entrarán en vigencia en el mes de julio del año 2001.