

UNIVERSIDAD TÉCNICA LATINOAMERICANA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA



**Universidad Técnica
Latinoamericana**

TRABAJO DE GRADUACIÓN

“Implementación de un sistema de control de temperatura y detección de mascarilla, de tipo Biométrico: Para la prevención de COVID19, en la Universidad Técnica Latinoamericana”

PARA OPTAR AL GRADO DE:

INGENIERÍA ELECTRÓNICA

PRESENTADO POR:

Oscar Rolando Mancía Rosales

Nicolas Ernesto Castaneda Barillas

Víctor Edgardo Rivas Córdova

SANTA TECLA, AGOSTO DE 2023



**Universidad Técnica
Latinoamericana**

AUTORIDADES UNIVERSITARIAS

ING. ROSENDO MAURICIO SERMEÑO PALACIOS
RECTOR

ING. FRANCISCO ALFREDO CARRILLO LARREYNAGA
VICE-RECTOR

ING. ROOSELVET ADOLFO OSORIO
SECRETARIO GENERAL

LIC. CARLOS MAURICIO MOLINA RENDEROS
FISCAL

ING. MAURICIO ANTONIO AGUIRRE ORELLANA
DECANO DE LA FACULTAD DE INGENIERÍA

ING. RENÉ EDUARDO CUÉLLAR FIGUEROA
DIRECTOR DE ESCUELA DE INGENIERÍA ELECTRÓNICA

SANTA TECLA, AGOSTO DE 2023



ASESOR

Ing. Nelson Antonio Trabanino Aguilar

JURADO EVALUADOR

Ing. Eduardo Antonio Ferman Arana

Ing. Francisco Ernesto Colorado Gutiérrez

Ing. Gustavo Raúl Alfaro

SANTA TECLA, AGOSTO DE 2023

UNIVERSIDAD TÉCNICA LATINOAMERICANA

ACTA DE CALIFICACIÓN DE
DEFENSA DE TRABAJO DE GRADUACIÓN

No. TRES MIL CIENTO SETENTA

A las nueve horas y quince minutos, del sábado veintiséis de agosto de dos mil veintitrés. Reunidos los Miembros del Tribunal Examinador del Trabajo de Graduación presentado por VICTOR EDGARDO RIVAS CORDOVA, en el salón de sesiones de la UNIVERSIDAD TÉCNICA LATINOAMERICANA. Se procedió:

PRIMERO: Que habiendo analizado el Trabajo de Graduación titulado:

"IMPLEMENTACION DE UN SISTEMA DE CONTROL DE TEMPERATURA Y DETECCION DE MASCARILLA, DE TIPO BIOMETRICO; PARA LA PREVENCIÓN DE COVID-19, EN LA UNIVERSIDAD TECNICA LATINOAMERICANA."

Se dio por aprobada, la parte escrita.

SEGUNDO: Que, con base a dicha aprobación de la parte escrita, se procedió a instalar la respectiva defensa oral del trabajo.

De conformidad a los resultados en dicha defensa, este Tribunal Examinador acuerda dar por APROBADO, con una calificación de OCHO PUNTO SEIS (8.6), el Trabajo de Graduación presentado por el alumno arriba detallado, obteniendo a partir de esta fecha su calidad de: INGENIERO EN ELECTRONICA

No habiendo más que hacer constar, damos por terminada el acta que firmamos.



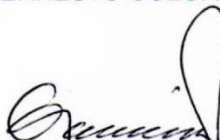
ING. GUSTAVO RAUL ALFARO



ING. EDUARDO ANTONIO FERMAN ARANA



ING. FRANCISCO ERNESTO COLORADO GUTIERREZ



ING. ROOSELVEY ADOLFO OSORIO
SECRETARIO GENERAL



UNIVERSIDAD TÉCNICA LATINOAMERICANA

ACTA DE CALIFICACIÓN DE
DEFENSA DE TRABAJO DE GRADUACIÓN

No. TRES MIL CIENTO SETENTA Y UNO

A las nueve horas y quince minutos, del sábado veintiséis de agosto de dos mil veintitrés. Reunidos los Miembros del Tribunal Examinador del Trabajo de Graduación presentado por NICOLAS ERNESTO CASTANEDA BARILLAS, en el salón de sesiones de la UNIVERSIDAD TÉCNICA LATINOAMERICANA. Se procedió:

PRIMERO: Que habiendo analizado el Trabajo de Graduación titulado:

"IMPLEMENTACION DE UN SISTEMA DE CONTROL DE TEMPERATURA Y DETECCION DE MASCARILLA, DE TIPO BIOMETRICO; PARA LA PREVENCIÓN DE COVID-19, EN LA UNIVERSIDAD TECNICA LATINOAMERICANA."

Se dio por aprobada, la parte escrita.

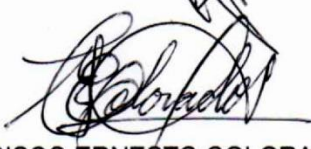
SEGUNDO: Que, con base a dicha aprobación de la parte escrita, se procedió a instalar la respectiva defensa oral del trabajo.

