DISEÑO DE UN SISTEMA DE RECONOCIMIENTO FACIAL COMO MEDIO DE CONTROL DE ACCESO BIOMÉTRICO MEDIADO POR TÉCNICAS DE INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA BASE DE SEGURIDAD DEL CEAD IBAGUÉ.

ING. JUAN MANUEL ALDANA PORRAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
IBAGUÉ - COLOMBIA
2018

DISEÑO DE UN SISTEMA DE RECONOCIMIENTO FACIAL COMO MEDIO DE CONTROL DE ACCESO BIOMÉTRICO MEDIADO POR TÉCNICAS DE INTELIGENCIA ARTIFICIAL COMO HERRAMIENTA BASE DE SEGURIDAD DEL CEAD IBAGUÉ.

JUAN MANUEL ALDANA PORRAS

Proyecto Aplicado como requisito para optar al título de:
Especialista en Seguridad Informática

Director (a):
PhD(c) Gabriel Mauricio Ramírez Villegas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
IBAGUÉ - COLOMBIA
2018

CONTENIDO

pág.

1 INTRODUCCIÓN 8

2 PROBLEMA DE INVESTIGACIÓN 10

2.1 Formulación del problema 11

3 JUSTIFICACIÓN 12

4 OBJETIVOS 15

4.1 Objetivo General 15

4.2 Objetivos Específicos 15

5 Marco referencial 16

5.1 Marco Conceptual 16

5.1.1 Seguridad Física. 16
5.1.2 Controles de acceso. 17
5.1.3 Detección de intrusos. 18
5.1.4 Reconocimiento Biométrico. 19
5.1.5 Diseño de un Sistema de Seguridad. 22

5.2 Marco teórico 23

5.2.1 Visión Computacional. 23
5.2.2 Librerías de Visión Computacional *OpenCV*. 25
5.2.3 Descriptores Imagen HOG. 32

5.3 MARCO LEGAL 36

5.3.1 Protección de la Información. 36
5.3.2 Ley Habeas Data. 37

6 Metodología 40

6.1 Tipo de Investigación 40

6.2 Población 40

6.3 Hipótesis 40

6.4 Operacionalización de las variables 40

6.5 Instrumentos de recolección de información 42

6.6 diseño y desarrollo 43

6.6.1 Sistema de Seguridad Física CEAD Ibagué 44
6.6.2 Sistema de detección de intrusos y control de acceso. 48

6.6.3 Selección y acondicionamiento del Algoritmo. 49
7 Resultados y Discusión.....55
7.1 Infografia desarrollo del proyecto 58
8 Conclusiones.....59
9 Referencias.....61
10 Anexo A.....66

FIGURAS

pág.

Figura 1. Ejemplos característicos Biométricas, a) Reconocimiento Facial, b) termografía facial, c)patrones oreja, diris, e) retina._____ 19
Figura 2. Ejemplo matriz espacio RGB _____ 24
Figura 3. Ejemplo de Visión Computacional, Detección de Objetos 3D_____ 25
Figura 4. Módulos librerías Dlib _____ 26
Figura 5. Ejemplo aplicación librería face recognition _____ 27
Figura 6. Ejemplo Face Land Mark._____ 28
Figura 7. Ejemplo SVM Lineal._____ 29
Figura 8. Ejemplo de Maquina de Vectores de Soporte, No Lineal _____ 30
Figura 9. Elemento procesador red neuronal_____ 31
Figura 10. Ecuación y ejemplo HOG _____ 32
Figura 11. Magnitud y orientación vector pixel HOG _____ 33
Figura 12. Rango de Orientación sin signo, con un sub rango de 9 intervalos __ 33
Figura 13. Ejemplo de Histogramas imagen _____ 34
Figura 14. Desplazamiento de bloques Histogramas imagen _____ 35
Figura 15. Imagen de 64x128, con un bloque de 16x16 y celdas de 8x8 pixeles 36
Figura 16. Ejemplo Matriz de Confusión._____ 41
Figura 17. Cámara Digital C310 HD WEBCAM. Toma de muestras _____ 43
Figura 18. Primera Planta - CEAD Ibagué. _____ 45
Figura 19. Ubicación del punto de acceso a la oficina de registro _____ 46
Figura 20. Vestíbulo principal - CEAD Ibagué _____ 46
Figura 21. Puerta de acceso a la sala del servidor central CEAD Ibagué _____ 47
Figura 22. Entrada a sala de tutores desde el vestíbulo Principal. _____ 47
Figura 23. Interior sala de tutores - CEAD Ibagué _____ 48
Figura 24. Diagrama algoritmo detección de rostros. _____ 49
Figura 25. Adquisición de imágenes y conversión en escala de grises. _____ 50
Figura 26. Descriptor HOG aplicado a una imagen de entrada. _____ 51
Figura 27. Detección de rostro_____ 51
Figura 28. Face Land Mark. Estimación de 68 puntos en un rostro. _____ 52
Figura 29. FaceLand Mark. _____ 52
Figura 30. Cuantificación de rostro – Deep Neuronal Network._____ 53
Figura 31, Detección final registrada por el algoritmo._____ 54
Figura 32. Organización elementos de pruebas y rostros autorizados._____ 55
Figura 33. Grafico del porcentaje de eficiencia de las variables dependientes establecidas. Sensibilidad 93%, especificidad98%, exactitud del 98%, precisión 91%._____ 57
Figura 34. Infografía desarrollo del proyecto. _____ 58
Figura 35. Gráfico de respuestas de formularios. Título de la pregunta: ¿Se han presentado incidentes relacionados con la seguridad física de los activos dentro de

las instalaciones del Centro (robo, daño de equipos, accesos no autorizados)?.. Número de respuestas: 20 respuestas. _____ 66
Figura 36. Gráfico de respuestas de formularios. Título de la pregunta: De ser afirmativa la anterior respuesta, ¿Cuál de las siguientes opciones se ajusta al tipo de incidente presentado? Marqué las que considere necesarias: Número de respuestas: 11 respuestas. _____ 67
Figura 37. Gráfico de respuestas de formularios. Título de la pregunta: ¿Con qué frecuencia se presentan estos incidentes de seguridad física? Número de respuestas: 10 respuestas. _____ 67

TABLAS

pág.

Tabla 1. Riesgos de seguridad relacionados con la disponibilidad, confidencialidad e integridad. 17
Tabla 2. Métodos de reconocimiento fácil según categorización. 22
Tabla 3 31
Tabla 4. Variables Independiente y dependiente. 41
Tabla 5. Formulas Tasa de detección, Tasa de Error, Exactitud y Precisión. 42
Tabla 6. Características Técnicas Equipo de pruebas. 43
Tabla 7. Categorización en correspondencia al tipo de detección realizada: 56
Tabla 8. Resultados finales variables independientes. 56
Tabla 9. Resultados Finales variables dependientes 57

1 INTRODUCCIÓN

En la actualidad, los sistemas de seguridad se estructuran buscando minimizar los riesgos a los cuales están expuestos los activos de una institución de cualquier índole, a partir de allí suele hacerse especial énfasis en la protección de la información que circula en ambientes digitales, configurando medidas de alto nivel alrededor del software, bases de datos y los medios de almacenamiento que conforman la infraestructura lógica de la misma.

El problema con algunas de estas implementaciones de seguridad es que descuidan los medios físicos encargados de procesar, transportar y almacenar dichos activos de información, lo cual, conlleva a generar espacios donde los riesgos potenciales asociados a la disponibilidad, integridad y confidencialidad aumentan de forma exponencial y la información contenida en estos elementos de hardware se ve comprometida.

Por consiguiente, dentro de la correcta articulación de un sistema de seguridad es necesario incorporar lineamientos que garanticen una adecuada protección de los activos claves que resguardan información sensible y de gran valor para sus propietarios. Así pues, uno de los principales medios utilizados para el control de acceso de cualquier tipo de personal dentro de las instalaciones físicas, es el control biométrico, este permite instaurar medidas con un alto nivel fiabilidad y a costos relativamente bajos.

De ahí, que es común encontrar dispositivos de acceso biométrico en muchos lugares, sobre todo porque estos se adaptan de forma específica a las necesidades de cada empresa. Para el caso particular del CEAD Ibagué[*], uno de los problemas que enfrenta en la actualidad es la carencia de controles de acceso a determinadas áreas de vital interés dentro de las instalaciones de la Universidad, lugares claves como la sala de los servidores, el ingreso a laboratorios y el acceso a la sala de tutores quedan en lugares de alcance público, donde se dificulta la labor personal de seguridad, sobre todo en horarios de alto flujo de personal.

[*] Centro de Educación Abierta y Distancia CEAD Es un componente organizacional de carácter universitario, articulado a un nodo, en el cual se desarrollan interrelaciones de índole académica y administrativa en forma reticular, para brindar oportunidades de socialización, formación, generación de conocimientos e interacción de estudiantes, cuerpo académico y comunidad, con el objeto de prestar servicios educativos con calidad y equidad social. [en línea] [citado el 12 de septiembre 2018]. Disponible en https://informacion.unad.edu.co/transparencia-y-acceso-a-la-informacion/acerca-de-la-unad/glosario/c

Así pues, se diseña un sistema de reconocimiento facial mediado por técnicas de inteligencia artificial que funcione en tiempo real y sea ubicado en sitios estratégicos en procura de salvaguardar los activos físicos de la universidad evitando accesos no autorizados adecuándose como complemento del sistema de seguridad actualmente implementado dentro del CEAD Ibagué.

2 PROBLEMA DE INVESTIGACIÓN

Actualmente la UNAD es la universidad más grande de Colombia, contando con alrededor de 100 mil estudiantes[1] en todo el territorio nacional, siendo así la primera mega universidad del país mediada por tecnologías de la información. No obstante, para el desarrollo de esta metodología virtual es necesario un despliegue tecnológico con una infraestructura enfocada en los servicios en línea (campus virtual).

A partir de allí, la seguridad de la información toma un rol crucial dentro de las actividades regulares de la UNAD, tal como lo expresa la Gerencia de Innovación y Desarrollo Tecnológico de esta misma universidad[2], la información institucional que se maneja a través de las redes, equipos y aplicaciones informáticas en general, representan un activo muy valioso para la universidad, el cual puede encontrarse expuesto a diversos riesgos, que de ser explotados causarían un impacto significativo en la continuidad de las funciones normales de la institución.

En ese orden de ideas, es necesario aclarar que la UNAD cuenta con varios centros a nivel nacional, todos reglamentados bajo los mismos lineamientos de seguridad[3], pero con recursos físicos limitados que pueden variar de un centro a otro; por lo cual no siempre se puede garantizar el cumplimiento a cabalidad de las normas establecidas para salvaguardar la información lógica que es procesada, almacenada y enviada por cualquiera de los activos propios de la misma.

Para el caso particular del CEAD Ibagué, se cuenta con una estructura de seguridad que podría asemejarse a un modelo de protección en profundidad, donde se tienen unas barreras administrativas y físicas que ofrecen cierta protección a los activos del centro frente riesgos. A pesar de ello se han presentado incidentes[4] de

[1] Universidad Nacional Abierta y a Distancia, La UNAD se constituye como la primera mega universidad pública en Colombia. Noticias UNAD [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://noticias.unad.edu.co/index.php/unad-noticias/todas/2362-la-unad-se-constituye-en-la-primera-megauniversidad-publica-de-colombia

[2] Gerencia de Innovación y Desarrollo Tecnológico. Seguridad de la Información. GIDT UNAD [en línea] [citado el 12 de septiembre 2018]. Disponible en https://gidt.unad.edu.co/seguridad-de-la-informacion

[3] Secretaria General. Política de seguridad de la información y gestión documental. GIDT [en línea] [citado el 12 de septiembre 2018]. Disponible en https://gidt.unad.edu.co/seguridad-de-la-informacion

[4] Anexo A. Encuestas

seguridad vinculados a robos y pérdida de información dentro de las instalaciones del centro.

Partiendo de la infraestructura física y del modelo de seguridad con que se cuenta actualmente en el CEAD Ibagué, se identifican limitaciones relacionadas a los sistemas de detección de intrusos y controles de acceso, esto debido a que dichas restricciones se llevan a cabo de forma manual por el personal de seguridad del centro, que se ve condicionado en relación a la cantidad de guardas disponibles y áreas físicas por controlar, sobre todo en momentos de gran afluencia de estudiantes y personal externo.

Por otra parte, determinados activos del centro no se encuentran correctamente resguardados en consonancia con los lineamientos de seguridad establecidos en la norma ISO 27002[5]; activos como el servidor de datos, sala de comunicaciones, sala de tutores y oficina de registro y control, no cuentan con una correcta política y sistema de control de accesos, uso de estaciones de trabajo y delimitación física de espacios, lo cual aumenta de forma significativa los riesgos asociados a la información almacenada, procesada y enviada desde esos activos.

Por todo lo anteriormente expuesto, se propone diseñar un sistema de seguridad biométrica basada en reconocimiento facial que permita llevar un control en tiempo real en puntos estratégicos dentro del CEAD, pudiendo discriminar entre el personal perteneciente a la Universidad (Estudiantes, personal académico y administrativo) y aquellos que no lo son, emitiendo una alerta correspondiente dentro del sistema interno de los vigilantes cuando se detecte un acceso no autorizado.

2.1 FORMULACIÓN DEL PROBLEMA

¿Es posible diseñar un sistema de seguridad biométrico (reconocimiento facial) mediado por técnicas de inteligencia artificial que permita llevar un control en tiempo real dentro de las instalaciones del CEAD Ibagué, que esté en capacidad de detectar personal no autorizado?

[5] El Portal de ISO27002. Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002. ISO27002.es [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.iso27000.es/iso27002.html

3 JUSTIFICACIÓN

Actualmente la información es uno de los activos más importantes con los que cuenta una empresa, de allí, que la seguridad asociada a esta tome un rol preponderante frente a las necesidades de la compañía de cara a garantizar la integridad, disponibilidad y confidencialidad de estos datos.

En consecuencia, es común que se invierta gran cantidad de recursos en procura de minimizar los riesgos asociados al procesamiento, envío y almacenamiento de la información, por lo cual se establecen medidas de seguridad orientadas a salvaguardar los activos digitales, tal como lo expone Harris[6] es común que las organizaciones fundamenten sus sistemas de seguridad en contramedidas de índole tecnológica, enfocadas en la protección digital de la información.

Por otra parte, si bien este tipo de medidas son necesarias, deben de estar acompañadas de un esquema de seguridad física cuyo objetivo es resguardar el personal, la información, instalaciones y cualquier activo de una compañía[7]. A pesar de ello, es habitual que la seguridad física no se encuentre dentro de la lista de prioridades en cuanto a la protección de información digital, de allí que los ambientes físicos y las instalaciones no se diseñen teniendo en cuenta determinados requerimientos de seguridad, prevaleciendo la comodidad y funcionalidad[8].

Por lo cual, las vulnerabilidades asociadas al procesamiento, envío y almacenamiento de la información, no se limitan de forma exclusiva a riesgos de índole digital; la integridad física de los elementos de hardware también se puede ver comprometida a causa de acciones deliberadas que conlleven a fraudes, vandalismo, sabotaje o robo.

---

[6] Harris, S. Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill. Citado por Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

[7] Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

[8] Harris. S. Op. cit.

Una muestra clara de este tipo de riesgos es el incidente ocurrido en el año 2014 en la empresa Coca Cola, la cual tuvo que afrontar procesos judiciales debido al robo de varias computadoras portátiles dentro de sus instalaciones, las cuales contenían información sensible acerca de más de 74000[9] empleados, proveedores y contratistas. Los demandantes acusaban a la compañía de negligencia debido a la falta de controles y un sistema de seguridad física insuficiente.

Así mismo, los riesgos asociados a este tipo de problemas no solo desencadenan daños o robos sobre los activos físicos, un ejemplo de ello es lo sucedido en el Departamento de defensa de los Estados Unidos en el año 2008, donde un empleado encontró una memoria USB en una de las áreas comunes de las instalaciones y procedió a revisarla en su computadora, a partir de allí se propago un virus por toda la red privada enviando información clasificada a servidores remotos en otros países[10].

Por todo esto, un buen procedimiento de seguridad debe integrar de forma holística aspectos relativos tanto a la seguridad digital como física de los activos, para ello la defensa en profundidad es un método que se ajusta a estos requerimientos; tal como lo plantea Hunter [11], la defensa en profundidad es un concepto usado para asegurar los activos y proteger la integridad del personal, mediante el uso de múltiples capas de protección. Si un atacante compromete una de las capas, aun tendría que penetrar capas adicionales para obtener acceso a los activos y llevar a cabo su cometido.

A partir de allí, uno de los aspectos primordiales dentro de un esquema de protección en profundidad es el control de acceso y sistema de detección de intrusos. Hunter[12] argumenta que la detección intrusos es imprescindible debido a que la conciencia del evento le permite a la organización responder y contener el incidente. permitiendo localizar donde ocurren las brechas y con qué frecuencia ayudando al equipo de seguridad a reducir vulnerabilidades

En ese orden de ideas y partiendo de la infraestructura física con la que cuenta el CEAD Ibagué, existen áreas de acceso público (visitantes) que concurren con tres sitios de vital importancia para el centro, la sala de servidores, las oficinas de registro

[9] Scott, M. COCA-COLA DATA BREACH HIGHLIGHTS IMPORTANCE OF LAPTOP SECURITY. . [en línea] [citado el 12 de septiembre 2018]. Disponible en: http://www.acfe.com/fraud-examiner.aspx?id=4294986501

[10] Lynn III, W. J. Defending a New Domain. . [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

[11] Hunter, D. Physical Security and Why It Is Important. Op. cit.

[12] Hunter, D.Physical Security and Why It Is Important. Ob. Cit.

y control y la sala de tutores, todos estos están al alcance de estas áreas públicas donde no existe un control claro de acceso o sistema de detección de intrusos que evite el paso de personal no autorizado.

Así pues, las falencias asociadas al sistema de seguridad física establecido dentro del CEAD, generan riesgos constantes sobre los activos de esta, por ello es necesario establecer una solución robusta que posibilite instaurar un control de acceso, estando en capacidad de monitorear en tiempo real los puntos clave dentro de la infraestructura física, pudiendo emitir alertas cuando personal no autorizado ingrese a estos sectores claves.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un sistema de seguridad biométrica que permita llevar un control de acceso y detección de intrusos en tiempo real de funcionarios y visitantes que circulan dentro de las instalaciones del CEAD Ibagué.

4.2 OBJETIVOS ESPECÍFICOS

- Identificar los activos de información de alto valor para la universidad y su ubicación dentro de las instalaciones del CEAD Ibagué
- Estimar el estado de riesgo actual de los activos de alto valor partiendo del sistema de seguridad implementado actualmente dentro del CEAD Ibagué.
- Establecer las condiciones de funcionamiento óptimas del sistema de control de acceso y detección de intrusos a partir del modelo biométrico de detección facial propuesto.
- Elaborar un algoritmo de detección e identificación de rostros mediado por técnicas de inteligencia artificial que cuente con una exactitud superior al 90%.

5 MARCO REFERENCIAL

5.1 MARCO CONCEPTUAL

5.1.1 Seguridad Física. La seguridad física hace referencia a las medidas y controles de acceso implementadas para proteger la infraestructura física de riesgos asociados a terceros (robo o modificación) o daños ocasionados por desastres naturales. Así pues, se puede hacer referencia a cualquier medio que contenga o haga parte de un sistema de información[13], bien sea un elemento de software, hardware o cualquier tipo de dispositivos de red.

Por otro lado, la constante evolución de la tecnología relacionada con él envió, procesamiento y almacenamiento de datos, trae consigo un crecimiento exponencial de las vulnerabilidades a las cuales están expuestos estos procesos. Hace solo algún tiempo, las computadoras eran elementos grandes y costosos que se mantenían en cuartos asegurados donde solo unas cuantas personas tenían acceso a estos [14]. Actualmente en las estaciones de trabajo es normal encontrar dispositivos móviles como laptops o smartphones que tienen acceso a la red interna de toda una compañía[15].

De allí, que las vulnerabilidades a las cuales están expuestas los activos de información dentro de una compañía no solo se limitan a ataques de tipo lógico, el tamaño[16] de los dispositivos de procesamiento y almacenamiento hace que la seguridad física, tome un rol preponderante frente al robo de equipos y dispositivos. La tabla 1 ilustra los principales riesgos a los cuales tiene que hacer frente una empresa en pro de mantener sus activos de información seguros.

---

[13] Nayak, U., & Rao, U. H. The InfoSec handbook: An introduction to information security [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://link.springer.com/book/10.1007%2F978-1-4302-6383-8

[14] Harris. S. Ob. Cit.

[15] Hunter. D. Ob. Cit.

[16] Oriyano, S. (Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley. Citado por Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

Tabla 1. Riesgos de seguridad relacionados con la disponibilidad, confidencialidad e integridad.

Riesgo	Descripción
Daño Físico	Disponibilidad
Robo	Disponibilidad e integridad
Ingreso no autorizado	Confidencialidad e integridad
Desastre natural	Disponibilidad
Intervención Humana (Vandalismo, sabotaje)	Disponibilidad y confidencialidad.
Emergencias (Fuego, humo, filtro de agua)	Disponibilidad

Fuente: Nayak, U., & Rao, U. H. (2014). The InfoSec handbook: An introduction to information security. Apress.

Por otra parte, existen elementos que se deben tener presentes al momento de diseñar un sistema de seguridad, uno de ellos es la locación física, para lo cual es indispensable contar con la información necesaria acerca de los riegos presentes y en qué tipo de incidente pueden desencadenar[17], de allí que aspectos como la visibilidad dentro de las instalaciones, los vecinos, rutas de acceso, trafico, población presente en el sector entre otras son datos relevantes que permiten fundamentar las decisiones tomadas a nivel administrativo en aras de establecer la correcta protección de los activos de información.

5.1.2 Controles de acceso. Los controles de acceso deben de plantearse como una política de seguridad alrededor de los activos involucrados directa o indirectamente con el procesamiento, uso o transmisión de información; así pues, es necesario proteger el acceso físico a cualquier terminal que esté conectado a la red interna de la empresa, cableado de red, servidores, suministro eléctrico entre otros.

Este tipo de protección parte de los principios básicos de disuasión, negación y detección los cuales implementados dentro de un sistema de protección en profundad permiten reducir los riesgos asociados a accesos no autorizados,

[17] Stewart, J., Chapple, M., & Gibson, D. (2012). Physical Security Requirements. In CISSP *Certified Information Systems* Security Professional study guide (6th ed., pp. 572-597,745-774). Indianapolis, IN USA: Wiley. Citado por Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

facilitando la toma de decisiones y ejecución de acciones de contingencia en caso de presentarse brechas de seguridad.

Igualmente, Hunter[18] hace énfasis en que toda organización debe contar con sistemas automatizados de control que permitan resguardar las instalaciones físicas, de ahí, que en un modelo óptimo de seguridad inicia con los controles administrativos, los cuales se convierten en la primera línea de defensa y culmina con el personal de la compañía, siendo este la última línea de defensa, limitando así la interacción directa de dicho personal con los atacantes. A partir de allí, toma gran importancia que estos controles sean el centro de atención al momento de sustentar e implementar medidas de seguridad administrativas[19].

Por otra parte, el uso de nuevas tecnologías aumenta la capacidad de monitorear continuamente el medio ambiente, en aras de detectar condiciones anormales y capturar información de interés, en tiempo real, brindando la oportunidad de reducir los costos de inspección al tiempo que se proporciona una mayor seguridad para el público[20], solventando las limitaciones sensoriales y de atención que puede llegar a tener cualquier personal encargado de seguridad.

5.1.3 Detección de intrusos. Los sistemas de detección de intrusos o IDS (por sus siglas en Ingles), agrupan gran cantidad de dispositivos capaces de detectar ingresos no autorizados[21] en áreas sensibles de la organización. Por lo general este tipo de dispositivos incluyen sensores volumétricos, sensores de contacto o vibración, sistemas de presión entre otros[22].

Por otra parte, el funcionamiento de este tipo de detección de intrusos debe de estar en capacidad de diferenciar cuando una persona está autorizada o no para estar en un lugar determinada de las instalaciones; de allí a que este tipo de sensores trabajen de forma conjunta con los sistemas de control de acceso, los cuales están estructurados en tres conceptos principales[23]: posesión (p. ej. Credencial de acceso), conocimiento (p. ej. pin de ingreso) y sistema biométrico (p. ej. Huella dactilar).

---

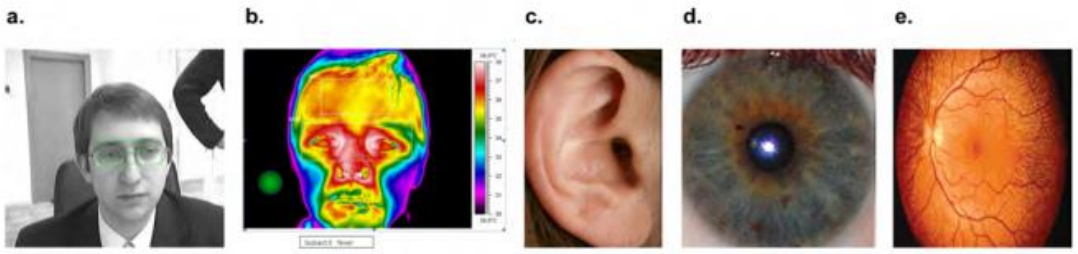
[18] Hunter. D. Ob. Cit.
[19] Stewart, J., Chapple, M., & Gibson, D. Ob. cit.
[20] Drago, A. Methods and Techniques for Enhancing Physical Security of Critical Infrastructures. [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.fedoa.unina.it/10532/1/PhDThesisAnnaritaDrago.pdf
[21] Ibid., pag 20.
[22] FENNELLY, Lawrence; PERRY, Marianna. Physical security: 150 things you should know. Butterworth-Heinemann, 2016. Pagina 75
[23] Drago. A. Ob. Cit., pag 18

Este tipo de integración permite entrar o salir al personal autorizado de áreas protegidas, no obstante, este tipo de sistemas presentan vulnerabilidades propias inherentes a las características propias de cada uno de ellos, por lo cual los enfoques de seguridad que cuentan con una conjunción de los tres conceptos principales tienen a suplir este tipo de vulnerabilidades.

5.1.4 Reconocimiento Biométrico. La biometría dentro del ámbito informático busca la aplicación de un conjunto de técnicas cuantificables que permitan realizar una identificación automática de los rasgos distintivos de una persona, de allí que características anatómicas como huellas dactilares, cara o iris y particularidades de comportamiento como habla, firma o patrones de escritura funcionen como identificadores biométricos o rasgos biométricos[24] que se utilizan primordialmente en sistemas de seguridad informática

Así pues, inicialmente se puede determinar que cualquier rasgo físico puede ser utilizado para tal fin, pero en pro de establecer condiciones ideales, este tipo de características deben de ser universales, distintivas, permanentes, medibles y cuantificables. Para tales fines, se han identificado un conjunto de rasgos que han sido ampliamente usados, tal como se ilustra en la Figura 1:

Figura 1. Ejemplos característicos Biométricas, a) Reconocimiento Facial, b) termografía facial, c)patrones oreja, diris, e) retina.



Fuente: SERRATOSA, Francesc. La biometría para la identificación de las personas. Universitat Oberta de Catalunya, 2008, p. 24.

[24] SERRATOSA, Francesc. La biometría para la identificación de las personas. Universitat Oberta de Catalunya, 2008, p. 8-20.

Por otra parte, es necesario establecer métodos que permitan cuantificar cualquier tipo de medida de escogida, por ello como lo plantea Sánchez[25]. "Las técnicas biométricas se basan en la medida directa o indirecta y su posterior análisis de un o un conjunto de rasgos (estáticos y/o dinámicos) del individuo para identificar automáticamente su identidad", a partir de allí se pueden identificar características propias de cada tipo de control biométrico[26].

Reconocimiento de voz[27], la voz del ser humano tiende a ser única e irrepetible y sus características difieren de una persona a otra, partiendo del tono y la frecuencia de esta; esto facilita el proceso de cuantificación de este tipo de señales, en aras del proceso de reconocimiento o autenticación de voz en sistemas de control biométrico, este tipo de medidas pueden requerir entornos controlados que faciliten la toma de datos y eviten la aparición de interferencias a causa de ruido.

Patrones de escritura[28], los patrones de escritura de un individuo tienden a ser un rasgo característico e irrepetible, lo que facilita su inclusión en sistemas de control a partir de la cuantificación de características como la presión aplicada al escribir, la orientación de las letras y el estilo de estas. Por otra parte, este tipo de control biométrico presenta limitaciones como medio de control de acceso, esto partiendo del *hardware* requerido para la toma de datos dispositivo (tableta *wacom* o similares).

Huella dactilar[29], este tipo de control biométrico parte de las características morfológicas propias de cada persona presentes en los pulpejos de ambas manos. Este tipo de control biométrico es ampliamente usado en la actualidad, su facilidad de uso y rapidez hacen que sea una opción viable para la mayoría de las empresas que buscan implementar este tipo de controles, los cuales se adaptan especialmente bien como medio verificación.

Reconocimiento de mano[30], las características morfológicas propias presentes en la mano de cualquier persona tienden a ser un rasgo característico e irrepetible, de allí que la distancia y ángulo de los dedos, cartílagos y huesos sean medidas cuantificables y comparables.

---

[25] SANCHEZ, Angel. Aplicaciones de la visión artificial y la biometría informática. Dykinson SL,(Madrid), URJC, 2005.
[26] Nayak, U., & Rao, U. H. The InfoSec handbook: An introduction to information security. Ob. cit
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.

Reconocimiento de Iris[31], este tipo de controles biométricos parte del reconocimiento del área que se encuentra alrededor de la pupila, las cuales presentan características distintivas, incluso pueden variar de un ojo a otro para una misma persona, por lo cual son especialmente útiles cuando se necesita implementar un nivel de seguridad alto.

Reconocimiento de Retina[32], los controles biométricos basados en reconocimiento de retina parten de los patrones generados por las venas presentes en los ojos humanos, específicamente en el área que refleja las imágenes provenientes del exterior. Este tipo de patrones varían de forma significativa de una persona a otra lo cual lo convierte en un medio de autenticación seguro, que en contraprestación necesita condiciones de toma de información específicos y es sensible a cambios en el medio (lumínicos).

Patrones Vasculares de la mano[33], al igual que con el reconocimiento de retina, en la mano de un ser humano hay presentes todo un sistema vascular, los cuales tienen rasgos característicos e irrepetibles, igualmente la toma de datos provenientes de la mano es relativamente sencilla y el hardware involucrado no es costoso.

5.1.4.1 Reconocimiento Facial. El reconocimiento facial es uno de métodos de detección biométrica más estudiados en los últimos años, la constante necesidad de controlar el flujo de personas en grandes terminales aéreas, terrestres, eventos sociales entre otros, ha permitido avances significativos en esta área, igualmente la cara, como el elemento central del reconocimiento se adapta fácilmente a este tipo de contextos en donde se hace necesario contar con una característica que de un nivel de fiabilidad aceptable, que sea un rasgo común y que normalmente se puede adquirir sin presentar grandes problemas.

Así pues “La cara es uno de los rasgos biométricos más aceptables debido a que es el rasgo biométrico más común usado por los humanos a la hora de reconocer a las personas, así como las interacciones visuales diarias.” [34], a partir de allí que en la actualidad muchas de las investigaciones que se llevan a cabo en distintas

[31] Nayak, U., & Rao, U. H. The InfoSec handbook: An introduction to information security. Ob. cit
[32] Ibid.
[33] Ibid.
[34] Ribalta, Albert Solé. Seguridad en los sistemas biométricos. Openlibra. [en línea] [citado el 12 de septiembre]. Disponible en https://openlibra.com/es/book/seguridad-en-los-sistemas-biometricos

universidades a nivel mundial, centren esfuerzos en lograr la eficiencia con la que actualmente las máquinas llevan a cabo este proceso.

5.1.4.3 Métodos de reconocimiento facial. La visión computacional es un área creciente dentro de las ramas de la inteligencia artificial, pero uno de los tópicos más trabajados es el de reconocimiento facial, este ha adquirido un nivel de madurez tal que es implementado en muchas aplicaciones del día a día, bien sea mediante las redes sociales, asistentes personales (smartphone) o el computador, por ello la cantidad de literatura disponible para este tópico es bastante amplia, para lo cual se va a delimitar a tres categorías propuestas por Zhao et al[35], métodos holísticos, basados en características y los híbridos, tal como se muestra en la Tabla 2.

Tabla 2. Métodos de reconocimiento fácil según categorización.

Método	**Trabajos**
Holísticos	*PCA – Principal Component Analisis* *Eigenface* *Probabilistic eingenface* *Fisherfaces/sibspace LDA* *SVM*
Basados en características	*Puere geometry methods* *Dynamics link architecture* *Hiddern Markov model* *Convolution Neural Network*
Híbridos	*Modular eigenface* *Hybrid LFA* *Shape-normalized* *Component-based*

Fuente: Pereyra, Pamela. Reconocimiento Facial Mediante Imágenes Estereoscópicas Para Control de Ingreso Universidad de Buenos Aires

5.1.5 Diseño de un Sistema de Seguridad. Un sistema de seguridad físico debe de establecerse partiendo de los indicadores claves de desempeño (KPIs)[36], los cuales

[35] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. Face recognition: A literature survey. ACM computing surveys. [en línea] [citado el 12 de septiembre]. Disponible en http://mplab.ucsd.edu/~marni/Igert/Zhao_2003.pdf

[36] Santander Peláez,M. . Measuring effectiveness in Information Security Controls. SANS Institute [en línea] [citado el 12 de septiembre]. Disponible en https://www.sans.org/reading-room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398.

deben ser revisados y monitoreados de forma periódica[37]. Estos indicadores o métricas suelen variar de una organización a otra dependiendo de las necesidades específicas respecto a la seguridad del sistema

Por otro lado, este tipo de métricas le brindan a la compañía una forma de cuantificar el rendimiento[38] de un sistema de seguridad en función de los objetivos planteados para el mismo. Este tipo de información le permite a la compañía tomar decisiones en pro de establecer mejores controles de seguridad en relación con los recursos utilizados.

Del mismo modo, es común que este tipo de métricas estén asociadas a indicadores claros y medibles, por ejemplo, el número de delitos ocurridos, tiempos de detección, tiempos de recuperación, impacto sobre el sistema, costos económicos relacionados con el delito afrontado, entre otros; gracias a esto, la empresa está en condiciones de identificar los riesgos y tomar medidas al respecto, bien sea para mitigarlos, transferirlos o aceptarlos, tal como lo expone Irwins[39], la organización debe tener un conocimiento claro de cómo todos los riesgos pueden llegar a afectar de forma conjunta a la empresa, para crear un perfil de riesgo

En consecuencia, estas métricas dotan a una empresa de la información necesaria para modelar un sistema de seguridad que vaya de la mano con los requerimientos propios de sus dependencias, los cuales deben establecerse a partir de un sistema de seguridad en profundidad, mediante el uso de múltiples capas de protección, garantizando así que, si un atacante compromete una de las capas, aun tendría que penetrar capas adicionales para obtener acceso a los activos y llevar a cabo su cometido[40].

5.2 MARCO TEÓRICO

5.2.1 Visión Computacional. Es una rama de la inteligencia artificial dedicada a capturar información del mundo real y darle un sentido propio que las máquinas

[37] Wailgum, T. Metrics for Corporate and Physical Security Programs . [en línea] [citado el 12 de septiembre]. Disponible en http://www.csoonline.com/article/2118531/metrics- budgets/metrics-for-corporate-and-physical-security-programs.html.
[38] Harris. S. Ob. Cit.
[39] Irwin, S. (2014, September 8). Creating a Threat Profile for your Organization. [en línea] [citado el 12 de septiembre]. Disponible en https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492
[40] Hunter. D. Ob. Cit.

puedan entender, esto con el fin de dotarlas de percepción41 pudiendo extraer información relevante de su entorno brindándoles la capacidad de tomar decisiones en base a ello, de una forma más estricta podríamos decir que la visión artificial o comprensión de imágenes describe la deducción automática de la estructura y propiedades de un mundo tridimensional, posiblemente dinámico, bien a partir de una o varias imágenes bidimensionales de ese mundo[42].

Existen muchos métodos de captura de datos y dispositivos destinados a ello, podemos establecer de manera general que la "percepción" de un computador puede ser mucho más amplia y abarcar métodos más complejos y hasta cierto punto más eficientes que los que alcanza un ser humano; no obstante, uno de los medio más comunes y simples de dotar a un computador de percepción es el uso de cámaras digitales.

A partir de allí en cada una de estas cámaras el plano de imagen se subdivide en una rejilla rectangular[43] de un determinado número de píxeles que guardan información relevante a el entorno (formas, colores, texturas, etc.), que no son más que un conjunto de datos numéricos que se procesa de manera específica buscando que esta rejilla de píxeles, se conviertan en una percepción real (con sentido) del entorno, la figura 2 ilustra la matriz generada a partir de la cuantificación de datos dentro de una imagen.

Figura 2. Ejemplo matriz espacio RGB

Fuente: Autor

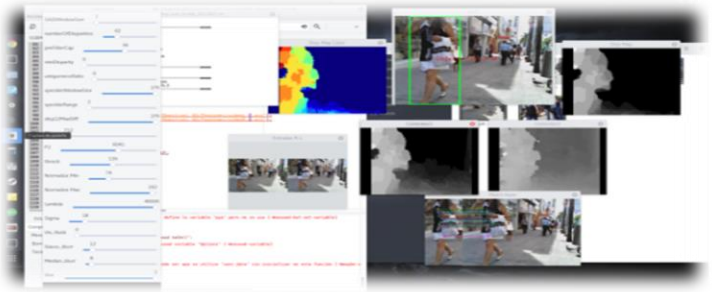
[41] RUSSELL, Stuart J.; NORVIG, Peter. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited,, 2016.
[42] NALWA, Vishvjit S. A guided tour of computer vision. Addison-Wesley Longman Publishing Co., Inc., 1994.
[43] RUSSELL, Stuart J.; NORVIG, Peter. Ob. Cit.

Tal como lo expone Gonzales [44], segmentar una imagen digital significa dividirla en zonas disjuntas e individualizadas. Es decir, consiste en diferenciar los diversos objetos y dónde se encuentran del fondo, que puede ser más o menos complejo, de la imagen. Así pues, para llevar a cabo esta segmentación de manera eficaz se debe tener en cuenta que una segmentación basada únicamente en atributos locales y de bajo nivel, tales como el brillo y el color, es un proceso expuesto a muchos errores.

Por otra parte, para delimitar los bordes asociados a los objetos de una forma fiable, es necesario incorporar también conocimiento de alto nivel referido a los tipos de objetos que se espera encontrar en una escena[45], para a partir de allí involucrar filtros de pre y pos-procesamiento con el fin de facilitar este tipo de procesos.

5.2.2 Librerías de Visión Computacional *OpenCV*. Es un conjunto de librerías[46] de código abierto dedicadas a la visión computacional, con una gran cantidad de algoritmos enfocados a la solución de problemas relacionados con esta área, *OpenCV* está estructurado de manera modular, lo que significa que incluye gran cantidad de librerías compartidas y estáticas, que ofrecen operaciones básicas de procesamiento de imágenes, análisis estructural, análisis de movimiento, reconocimiento del modelo, reconstrucción 3d entre otras, la figura 13 ilustra el funcionamiento de este tipo de librerías en la detección de objetos tridimensionales.

Figura 3. Ejemplo de Visión Computacional, Detección de Objetos 3D



Fuente: Autor.

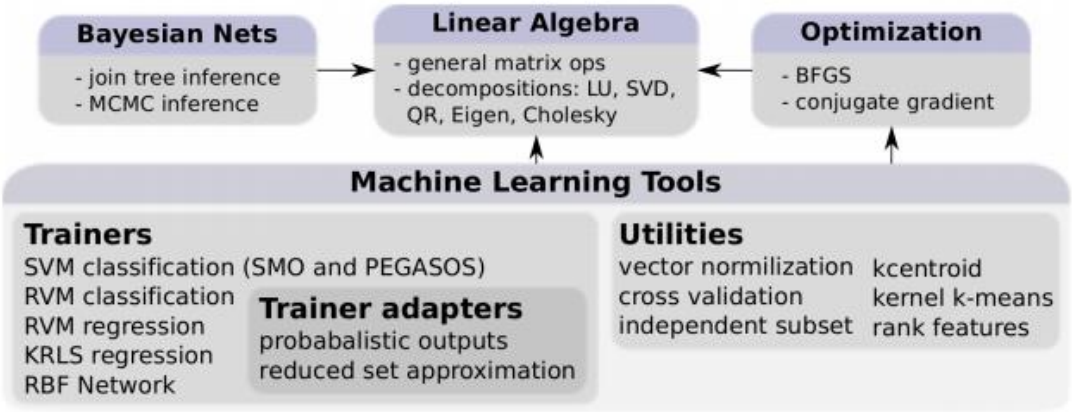
[44] MARCOS, A. González, et al. Técnicas y algoritmos básicos de visión artificial. Universidad de la Rioja, [en línea] [citado el 12 de septiembre]. Disponible en https://publicaciones.unirioja.es/catalogo/online/VisionArtificial.pdf
[45] RUSSELL, Stuart J.; NORVIG, Peter. Ob. Cit.
[46] OpenCV. OpenCV Documentation. [en línea] [citado el 12 de septiembre de 2018]. Disponible en https://docs.opencv.org/3.4/

5.2.2.1 Módulos *OpenCV*. Dentro de las características que se encuentran en estas librerías[47], hay módulos dedicados a áreas específicas de la visión computacional, brindado funciones relacionadas manipulaciones básicas, transformación de imágenes, filtros, operadores de convulsión, funciones de interfaz de usuario y algoritmos destinados a la descripción, detección y comparación de puntos clave (*keypoints*) en las imágenes entre otros.

5.2.2.2 Librerías *Dlib*. Es una librería de código abierto enfocada en ofrecer herramientas relacionadas con las diferentes técnicas de inteligencia artificial, King[48] describe *Dlib-ml* como una biblioteca de código abierto, dirigida tanto a ingenieros como a investigadores, cuyo objetivo es proporcionar un entorno igualmente rico para el desarrollo de software de aprendizaje automático en el lenguaje C ++.

De este modo, las librerías contienen la implementación de varias técnicas de inteligencia artificial; en consecuencia, están compuestas de forma modular y contienen cuatro elementos principales, módulo de Redes Bayesianas, módulo de algebra linear, módulo de optimización y módulo de herramientas de aprendizaje de máquina. La figura 4, ilustra las técnicas implementadas en cada uno de los módulos enunciados anteriormente.

Figura 4. Módulos librerías Dlib

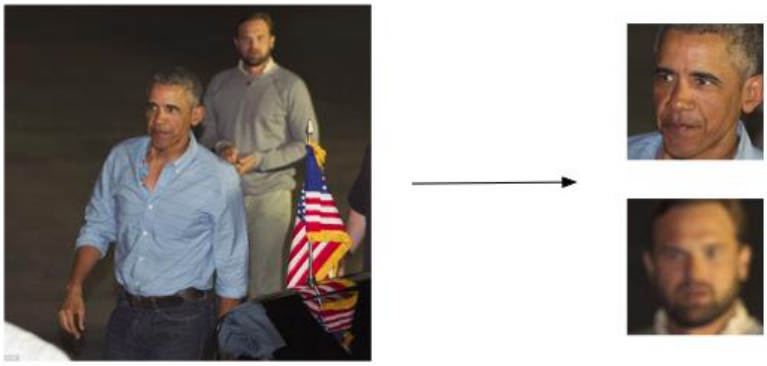


Fuente: KING, Davis E. Dlib-ml: A machine learning toolkit. Journal of Machine Learning Research, 2009, vol. 10, no Jul, p. 1755-1758

[47] OpenCV. Ob. Cit.
[48] KING, Davis E. Dlib-ml: A machine learning toolkit. *Journal of Machine Learning Research*, 2009, vol. 10, no Jul, p. 1755-1758.

5.2.2.3 Librería *Face Recognition*. Es una librería creada por Adam Geitgey con el fin de facilitar el desarrollo de aplicaciones que necesiten hacer uso de técnicas de inteligencia artificial encaminadas a la detección e identificación de rostros. Dicha implementación utiliza como base los algoritmos estructurados en las librerías *DLib*; su objetivo principal tal como lo plantea su autor[49] es reconocer y manipular rostros desde Python o desde la línea de comandos con la biblioteca de reconocimiento facial más simple del mundo. La figura 5 ilustra el funcionamiento de las librerías.

Figura 5. Ejemplo aplicación librería *face recognition*



FuenteKING, Davis E. Dlib-ml: A machine learning toolkit. Journal of Machine Learning Research, 2009, vol. 10, no Jul, p. 1755-1758.

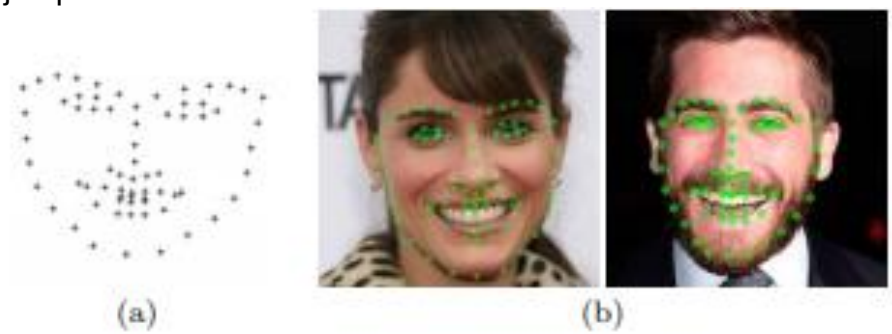
5.2.2.4 *Face Land Mark*. En el campo de la visión computacional, los puntos de referencia faciales juegan un papel determinante en las tareas de detección e identificación de rostros. Por otra parte, muchos de los métodos de análisis dedicados a la identificación de expresiones faciales, estimación de posición de la cabeza e identificación de emociones entre otras, se fundamentan sobre esta técnica.

Wu[50] indica que los algoritmos FLM apuntan a identificar los puntos clave de referencia dentro de un rostro, los cuales pueden ser puntos dominantes que describen la ubicación única de un componente facial (por ejemplo, esquina del ojo)

[49] GEITGEY, Adam. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning. Medium. https://medium. com/@ ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78, 2016.
[50] WU, Yue; JI, Qiang. Facial Landmark Detection: A Literature Survey. International Journal of Computer Vision, 2017, p. 1-28.

o un punto interpolado que conecta estos puntos dominantes alrededor de los componentes faciales y el contorno facial. La figura 6 ilustra este punto.

Figura 6. Ejemplo *Face Land Mark.*



Autor: WU, Yue; JI, Qiang. Facial Landmark Detection: A Literature Survey. International Journal of Computer Vision, 2017, p. 1-28.

La detección de este tipo de características es un desafío por varias razones. Primero[51], el aspecto facial cambia significativamente a través de sujetos bajo diferentes expresiones faciales y la posición de la cabeza. En segundo lugar, las condiciones ambientales como la iluminación afectan la apariencia de las caras en las imágenes faciales. En tercer lugar, la oclusión facial por otros objetos u oclusión propia debido a la posición de la cabeza dan lugar a una toma de características incompleta.

Wu[52] clasifica los algoritmos de detección de puntos faciales en tres categorías principales: métodos holísticos, métodos del Modelo Local Restringido (CLM) y los métodos basados en la regresión. Dichos modelos difieren en la forma de utilizar la apariencia facial. Los métodos holísticos construyen explícitamente modelos para representar la apariencia facial global y la información de formas. Los CLM aprovechan explícitamente el modelo de forma global, pero construyen los modelos de apariencia local. Los métodos basados en regresión capturan implícitamente información de forma y apariencia facial.

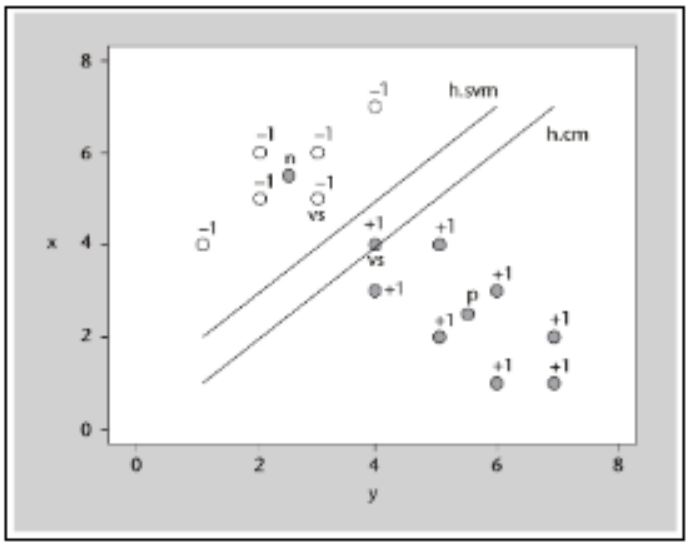
5.2.2.5 *Support Vector Machine*. Las máquinas de vectores de soporte o SVM (*support vector machine*, por su siglas en inglés) son un método de clasificación basado en la minimización del riesgo estructural(SRM) a partir de la teoría del aprendizaje estadístico; las cuales funcionan como clasificadores en multitud de ámbitos, para el contexto general de este trabajo se complementan con los vectores de características obtenidos a partir de los descriptores HOG, mapeando los

[51] Ibid
[52] Ibid

puntos de entrada a un espacio de características de una dimensión mayor, para luego encontrar el híper plano que los separe y maximice el margen entre las clases.

Colmenares[53] define las máquinas de vectores de soporte son un algoritmo de optimización que escoge el hiperplano con margen máximo de entre todos los posibles hiperplanos que separan los ejemplos positivos de los negativos (el que tiene la misma distancia a los ejemplos positivos que a los negativos). Describe el hiperplano a partir de los llamados vectores de soporte. Estos suelen ser los puntos más cercanos al hiperplano y los que lo definen. En la figura 7, h.svm corresponde al hiperplano de margen máximo que encontrarán las SVM para este conjunto y los vectores de soporte están marcados con vs.

Figura 7. Ejemplo SVM Lineal.



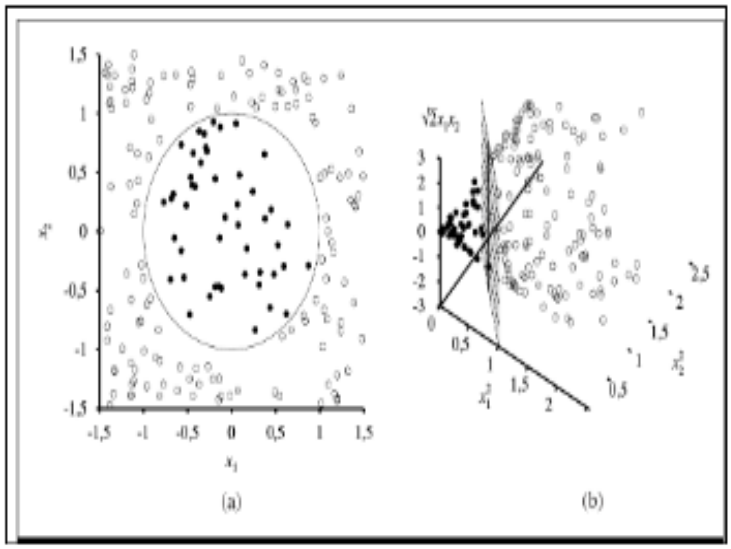
Fuente: Colmenares, G. Análisis Multivariante y Aplicaciones. Universidad de Los Andes Mérida-Venezuela. [en línea] [citado el 20de septiembre 2018]. Disponible en http://webdelprofesor.ula.ve/economia/gcolmen/postgrado2.html

5.2.2.6 Máquina de Vectores No Lineal. Aunque las máquinas de vectores de soporte son lineales en su forma básica, pueden ser transformadas en una forma dual[54], en la que los ejemplos de entrenamiento sólo aparecen dentro de productos escalares, permitiendo el uso de funciones núcleo para producir clasificadores no lineales, como se observa en la figura 8.

[53] Colmenares, G.Análisis Multivariante y Aplicaciones. Universidad de Los Andes Mérida-Venezuela. [en línea] [citado el 20de septiembre 2018]. Disponible en http://webdelprofesor.ula.ve/economia/gcolmen/postgrado2.html

[54] RUSSELL, Stuart J.; NORVIG, Peter. Inteligencia Artificial: un enfoque moderno. 2004.

Figura 8. Ejemplo de Maquina de Vectores de Soporte, No Lineal



Fuente: RUSSELL, Stuart J.; NORVIG, Peter. Inteligencia Artificial: un enfoque moderno. 2004.

Por otra parte, para algunos conjuntos de entrenamiento no es deseable obtener un hiperplano perfecto[55], es preferible permitir algunos errores en el conjunto de entrenamiento para obtener “mejores” hiperplanos. Esto se consigue con una variante del problema de optimización, llamada margen flexible, donde la contribución a la función objetivo de la minimización del margen y los errores en el conjunto de entrenamiento se pueden balancear a través de un parámetro normalmente llamado C.

5.2.2.7 Redes Neuronales Artificial.Las Redes Neuronales Artificiales están inspiradas en el funcionamiento del cerebro humano y con el pasar de los años se han destacado por tener unas características propias muy útiles en la resolución de determinados tipos de problemas, en especial en el reconocimiento y clasificación de patrones, que es para lo que se utilizaran en este sistema; por otra parte, en la tabla 3 se ilustran algunas de las características propias de las redes neuronales son:

[55] Ibid

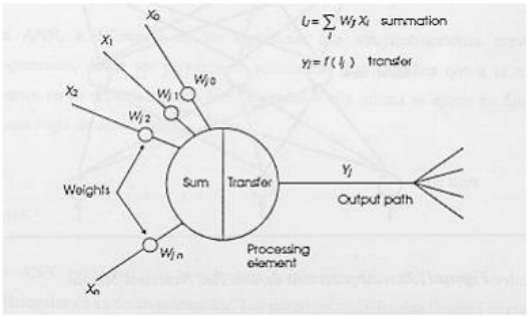
Tabla 3. Caracteristicas Redes Neuronales

Aprender	Generalizar	Abstraer
Adquirir el conocimiento de una cosa por medio del estudio, ejercicio o experiencia. Las ANN pueden cambiar su comportamiento en función del entorno. Se les muestra un conjunto de entradas y ellas mismas se ajustan para producir unas salidas consistentes.	Extender o ampliar una cosa. Las ANN generalizan automáticamente debido a su propia estructura y naturaleza. Estas redes pueden ofrecer, dentro de un margen, respuestas correctas a entradas que presentan pequeñas variaciones debido a los efectos de ruido o distorsión.	Aislar mentalmente o considerar por separado las cualidades de un objeto. Algunas ANN son capaces de abstraer la esencia de un conjunto de entradas que aparentemente no presentan aspectos comunes o relativos

Fuente: OLABE, Xabier Basogain. Redes neuronales artificiales y sus aplicaciones. Publicaciones de la Escuela de Ingenieros 101pp, 1998.

Olabe[56] expone que En las Redes Neuronales Artificiales, ANN, la unidad análoga a la neurona biológica es el elemento procesador, PE (*process element*). Un elemento procesador tiene varias entradas y las combina, normalmente con una suma básica. La suma de las entradas es modificada por una función de transferencia y el valor de la salida de esta función de transferencia se pasa directamente a la salida del elemento procesador. La figura 9 ilustra el funcionamiento del elemento procesador de una red neuronal artificial.

Figura 9. Elemento procesador red neuronal



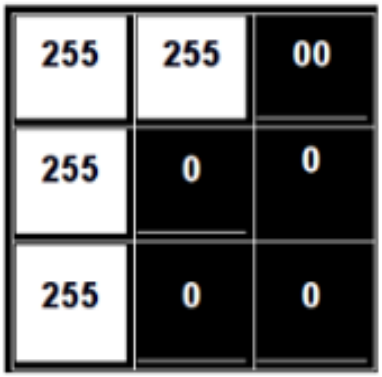
Fuente: OLABE, Xabier Basogain. Redes neuronales artificiales y sus aplicaciones. Publicaciones de la Escuela de Ingenieros 101pp, 1998.

[56] OLABE, Xabier Basogain. Redes neuronales artificiales y sus aplicaciones. Publicaciones de la Escuela de Ingenieros 101pp, 1998.

5.2.3 Descriptores Imagen HOG. Los descriptores de imagen se utilizan dentro de las técnicas de visión computacional con el fin de poder cuantificar la información dentro de las imágenes, para ello los descriptores de imagen HOG (*Histogram Oriented Gradient*) por sus siglas en inglés, utilizan la gradiente en cada uno de sus píxeles como información primaria[57], esta gradiente puede definirse como el cambio intensidad de una imagen en cierta dirección, este cambio está definido por un vector de dos valores, intensidad y dirección.

El cálculo del gradiente para cada uno de los pixeles se realiza partiendo de la diferencia de intensidad de los píxeles adyacentes, tanto verticales como horizontales, tal como se muestra en la figura 10.

Figura 10. Ecuación y ejemplo HOG



$$dx = I(x+1, y) - I(x-1, y)$$

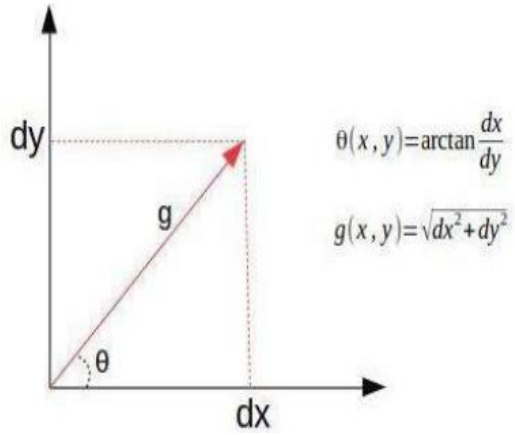
$$dy = I(x, y+1) - I(x, y-1)$$

Fuente: DALAL, Navneet; TRIGGS, Bill. *Histograms of oriented gradients for human detection. En Computer Vision and Pattern Recognition*, 2005. CVPR 2005. IEEE Computer Society Conference on. IEEE, 2005. p. 886-893

Para el caso anterior la diferencia tanto horizontal como vertical del pixel central de la imagen es 255, por otra parte, podemos graficar dx y dy en un plano de coordenadas, lo cual nos permitirá encontrar un vector cuya magnitud g y orientación θ corresponden con las del píxel en cuestión, tal como se ilustra en la figura 11.

[57] Valveny, E., Varnell, M., Lopez, A. Detección de Objetos, Universidad Autónoma de Barcelona, [en línea] [citado el 12 de septiembre 2018]. Disponible en https://www.coursera.org/learn/deteccion-objetos/home/welcome

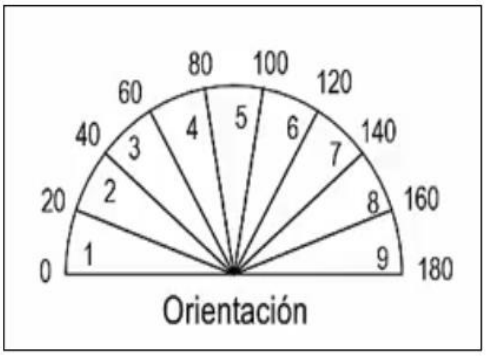
Figura 11. Magnitud y orientación vector pixel HOG



Fuente: Autor

Una vez calculada la información local de cada uno de los pixeles, se necesita agrupar esta información para obtener un descriptor de imagen, para ello se divide la imagen en un número fijo de celda, cada una de ellas conformada por un determinado número de píxeles y una orientación establecida dentro de un rango determinado[58], que puede ir de 0 a 180º(sin signo) o de 0 a 360º (con signo) y esta a su vez va dividida dentro de un sub rango de grados definidos en intervalos como se muestra en la figura 12.

Figura 12. Rango de Orientación sin signo, con un sub rango de 9 intervalos



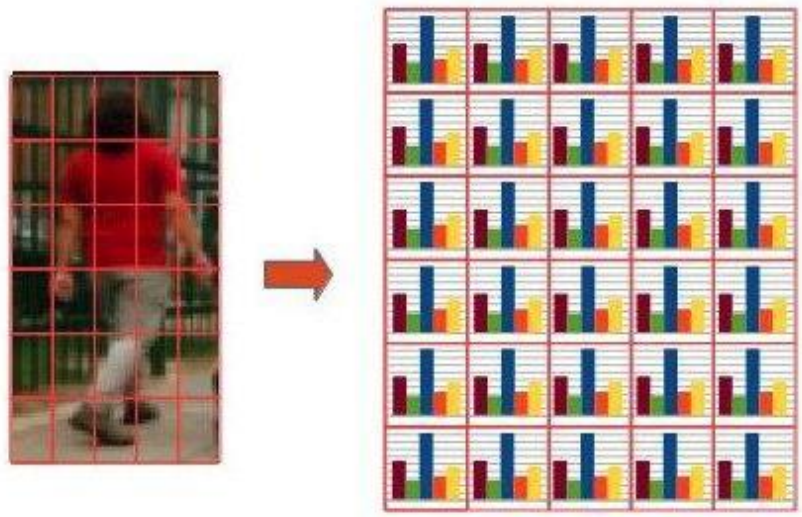
Fuente: DALAL, Navneet; TRIGGS, Bill. Histograms of oriented gradients for human detection. En Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on. IEEE, 2005. p. 886-893

[58] Valveny & López. Ob. cit.

A partir de estos intervalos y para calcular el histograma de orientaciones en cada una de las celdas se acumulan orientaciones similares en un intervalo definido, para ello se calcula el factor de asociación[59], el cual determina a que intervalo corresponde cada orientación, este factor es la diferencia entre el la distancia una orientación determinada a el centro de dicho intervalo por el rango de dicho intervalo, esto por otra parte nos permite corregir errores al momento de asignar orientaciones con valores similares, permitiendo asignar estos valores a dos intervalos

Una vez encontrado el correspondiente histograma de cada una de las celdas, esto brindara información relevante acerca de los cambios de gradiente dominante en cada celda[60], como se muestra en la figura 7, posteriormente cada una de estas celdas se establece una agrupación de celdas con un tamaño determinado, al cual se le llamara bloque, en él se concatenan los histogramas de sus celdas correspondientes en un vector y se normalizara por valor establecido con el fin de evitar variaciones de iluminación en la imagen, para lo cual se divide cada uno de los componentes del vector por su norma L2.

Figura 13. Ejemplo de Histogramas imagen

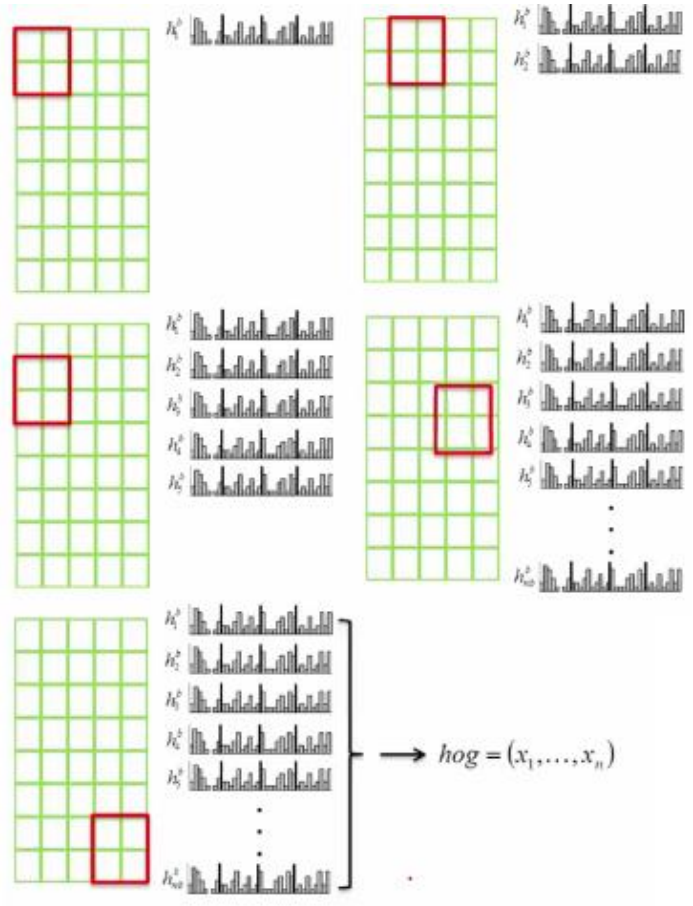


Fuente: Autor

[59] Ibid
[60] Ibid

Posteriormente cada uno de estos bloques se desplaza de manera horizontal y vertical a partir de un número determinado de celdas, por lo general de a una, la figura 14 ilustra la concatenación de cada uno de los histogramas encontrados en los bloques[61] da como resultado final el descriptor de la imagen.

Figura 14. Desplazamiento de bloques Histogramas imagen



Fuente: DALAL, Navneet; TRIGGS, Bill. Histograms of oriented gradients for human detection. En Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on. IEEE, 2005. p. 886-893

Al culminar el proceso global del descriptor, se obtiene una cuantificación a partir de la gradiente de todos los pixeles presentes en la imagen en cuestión, la figura 15 ilustra el resultado del proceso para una imagen de 64x128, con un bloque de 16x16 y celdas de 8x8 pixeles.

[61] Valveny & López. Ob. cit.

Figura 15. Imagen de 64x128, con un bloque de 16x16 y celdas de 8x8 pixeles

Fuente: Autor

5.3 MARCO LEGAL

5.3.1 Protección de la Información. En Colombia la ley 1273 de 2009 “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 y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[62]. El cual penaliza los delitos de tipo informático y relacionados con la protección de datos, esto debido a la necesidad de legislar y garantizar medidas frente a las nuevas tecnologías de la información que están relacionadas con cada ámbito de la actualidad, desde empresas hasta personas naturales.

Artículo 269A[63] Acceso abusivo a un sistema informático: Sin importar el tipo de seguridad presente en un sistema de información, cualquier ingreso sin autorización o permanencia en contra de la voluntad de quien tenga el derecho legítimo a excluirlo es considerado un delito.

[62] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273 (Enero 5 de 2009) . SENADO DE LA REPUBLICA. Ley 1273 de 2009. [en línea] [citado el 12 de septiembre 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[63] Ibid

Artículo 269B[64] Obstaculización ilegítima de sistema informático o red de telecomunicación: Cualquier tipo de obstaculización que limite o impida el acceso a un sistema informático, afectando su normal funcionamiento, restringiendo el acceso a la información allí contenida.

Artículo 269C[65] Interceptación de datos informáticos: La persona que sin contar con una orden judicial intercepte información que circula por medio de cualquier sistema informático atentando en contra de la confidencialidad de los que allí transitan es considerado un delito.

Artículo 269D[66] Daño informático: Llevar a cabo cualquier tipo de acción que incida de forma negativa en un sistema informático, bien sea a los datos que transitan o se almacenan atentando contra la integridad de la información disponibles, es considerado un delito

Artículo 269E[67] Uso de software malicioso: El uso, implementación y distribución de cualquier software que pueda generar daños en sistemas de información, atentando contra la disponibilidad, integridad y confidencialidad de la información es considerado un delito.

Artículo 269F[68] Violación de datos personales: Datos personales: sin importar el medio de obtención, la sustracción de cualquier tipo de datos personales de un sistema informático sin la autorización pertinente de sus propietarios es considerada un delito.

Artículo 269G[69] Suplantación de sitios web para capturar datos personales: El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en un delito.

5.3.2 Ley Habeas Data. En Colombia, el derecho fundamental de todo ciudadano para poder conocer, actualizar y ajustar cualquier tipo de información de índole

[64] Ibid
[65] Ibid
[66] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. Ob. cit.
[67] Ibid
[68] Ibid
[69] Ibid

personal que se encuentre almacenada en entidades tanto privadas como públicas, está reglamentada por la ley 1266 del 2008 “Habeas Data”[70; partir de allí se establecen los diferentes tipos de datos personales, públicos, semiprivados y privados, tal como se definen en la ley citada en cuestión:

> Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas[71].

> Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley. Así mismo se define el dato privado, el cual es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.[72]

No obstante, mediante LEY ESTATUTARIA 1581 DE 2012 se establecen disposiciones generales para el tratamiento de datos, allí en su artículo 5 se establece un nuevo tipo de datos personales, dentro de los cuales están los datos de biométricos:

> Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[73]

---

[70] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1266 (Enero 5 de 2009) . SENADO DE LA REPUBLICA. Ley 1266 2008. [en línea] [citado el 12 de septiembre 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[71] Ibid

[72] Ibid

[73] COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1581 (Octubre 17 de 2012) . SENADO DE LA REPUBLICA. Ley 1581 2012. [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Este artículo en cuestión introduce el concepto de datos Biométricos los cuales se catalogan como datos sensibles y se enmarcan en la ley de habeas data. Así pues, es necesario que las personas que hagan parte de proyecto expresen de forma voluntaria y escrita su consentimiento para utilizar sus registros faciales con fines investigativos y sin ánimo de lucro.

6 METODOLOGÍA

6.1 TIPO DE INVESTIGACIÓN

El desarrollo de este proyecto se realizó bajo una metodología de investigación de tipo aplicada, utilizando un modelo cuasi experimental en donde los datos se procesaron con un enfoque cuantitativo. Igualmente partiendo de los requerimientos propios del problema planteado en este trabajo, se estableció un diseño sin grupo de control y sin selección aleatoria.

6.2 POBLACIÓN

Las pruebas que realizarse con el algoritmo diseñado se llevaron a cabo en la sala principal de tutores del CEAD Ibagué, estableciendo como marco muestral los docentes pertenecientes a las escuelas ECBTI, ECSAH y ECEDU que cumplen sus labores diarias en el dicho espacio. Así pues, el grupo de estudio seleccionado cuenta con un total de 31 individuos. Igualmente, la unidad de observación está representada por la misma unidad maestral, es decir, cada docente representa una unidad.

6.3 HIPÓTESIS

A partir del uso de técnicas de visión computacional e Inteligencia artificial es posible crear un sistema de control de acceso mediado por modelos biométricos que sirva como herramienta de detección de intrusos y control de acceso dentro del sistema de seguridad del CEAD Ibagué.

6.4 OPERACIONALIZACIÓN DE LAS VARIABLES

Para evaluar de forma cuantitativa la calidad y efectividad del detector de rostros dentro de un contexto general, se propone trabajar con una matriz de confusión, siendo esta una técnica ampliamente utilizada dentro la visión computacional[74] para la verificación de clasificadores, para ello vamos a partir de las siguientes variables:

[74] PATTERSON, Josh; GIBSON, Adam. Deep Learning: A Practitioner's Approach. " O'Reilly Media, Inc.", 2017.

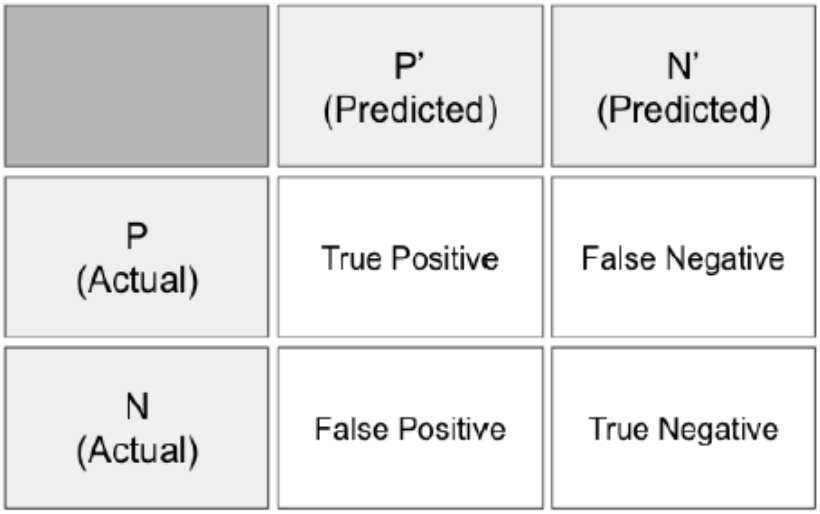
Tabla 4. Variables Independiente y dependiente.

Variables independientes	Variables dependientes
True positives (TP) *False positives (FP)* *True negatives (TN)* *False negatives (FN)*	*Sensitivity* *Specificity* *Accuracy* *Precision*

Fuente: Autor

Por consiguiente, los reales positivos y negativos son detecciones correctas dentro de cada una de sus categorías, es decir, elementos correctamente identificados bien sea por detección u omisión. Por otra parte, los falsos negativos y falsos positivos son detecciones incorrectas dentro de cada una de sus clases. En la siguiente figura se ilustra la clasificación de estas variables a partir de una matriz de confusión:

Figura 16. Ejemplo Matriz de Confusión.



Fuente: PATTERSON, Josh; GIBSON, Adam. Deep Learning: A Practitioner's Approach. " O'Reilly Media, Inc.", 2017.

Por otra parte, las variables dependientes se establecen en función de la calidad del sistema de detección establecido, evaluando 4 puntos fundamentales, Tasa de detección, Tasa de Error, Exactitud y Precisión; por lo cual para instaurarse como una unidad operacional se establecen las siguientes fórmulas.

Tabla 5. Formulas Tasa de detección, Tasa de Error, Exactitud y Precisión.

Métrica	**Cuantificación**
Sensitivity	TP / (TP + FN)
Specificity	TN / (TN + FP)
Accuracy	(TP + TN) / (TP + FP + FN + TN)
Precision	TP / (TP + FP)
F1	2TP / (2TP + FP + FN)

Fuente: PATTERSON, Josh; GIBSON, Adam. Deep Learning: A Practitioner's Approach. " O'Reilly Media, Inc.", 2017

Cabe realizar la salvedad con respecto al *Ground truth*, que dentro del contexto particular de la visión computacional es el resultado ideal que debería de producir un clasificador cualquiera a partir de la cantidad de detecciones ideales (100%), por lo general este se calcula de forma manual dependiendo del contexto en que se esté trabajando.

6.5 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para poder depurar y mejorar la efectividad del sistema de detección biométrico es necesario recolectar muestras para el correspondiente procesamiento y puesta en marcha del algoritmo, a partir de allí se implantan determinados cambios al mismo buscando adaptarlo a los requerimientos específicos del contexto en donde se desarrolla, en este caso la sala de tutores del CEAD Ibagué.

Por consiguiente, para realizar la toma de dichas muestras se utiliza un sistema que permita capturar y guardar la información de forma eficiente; para ello se empleó una cámara digital marca Logitech, modelo C310 HD WEBCAM, la cual se ilustra en la figura 17.

Figura 17. Cámara Digital C310 HD WEBCAM. Toma de muestras

Fuente: Logitech. C310 HD WEBCAM. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.logitech.com/es-es/product/hd-webcam-c310

Igualmente se utilizó un medio portable para procesar y guardar la información recogida por la cámara digital, para ello se dispuso de un computador portátil con los requerimientos técnicos suficientes para brindar un rendimiento optimo a problemas relacionados con la visión computacional. Las características técnicas del equipo utilizado se ilustran en la tabla 6.

Tabla 6. Características Técnicas Equipo de pruebas.

Computador Portátil MSI GP602QF	
Sistema Operativo	Ubuntu 18.01
Procesador	Intel I7 4700HQ
GPU	Nvidia GForce 950M
Memoria RAM	8 gigas
Disco Duro	1000 gigas
Lenguaje de Programación	Python
Resolución del Video	640*480

Fuente: Autor

6.6 DISEÑO Y DESARROLLO

El presente proyecto propone el diseño de un sistema de detección de intrusos y control de acceso mediado por modelos biométricos e inteligencia artificial. Esto, con el objetivo de ofrecer una herramienta complementaria al sistema de seguridad actualmente implementado en el CEAD Ibagué, permitiendo mitigar los riesgos a los

cuales se encuentran expuestos determinados activos de gran valor para la universidad. Dicho sistema parte del uso de una cámara de seguridad conectada de forma permanente a un servidor, el cual, será el encargado de procesar en tiempo real toda la información y realizar la detección del personal no autorizado.
Por otra parte, se identificaron las áreas problemáticas dentro de las instalaciones del CEAD Ibagué, las cuales por su ubicación física e implementación dentro del sistema de seguridad representan un riesgo para los activos de información de la universidad. Luego se establece un sector específico para llevar a cabo las pruebas del sistema de detección de intrusos y control de acceso, buscando determinar las condiciones ideales de funcionamiento que permitan una mayor precisión y confiabilidad por parte de este.

No obstante, los requerimientos a nivel de procesamiento de datos son altos; por lo cual se ajustarán los requisitos funcionales del algoritmo a partir del hardware disponible para ello (640 núcleos CUDA) sin dejar de lado en ningún momento uno de los objetivos principales que es lograr una precisión superior al 95%.

6.6.1 Sistema de Seguridad Física CEAD IbaguéEn la actualidad, el sistema de seguridad implementado dentro de las instalaciones del CEAD Ibagué se fundamenta en los controles manuales realizados por parte del personal de seguridad dentro de la universidad, tanto para el control y restricciones a lugares de acceso limitado.

Por otra parte, hay que tener presente que el CEAD Ibagué cuenta con un sistema de cámaras de seguridad deficiente, que no cubre los puntos cruciales de acceso, lo que dificulta enormemente la labor del personal de seguridad, que tienen que estar realizando rondas de forma constante para verificar que los visitantes no se encuentren en áreas de acceso restringido como la sala de tutores, la oficina de registro y control y los laboratorios.

Por otra parte, se determinaron las zonas de acceso y circulación pública, en donde transitan visitantes e interesados en matricularse en la Universidad. Igualmente, se identifican los puntos críticos, en los cuales se resguardan activos físicos que procesan o almacenan información digital cuya integridad y disponibilidad es vital para el desarrollo de las actividades rutinarias del CEAD y la labor de docencia. La figura 18 ilustra el punto anteriormente expuesto, en verde marcadas las zonas de libre circulación para los visitantes. Recuadros rojos marcan las zonas de interés: Registro y control, Sala de Tutores, Servidor y centro de comunicaciones:

Figura 18. Primera Planta - CEAD Ibagué.

Fuente: Jorge Tapiero - Líder GIDT Zona Sur

A partir de allí, podemos establecer tres puntos relevantes que se encuentran dentro de esas áreas de acceso común, la oficina de registro y control, la sala que alberga el servidor local del CEAD y la sala de tutores; en todas ellas se maneja información relacionada a procesos académicos y administrativos.

Ahora bien, la oficina de registro y control cuenta con una puerta de acceso lateral y con unas ventanillas para atención al público, la puerta de acceso se encuentra en el pasillo que lleva al vestíbulo principal del primer piso; esta puerta sólo puede ser usada por los funcionarios autorizados de registro y toda la atención a público se realiza desde las ventanillas dispuestas para ello en el vestíbulo principal. También cabe aclarar que dentro de la oficina no hay cámaras de seguridad y la puerta no cuenta con ningún tipo de control de acceso la figura 19 ilustran este punto:

Figura 19. Ubicación del punto de acceso a la oficina de registro

Fuente: Autor

Posteriormente, se llega al vestíbulo principal, tal como se muestra en la figura 21, dicho vestíbulo brinda acceso a las ventanillas de registro, la sala que alberga el servidor y la sala de tutores; igualmente por este vestíbulo circula gran cantidad de personas externas a la universidad durante momentos de alto flujo de personal, bien sea por la realización de eventos o a periodos de matrícula, lo cual hace realmente difícil llevar un seguimiento permanente por parte del personal de seguridad, sobre todo porque no hay cámaras de seguridad en este sector.

Figura 20. Vestíbulo principal - CEAD Ibagué

Fuente: Autor

Dentro de los accesos ubicados en el vestíbulo principal se encuentra la sala que resguarda el servidor del CEAD, la cual, si bien gran parte del tiempo mantiene su puerta cerrada, está ubicado en un sitio donde el riesgo de daño de activos por actos deliberados (vandálicos) es alta. Su puerta de ingreso no utiliza ningún tipo de control de acceso y no cuenta con cámaras de seguridad dentro de la sala.

Figura 21. Puerta de acceso a la sala del servidor central CEAD Ibagué

Fuente: Autor

Por último, este vestíbulo también brinda acceso directo a la sala de tutores; no obstante, la puerta de dicha sala por lo general mantiene abierta y dentro de ese espacio no hay sistema de cámaras de seguridad. Las figuras 23 enseñan la entrada a dicha sala desde el acceso público.

Figura 22. Entrada a sala de tutores desde el vestíbulo Principal.

Fuente: Autor

Por otra parte hay que tener presente que dentro de la universidad, no se ejecutan de forma rigurosa las políticas de seguridad relacionadas con el uso de estaciones de trabajo, a partir de allí que en reiteradas ocasiones los tutores dejan sus equipos sin ningún tipo de bloqueo; esto sumado a la falta de control de acceso a sala

representa un riesgo alto de seguridad con relación a la información contenida en dichos equipos, que no solo es propia de los docentes, datos de acceso al campus, notas de los cursos, datos personales y demás elementos del proceso académico de los estudiantes se encuentra allí, poniendo en riesgo su integridad y confidencialidad.

6.6.2 Sistema de detección de intrusos y control de acceso. Luego de realizar la revisión de las instalaciones del CEAD y partiendo de las características propias de cada uno de los puntos físicos relacionados en el apartado anterior, se selecciona la sala de tutores como espacio ideal para realizar las pruebas del sistema de detección de intrusos y control acceso, esto debido al flujo constante de personal, lo cual permite ponerlo a prueba dentro de un ambiente complejo y cambiante.

Figura 23. Interior sala de tutores - CEAD Ibagué

Fuente: Autor

Por consiguiente, se evaluó la posición ideal de la cámara encargada de la toma de datos para el control dentro de la sala de tutores, por lo cual se evaluaron diferentes ángulos, buscando que los rasgos faciales y la cobertura de la entrada se identificaran de forma clara y sin puntos ciegos. En consecuencia, se decidió colocar la cámara a un Angulo de 120º de la entrada principal de la sala de tutores con una altura de 1.82 metros de alto.

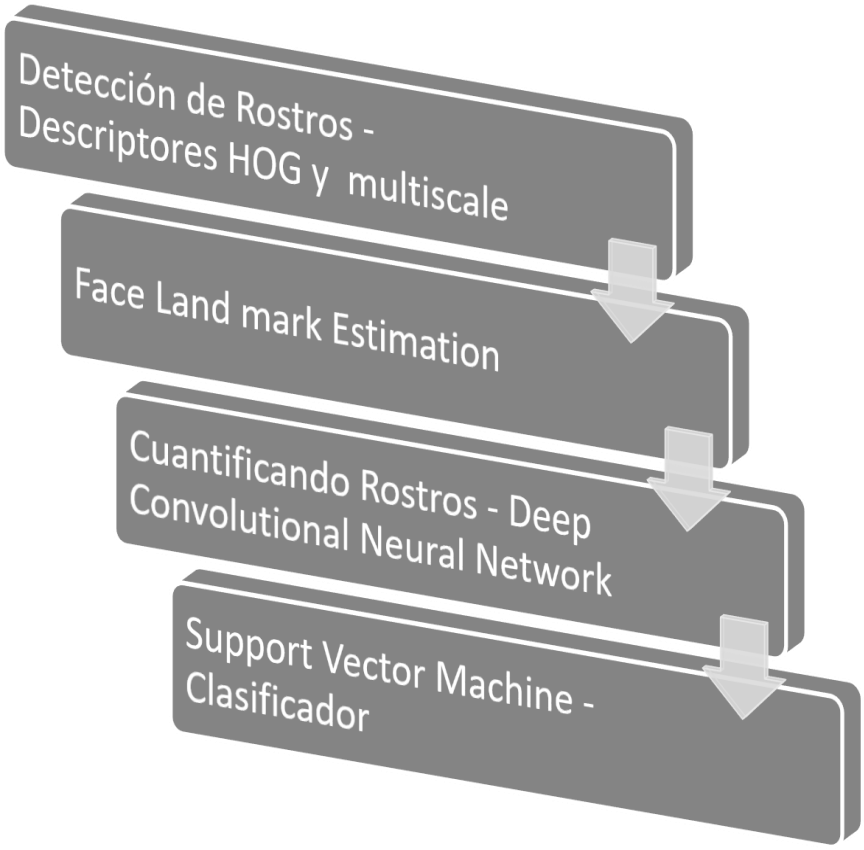
6.6.2.1 Diseño de la Prueba. Una vez determinada la posición del sistema de captura de imágenes dentro de la sala de tutores, es necesario establecer cuáles son las condiciones ideales para poner a prueba el algoritmo y verificar el desempeño de este. Por ello, se estableció el sábado como el espacio ideal para llevarla cabo, debido a que es el día de la semana en que flujo de personal dentro de las instalaciones del CEAD Ibagué es mayor.

En consecuencia, se utilizó el dispositivo de captura de imágenes el sábado 15 de septiembre de 2’18, capturando de forma ininterrumpida el flujo de entrada y salida

de personas de la sala de tutores durante un espacio de 240 minutos, para posteriormente procesar la información y determinar el rendimiento del sistema propuesto.

6.6.3 Selección y acondicionamiento del Algoritmo. El reconocimiento facial es un campo ampliamente estudiado en la actualidad, de allí que las técnicas y librerías disponibles para su implementación estén al alcance de la mayoría de los desarrolladores. Para este trabajo en particular se utilizó como base el algoritmo de detección de rostros implementado por Geitgey75 en las librerías FaceRecognition mediante el uso de Deep Learning y visión computacional. Apoyado sobre OpenCV. La figura 25 muestra un esquema de funcionamiento general del mismo.

Figura 24. Diagrama algoritmo detección de rostros.



Fuente: Autor

[75] GEITGEY, Adam. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning. Medium. https://medium. com/@ ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78, 2016.

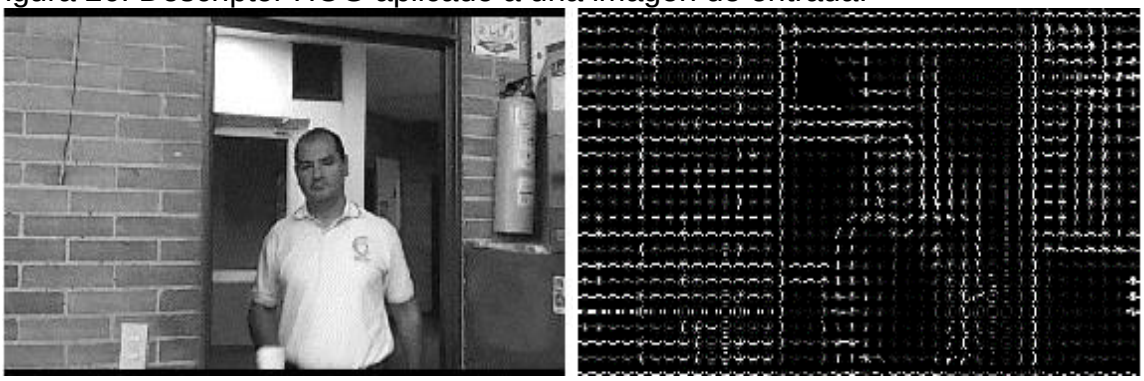
6.6.3.1 Detección de rostros – Descriptores HOG y *Multiscale*. El proceso de adquisición de imágenes se realiza cuadro a cuadro a partir de la información recibida desde la cámara digital, luego en la primera parte del algoritmo se convierte la imagen de entrada a escala de grises (0 - 255), esto con el fin de poder evaluar la información de la imagen mediante los descriptores HOG, la figura 26 ilustra esta primera etapa del proceso:

Figura 25. Adquisición de imágenes y conversión en escala de grises.

Fuente: Autor

Una vez la imagen de entrada está en escala de grises, se aplican los descriptores HOG, los cuales evalúan cada uno de los pixeles presentes en la imagen y determinan su gradiente con respecto a su entorno, para a partir de allí se realiza la cuantificación de los elementos presentes en esta, la figura 22 ilustra el funcionamiento de los descriptores HOG dentro de la imagen:

Figura 26. Descriptor HOG aplicado a una imagen de entrada.



Fuente: Autor

Posteriormente, se evalúa la información contenida en la imagen a partir de la cuantificación realizada mediante los descriptores HOG, para esto se divide la imagen en regiones y se recorren de forma secuencial (*multiscale*) verificando los datos contenidos en cada uno de estos sectores mediante el uso de *una support vector machine* previamente entrenada para detectar rostros; a partir de allí, las detecciones se marcan en la imagen mediante un recuadro rojo.

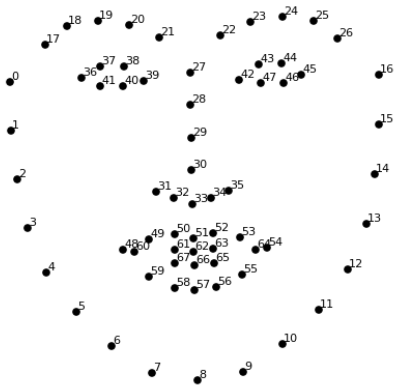
Figura 27. Detección de rostro

Fuente: Autor

Por otra parte, la detección de rostros realizada hasta el momento no garantiza que la ubicación de la cara sea totalmente frontal, por lo cual es necesario adecuar las detecciones para facilitar el trabajo que va a realizar posteriormente la Red Neuronal

Convolucional, para ello se utiliza el algoritmo *Face Land Mark Estimation*[76]*.* Este algoritmo permite identificar 68 puntos concretos dentro del rostro de una persona, la figura 23 y 24 ilustran este punto.

Figura 28. *Face Land Mark*. Estimación de 68 puntos en un rostro.



Fuente: AMOS, Brandon, et al. Openface: A general-purpose face recognition library with mobile applications. CMU School of Computer Science, 2016.

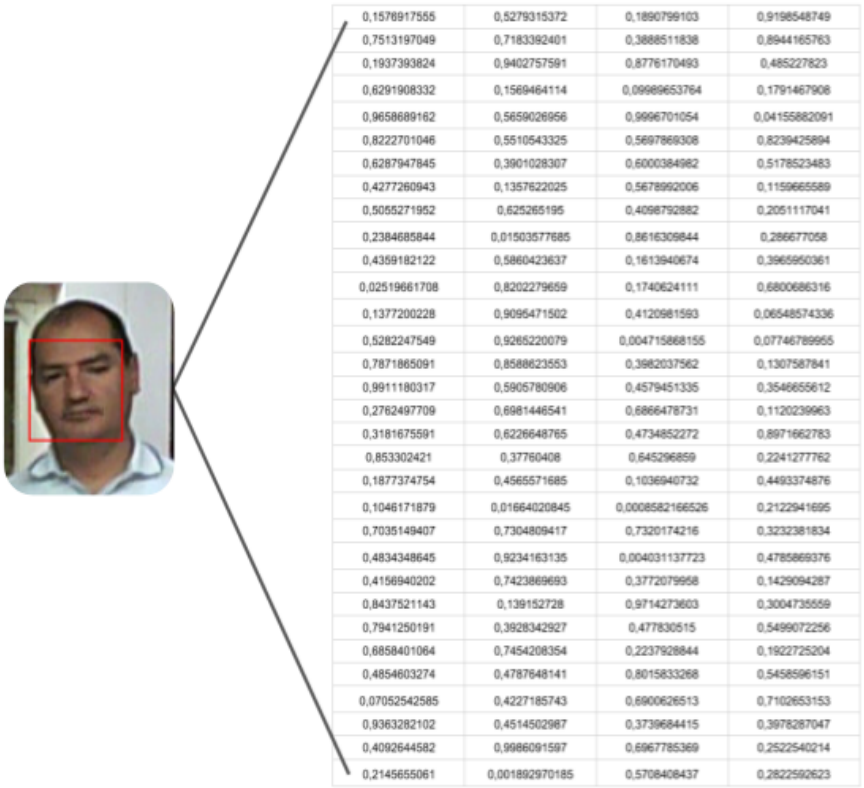
Figura 29. *FaceLand Mark.*

Fuente: Autor

[76] KAZEMI, Vahid; SULLIVAN, Josephine. One millisecond face alignment with an ensemble of regression trees. En Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2014. p. 1867-1874.

Una vez se han detectado y aislado los rostros en la imagen, es necesario generar una medida que permita comparar de forma fiable los rasgos únicos presentes en cada uno de ellos, para lo cual se utiliza una Red Neuronal Convolucional previamente entrenada[77], la cual identifica y cuantifica 128 puntos de interés a partir de rasgos característicos del rostro, la figura 31 ilustra este punto.

Figura 30. Cuantificación de rostro – Deep Neuronal Network.



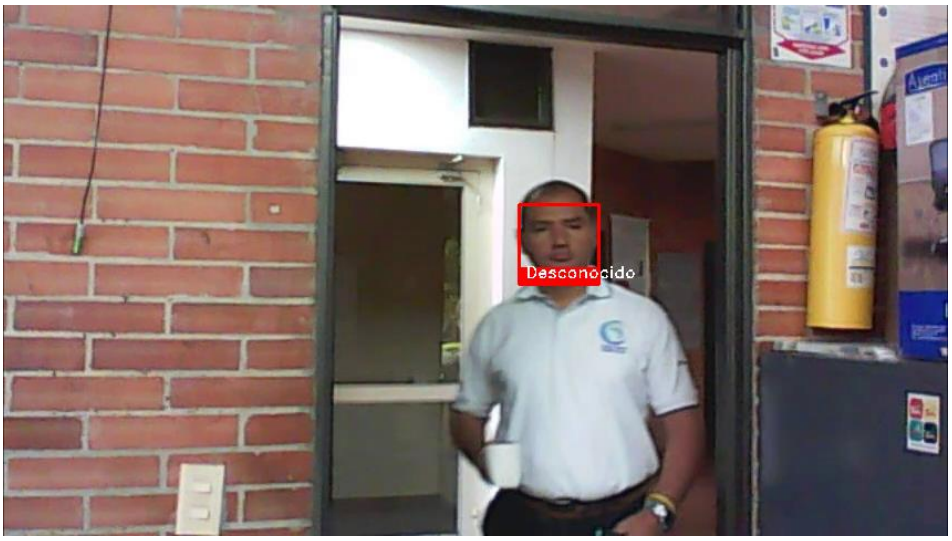
0,1578917555	0,5279315372	0,1890799103	0,9198548749
0,7513197049	0,7183392401	0,3888511838	0,8944165763
0,1937393824	0,9402757591	0,8776170493	0,485227823
0,6291908332	0,1569464114	0,09989653764	0,1791467908
0,9658689162	0,5659026956	0,9996701054	0,04155882091
0,8222701046	0,5510543325	0,5697869308	0,8239425894
0,6287947845	0,3901028307	0,6000384982	0,5178523483
0,4277260943	0,1357622025	0,5678992006	0,1159665589
0,5055271952	0,625265195	0,4098792882	0,2051117041
0,2384685844	0,01503577685	0,8616309844	0,286677058
0,4359182122	0,5860423637	0,1613940674	0,3965950361
0,02519661708	0,8202279659	0,1740624111	0,6800686316
0,1377200228	0,9095471502	0,4120981593	0,06548574336
0,5282247549	0,9265220079	0,004715868155	0,07746789955
0,7871865091	0,8588623553	0,3982037562	0,1307587841
0,9911180317	0,5905780906	0,4579451335	0,3546655612
0,2762497709	0,6981446541	0,6866478731	0,1120239963
0,3181675591	0,6226648765	0,4734852272	0,8971662783
0,853302421	0,37760408	0,645296859	0,2241277762
0,1877374754	0,4565571685	0,1036940732	0,4493374876
0,1046171879	0,01664020845	0,0008582166526	0,2122941695
0,7035149407	0,7304809417	0,7320174216	0,3232381834
0,4834348645	0,9234163135	0,004031137723	0,4785869376
0,4156940202	0,7423869693	0,3772079958	0,1429094287
0,8437521143	0,139152728	0,9714273603	0,3004735559
0,7941250191	0,3928342927	0,477830515	0,5499072256
0,6858401064	0,7454208354	0,2237928844	0,1922725204
0,4854603274	0,4787648141	0,8015833268	0,5458596151
0,07052542585	0,4227185743	0,6900626513	0,7102653153
0,9363282102	0,4514502987	0,3739684415	0,3978287047
0,4092644582	0,9986091597	0,6967785369	0,2522540214
0,2145655061	0,001892970185	0,5708408437	0,2822592623

Fuente: Autor

En ese orden de ideas, la cuantificación del rostro permite establecer un conjunto de valores únicos a partir de las caracterices biométricas de una persona, para posteriormente ser comparados con la información biométrica del personal autorizado para circular por la sala, de allí que se pueda generar una detección final identificando claramente si la persona cuenta con autorización correspondiente, tal como se ilustra en la figura 32.

[77] AMOS, Brandon, et al. Openface: A general-purpose face recognition library with mobile applications. CMU School of Computer Science, 2016.

Figura 31, Detección final registrada por el algoritmo.



Fuente: Autor.

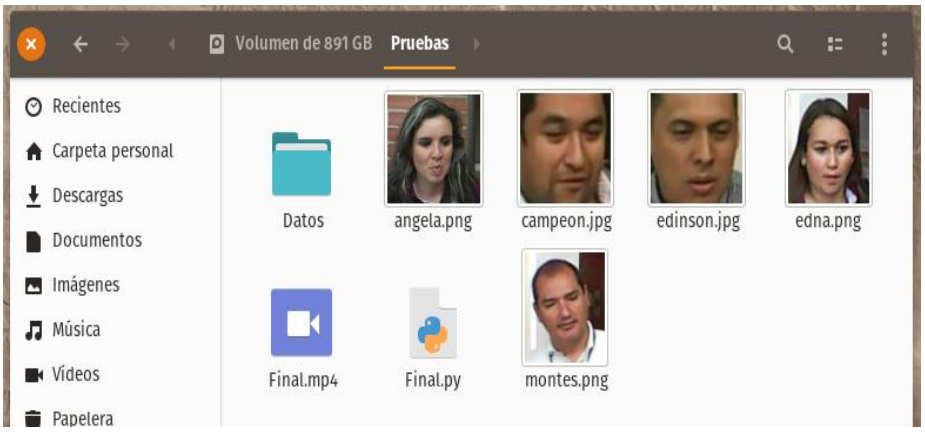
7 RESULTADOS Y DISCUSIÓN

Para evaluar el algoritmo seleccionado se diseñó una prueba teniendo en cuenta la complejidad del medio al cual se tiene que enfrentar y a las imitaciones de hardware con las que cuenta este proyecto. Por consiguiente, tal como se establece en el apartado de Diseño de Prueba, se utilizó el dispositivo de captura de imágenes durante una jornada laboral en un espacio de 240 minutos.

En en este punto cabe aclarar que de los 36 docentes que laboran actualmente en la sala de tutores del CEAD Ibagué, se seleccionó un grupo de 5 docentes, los cuales dieron su consentimiento para que sus datos biométricos estuvieran guardados dentro del programa y sirvieran como la base de datos de aquellos que están autorizados, es decir, los restantes 31 aparecen como personal no autorizado para ingresar a la sala. Todo esto con el fin de facilitar la ejecución de este partiendo, minimizando los requerimientos de procesamiento del mismo, dado a que solo se cuenta con 650 núcleos CUDA para procesar la información.

A partir de allí, se organizó la información recolectada para llevar a cabo las pruebas del algoritmo, para ello el programa se diseño para ir guardando todas las detecciones realizadas en una capeta (Datos) y calcular la información biométrica en tiempo real, esto con el objetivo de guardar este tipo de datos dentro del disco duro, garantizando que dicha información no será utilizada en un futuro. La figura 33 Ilustra la organización realizada para las pruebas.

Figura 32. Organización elementos de pruebas y rostros autorizados.



Fuente: Autor

Igualmente, para poder procesar la información es necesario establecer la función de la matriz de confusión y su relación con los datos analizados, por lo cual se establecen dos categorías de detección, Personal autorizado y personal no autorizado. La tabla 7 establece la función de cada categoría en correspondencia al tipo de detección realizada:

Tabla 7. Categorización en correspondencia al tipo de detección realizada:

Matriz de Confusión	**Resultado de la Clasificación**	
	Personal Autorizado (Predicción)	Personal No autorizado (Predicción)
Personal Autorizado (Actual)	True Positive	False Negative
Personal No autorizado (Actual)	False Positive	True Negative

Fuente: Autor

Una vez ejecutado el algoritmo se obtuvieron un total de 4901 detecciones, las cuales se procesaron a partir de los lineamientos establecidos dentro de la metodología de este trabajo, teniendo como resultado los datos expuestos en la tabla 8.

Tabla 8. Resultados finales variables independientes.

Detecciones Finales	
Detecciones Totales	4901
True Positive (TP)	570
False Positive (FP)	54
False Negative (FN)	40
True Negative (TN)	4291

Fuente: Autor

En consecuencia, se procede a calcular los valores finales para cada una de las variables establecidas en concordancia con lo establecido dentro de la parte metodológica, la tabla 9 relaciona los resultados finales de cada una de ellas.

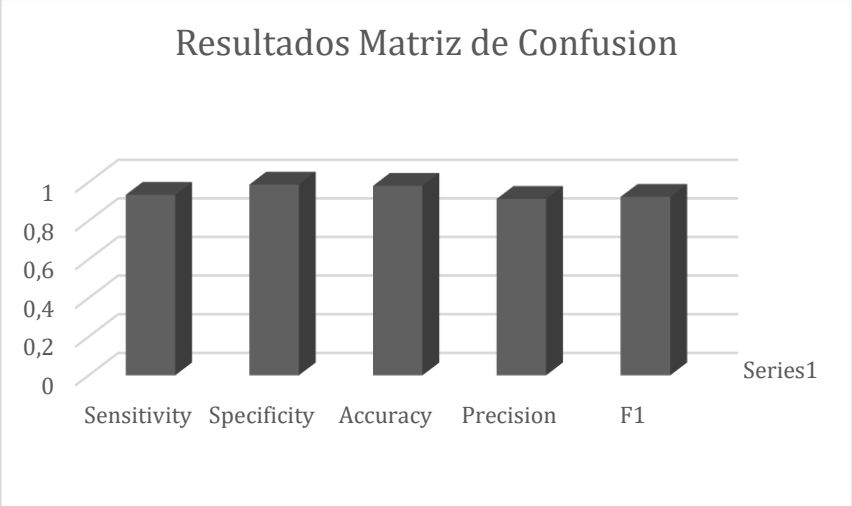
Tabla 9. Resultados Finales variables dependientes

Detecciones Finales	
Sensitivity: TP / (TP + FN)	0,934426229508197
Specificity: TN / (TN + FP)	0,987571921749137
Accuracy: (TP + TN) / (TP + FP + FN + TN)	0,981029263370333
Precision: TP / (TP + FP)	0,913461538461538
F1: 2TP / (2TP + FP + FN)	0,923824959481361

Fuente: Autor

A partir de los resultados obtenidos se pueden destacar varios aspectos del algoritmo seleccionado, el primero es el porcentaje de la sensibilidad a detecciones el cual esta sobre el 93%, esta medida nos indica la tasa de detecciones positivas realizadas correctamente. Por otra parte, la especificidad cuantifica la capacidad del programa de obviar falsos positivos (FP), en este apartado se obtuvo un 98%. La figura 34 ilustra el porcentaje de precisión de las variables dependientes.

Figura 33. Grafico del porcentaje de eficiencia de las variables dependientes establecidas. Sensibilidad 93%, especificidad98%, exactitud del 98%, precisión 91%.



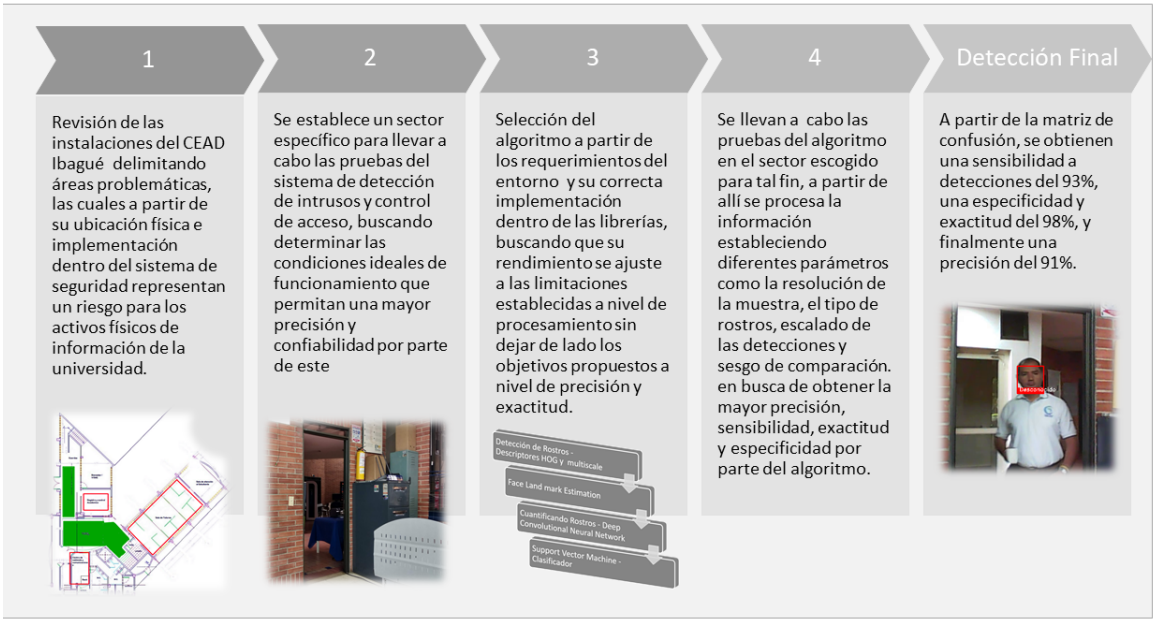
Fuente: Autor

Por otra parte, y en concordancia con los objetivos planteados, se obtuvo una exactitud del 91% y una precisión global del 91%. Eb este punto cabe destacar que debido a las limitaciones de hardware la resolución de las imágenes se vio limitada a muestras de video de una resolución de 640*480; así mismo, fue necesario

escalar las imágenes y las detecciones realizadas a un factor de 0.50 con el fin de poder ejecutar el programa en tiempo real y ajustándose a los 640 núcleos CUDA disponibles.

7.1 INFOGRAFIA DESARROLLO DEL PROYECTO

Figura 34. Infografía desarrollo del proyecto.



Fuente: Autor

8 CONCLUSIONES

En la actualidad, la seguridad informática ha tomado un rol predominante en la consecución de objetivos a nivel empresarial, de allí que la protección de activos de información sea un asunto de primer nivel dentro de las políticas y controles de seguridad implementados; por lo cual las empresas destinan gran cantidad de recursos a la protección de datos a nivel lógico tratando de mitigar los riesgos a los cuales se encuentran expuestos. No obstante, una incorrecta estructuración de este tipo de medidas tiende a descuidar los elementos encargados de procesar, almacenar y transportar la información, es decir la parte física.

En ese orden de ideas, este trabajo se enmarco en el diseño de un sistema de seguridad biométrica que funcione como medio de control de acceso y detección de intrusos, facilitando la detección de personal no autorizado dentro de las instalaciones del CEAD Ibagué. Todo esto, mediado por técnicas de inteligencia artificial y visión computacional.

A partir de allí y en correspondencia con los objetivos planteados, se identificaron las áreas críticas que representan un riesgo de seguridad para los activos informáticos dentro de las Instalaciones del CEAD Ibagué; como resultado se referenciaron las oficinas de Registro y Control, la sala servidores y la sala de tutores como puntos débiles dentro del sistema de seguridad y que representan un riesgo alto para la integridad de los activos lógicos de la Universidad.

Posteriormente se establecen las condiciones ideales para el funcionamiento del algoritmo a partir de las limitaciones de hardware con las que cuenta el proyecto y las características propias del contexto en el que debe desenvolverse. Para ello se realizaron ajustes dentro de la escala de detecciones, resolución de la imagen y límites de verificación (coincidencia dentro de los rostros); los cuales debieron ser ajustados para obtener un rendimiento ideal y que responda a los objetivos planteados.

En consecuencia, se planteó el uso de un algoritmo fundamentado en un modelo biométrico de detección facial, el cual fue sometido a una prueba de campo y evaluado mediante una matriz de confusión, teniendo como resultados una sensibilidad a detecciones del 93%, una especificidad y exactitud del 98%, y finalmente una precisión del 91%; mostrando ser un sistema robusto y lo suficientemente preciso para ser implementado como un complemento de seguridad física dentro del CEAD Ibagué.

Por otra parte, a partir de los resultados encontrados, se evidencia que el estado actual de las técnicas de inteligencia artificial y sus aplicaciones prácticas mediante algoritmos implementados en distintas librerías pone al alcance de cualquier disciplina un conjunto de técnicas de alto nivel, que pueden ser usadas para resolver problemas prácticos dentro de contextos específicos.

Para finalizar, es claro que la implementación y uso de técnicas de inteligencia artificial se ajustan de forma adecuada a los requerimientos planteados en el objetivo principal de este proyecto, permitiendo desarrollar una solución lo suficientemente robusta para ser ejecutada en un contexto real, pudiendo integrarse en un sistema general de seguridad, complementando y facilitando la labor del personal inmerso en dicho proceso.

9 REFERENCIAS

AMOS, Brandon, et al. Openface: A general-purpose face recognition library with mobile applications. CMU School of Computer Science, 2016.

Colmenares, G.Análisis Multivariante y Aplicaciones. Universidad de Los Andes Mérida-Venezuela. [en línea] [citado el 20de septiembre 2018]. Disponible en http://webdelprofesor.ula.ve/economia/gcolmen/postgrado2.html

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1266 (Enero 5 de 2009) . SENADO DE LA REPUBLICA. Ley 1266 2008. [en línea] [citado el 12 de septiembre 2018]. Disponible en internet:

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1273 (Enero 5 de 2009) . SENADO DE LA REPUBLICA. Ley 1273 de 2009. [en línea] [citado el 12 de septiembre 2018]. Disponible en internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

COLOMBIA. SENADO DE LA REPÚBLICA. Ley 1581 (Octubre 17 de 2012) . SENADO DE LA REPUBLICA. Ley 1581 2012. [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Drago, A. Methods and Techniques for Enhancing Physical Security of Critical Infrastructures. [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.fedoa.unina.it/10532/1/PhDThesisAnnaritaDrago.pdf

El Portal de ISO27002. Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002. ISO27002.es [en línea] [citado el 12 de septiembre 2018]. Disponible en http://www.iso27000.es/iso27002.html

FENNELLY, Lawrence; PERRY, Marianna. Physical security: 150 things you should know. Butterworth-Heinemann, 2016. Pagina 75

GEITGEY, Adam. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning. Medium. https://medium. com/@ ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78, 2016

GEITGEY, Adam. Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning. Medium. https://medium. com/@ ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78, 2016

Gerencia de Innovación y Desarrollo Tecnológico. Seguridad de la Información. GIDT UNAD [en línea] [citado el 12 de septiembre 2018]. Disponible en https://gidt.unad.edu.co/seguridad-de-la-informacion

Guide (pp. 393-409). Indianapolis, IN USA: Wiley. Citado por Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

Harris, S. Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill. Citado por Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120.

Hunter, D. Physical Security and Why It Is Important. SANS Institute InfoSec Reading Room. [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

Irwin, S. (2014, September 8). Creating a Threat Profile for your Organization. [en línea] [citado el 12 de septiembre]. Disponible en https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

KAZEMI, Vahid; SULLIVAN, Josephine. One millisecond face alignment with an ensemble of regression trees. En Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2014. p. 1867-1874

KING, Davis E. Dlib-ml: A machine learning toolkit. Journal of Machine Learning Research, 2009, vol. 10, no Jul, p. 1755-1758.

Lynn III, W. J. Defending a New Domain. . [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

MARCOS, A. González, et al. Técnicas y algoritmos básicos de visión artificial. Universidad de la Rioja, [en línea] [citado el 12 de septiembre]. Disponible en https://publicaciones.unirioja.es/catalogo/online/VisionArtificial.pdf

NALWA, Vishvjit S. A guided tour of computer vision. Addison-Wesley Longman Publishing Co., Inc., 1994.

Nayak, U., & Rao, U. H. (2014). The InfoSec handbook: An introduction to information security. Apress.

OLABE, Xabier Basogain. Redes neuronales artificiales y sus aplicaciones. Publicaciones de la Escuela de Ingenieros 101pp, 1998

OpenCV. OpenCV Documentation. [en línea] [citado el 12 de septiembre de 2018]. Disponible en https://docs.opencv.org/3.4/

PATTERSON, Josh; GIBSON, Adam. Deep Learning: A Practitioner's Approach. " O'Reilly Media, Inc.", 2017.

Ribalta, Albert Solé. Seguridad en los sistemas biométricos. Openlibra. [en línea] [citado el 12 de septiembre]. Disponible en https://openlibra.com/es/book/seguridad-en-los-sistemas-biometricos

RUSSELL, Stuart J.; NORVIG, Peter. Artificial intelligence: a modern approach. Malaysia; Pearson Education Limited,, 2016.

RUSSELL, Stuart J.; NORVIG, Peter. Inteligencia Artificial: un enfoque moderno. 2004.

SANCHEZ, Angel. Aplicaciones de la visión artificial y la biometría informática. Dykinson SL,(Madrid), URJC, 2005.

Santander Peláez,M. . Measuring effectiveness in Information Security Controls. SANS Institute [en línea] [citado el 12 de septiembre]. Disponible en https://www.sans.org/reading- room/whitepapers/basics/measuring-effectiveness-information-security-controls-33398.

Scott, M. COCA-COLA DATA BREACH HIGHLIGHTS IMPORTANCE OF LAPTOP SECURITY. . [en línea] [citado el 12 de septiembre 2018]. Disponible en: http://www.acfe.com/fraud-examiner.aspx?id=4294986501

Secretaria General. Política de seguridad de la información y gestión documental. GIDT [en línea] [citado el 12 de septiembre 2018]. Disponible en https://gidt.unad.edu.co/seguridad-de-la-informacion

SERRATOSA, Francesc. La biometría para la identificación de las personas. Universitat Oberta de Catalunya, 2008, p. 8-20.

Stewart, J., Chapple, M., & Gibson, D. (2012). Physical Security Requirements. In CISSP Certified Information Systems Security Professional study guide (6th ed., pp. 572-597,745-774). Indianapolis, IN USA: Wiley.

Universidad Nacional Abierta y a Distancia, La UNAD se constituye como la primera mega universidad pública en Colombia. Noticias UNAD [en línea] [citado el 12 de septiembre 2018]. Disponible en: https://noticias.unad.edu.co/index.php/unad-noticias/todas/2362-la-unad-se-constituye-en-la-primera-megauniversidad-publica-de-colombia

Valveny, E., Varnell, M., Lopez, A. Detección de Objetos, Universidad Autónoma de Barcelona, [en línea] [citado el 12 de septiembre 2018]. Disponible en https://www.coursera.org/learn/deteccion-objetos/home/welcome

Wailgum, T. Metrics for Corporate and Physical Security Programs . [en línea] [citado el 12 de septiembre]. Disponible en http://www.csoonline.com/article/2118531/metrics-budgets/metrics-for-corporate-and-physical-security-programs.html

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. Face recognition: A literature survey. ACM computing surveys. [en línea] [citado el 12 de septiembre]. Disponible en http://mplab.ucsd.edu/~marni/Igert/Zhao_2003.pdf

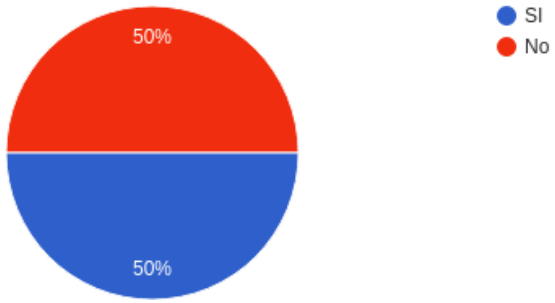
10 ANEXO A

Encuesta Identificación de Incidentes de Seguridad en la Universidad Nacional Abierta y a Distancia – UNAD

El objetivo de la encuesta es validar los incidentes relacionados a la seguridad física presentados en las instalaciones de la Universidad (UDR, CCAV y CEAD). La cual fue respondida por 20 tutores pertenecientes al CEAD Ibagué, Zona Sur y se realizo mediante el siguiente enlace: https://goo.gl/forms/LihcfkY0bg2amWls2.

Pregunta 1. ¿Se han presentado incidentes relacionados con la seguridad física de los activos dentro de las instalaciones del Centro (robo, daño de equipos, accesos no autorizados)?.

Figura 35. Gráfico de respuestas de formularios. Título de la pregunta: ¿Se han presentado incidentes relacionados con la seguridad física de los activos dentro de las instalaciones del Centro (robo, daño de equipos, accesos no autorizados)?.. Número de respuestas: 20 respuestas.

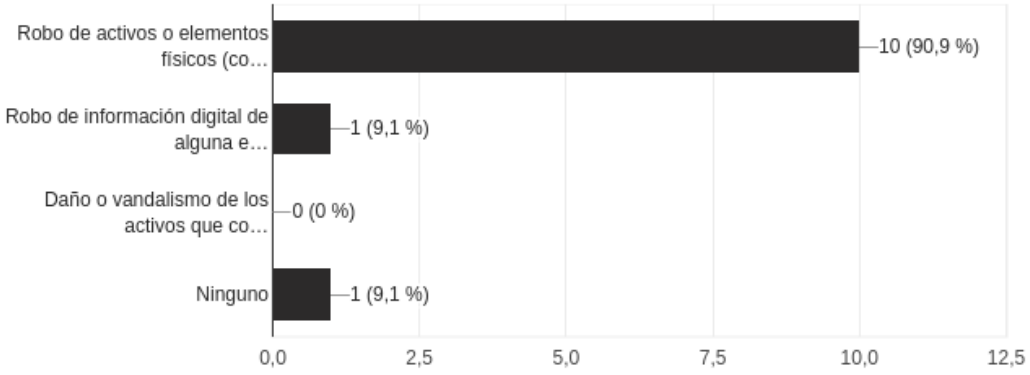


Fuente: Autor

Pregunta 2. De ser afirmativa la anterior respuesta, ¿Cuál de las siguientes opciones se ajusta al tipo de incidente presentado? Marqué las que consideré necesarias:

- Robo de activos o elementos físicos (computadores, celulares, tablets)
- Robo de información digital de alguna estación de trabajo o terminal
- Daño o vandalismo de los activos que contienen información digital
- Otra

Figura 36. Gráfico de respuestas de formularios. Título de la pregunta: De ser afirmativa la anterior respuesta, ¿Cuál de las siguientes opciones se ajusta al tipo de incidente presentado? Marqué las que considere necesarias: Número de respuestas: 11 respuestas.

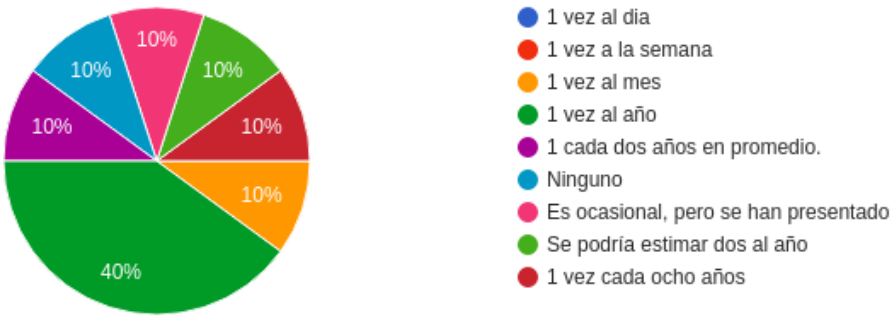


Fuente: Autor.

Pregunta 3. ¿Con qué frecuencia se presentan estos incidentes de seguridad física?

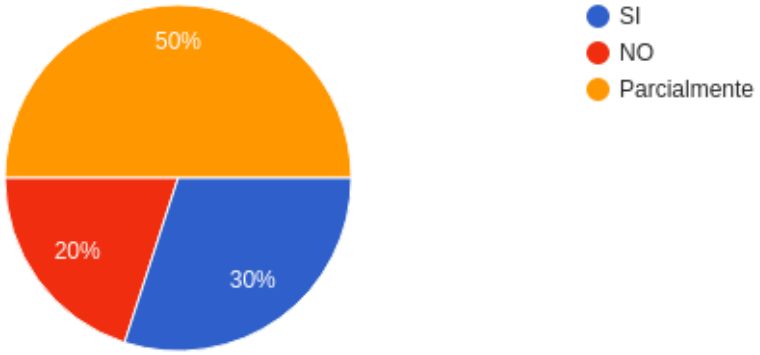
- 1 vez al día
- 1 vez a la semana
- 1 vez al mes
- 1 vez al año
- Otra

Figura 37. Gráfico de respuestas de formularios. Título de la pregunta: ¿Con qué frecuencia se presentan estos incidentes de seguridad física? Número de respuestas: 10 respuestas.



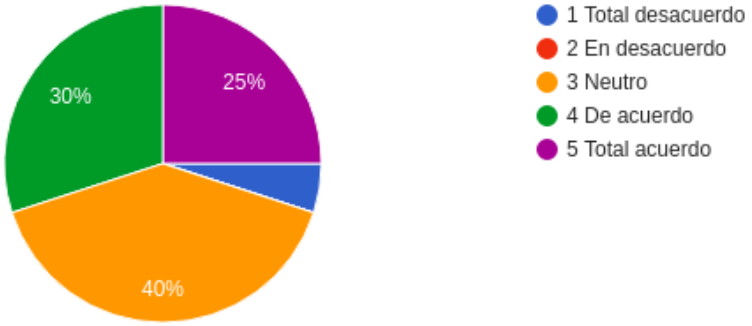
Fuente: Autor

Pregunta 4. ¿En el centro regional en el cual se encuentra, se implementan políticas de seguridad con respecto al uso de estaciones de trabajo?



Fuente: Autor

Pregunta 5. ¿Considera que la seguridad física implementada en su centro responde a las necesidades propias de la protección de activos (servidores, computadores personales, estaciones de trabajo) y salvaguarda de forma correcta la información que puede ser de vital importancia para la universidad?



Fuente: Autor