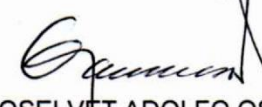
De conformidad a los resultados en dicha defensa, este Tribunal Examinador acuerda dar por APROBADO, con una calificación de *SIETE PUNTO OCHO (7.8)*, el Trabajo de Graduación presentado por el alumno arriba detallado, obteniendo a partir de esta fecha su calidad de: INGENIERO EN ELECTRONICA

No habiendo más que hacer constar, damos por terminada el acta que firmamos.


ING. GUSTAVO RAUL ALFARO


ING. EDUARDO ANTONIO FERMAN ARANA


ING. FRANCISCO ERNESTO COLORADO GUTIERREZ


ING. ROOSELVET ADOLFO OSORIO
SECRETARIO GENERAL



UNIVERSIDAD TÉCNICA LATINOAMERICANA

ACTA DE CALIFICACIÓN DE
DEFENSA DE TRABAJO DE GRADUACIÓN

No. TRES MIL CIENTO SETENTA Y DOS

A las nueve horas y quince minutos, del sábado veintiséis de agosto de dos mil veintitrés. Reunidos los Miembros del Tribunal Examinador del Trabajo de Graduación presentado por OSCAR ROLANDO MANCIA ROSALES, en el salón de sesiones de la UNIVERSIDAD TÉCNICA LATINOAMERICANA. Se procedió:

PRIMERO: Que habiendo analizado el Trabajo de Graduación titulado:

"IMPLEMENTACION DE UN SISTEMA DE CONTROL DE TEMPERATURA Y DETECCION DE MASCARILLA, DE TIPO BIOMETRICO; PARA LA PREVENCIÓN DE COVID-19, EN LA UNIVERSIDAD TECNICA LATINOAMERICANA."

Se dio por aprobada, la parte escrita.

SEGUNDO: Que, con base a dicha aprobación de la parte escrita, se procedió a instalar la respectiva defensa oral del trabajo.

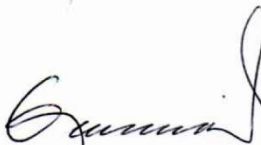
De conformidad a los resultados en dicha defensa, este Tribunal Examinador acuerda dar por APROBADO, con una calificación de **OCHO PUNTO OCHO (8,8)**, el Trabajo de Graduación presentado por el alumno arriba detallado, obteniendo a partir de esta fecha su calidad de: INGENIERO EN ELECTRONICA

No habiendo más que hacer constar, damos por terminada el acta que firmamos.


ING. GUSTAVO RAUL ALFARO


ING. EDUARDO ANTONIO FERMAN ARANA


ING. FRANCISCO ERNESTO COLORADO GUTIERREZ


ING. ROOSELVEY ADOLFO OSORIO
SECRETARIO GENERAL



Índice

Introducción.....	i
Capítulo I: Planteamiento del Problema	1
1.1 Antecedentes	1
1.1.3 <i>Cómo se propaga el COVID-19</i>	2
1.1.4 <i>Los síntomas más habituales del COVID-19</i>	2
1.1.5 <i>Criterios clínicos del diagnóstico COVID-19</i>	3
1.1.6 <i>Prevenciones</i>	5
1.2. Generalidades del proyecto	6
1.3. Formulación del problema	8
1.4 Descripción del proyecto.	8
1.5 Importancia de la investigación.....	9
1.6 Justificación	9
1.7 Alcances del proyecto.....	9
1.8 Limitaciones.....	9
1.8.1. <i>Delimitaciones Espacial.</i>	10
1.8.2. <i>Delimitación Temporal</i>	10
1.9 Objetivos.....	11
1.9.1 <i>Objetivo general</i>	11
1.9.2. <i>Objetivos específicos</i>	11
1.10 Marco de referencia	12
1.10.1 <i>Antecedentes del tema de estudio.</i>	12
Capítulo II: Generalidades, conceptos básicos.....	13
2.1. Concepto de biometría	13
2.2. Evolución histórica de la biometría	13
2.3. Necesidad de la Biometría	16
2.4. Funcionamiento de un sistema biométrico.....	17
2.5. Sensores biométricos	18
2.5.1 <i>Sensores Ópticos</i>	18
2.5.2 <i>Sensores Termoeléctricos</i>	19
2.5.3 <i>Sensores Capacitivos</i>	20
2.5.4 <i>Sensores E-Field (de Campo Eléctrico)</i>	21

2.5.5 Sensores sin contacto	22
2.5.6 Micrófonos ópticos unidireccionales	22
2.6 Procesamiento de la información	23
2.6.1 Recolección De Datos.....	24
2.6.2 Transmisión.....	24
2.6.3 Procesado De Señal.....	25
2.6.4 Decisión.....	26
2.6.5 Almacenamiento.....	27
2.7 Clasificación de los sistemas biométricos.....	30
2.7.1 Huella dactilar	32
2.7.1.1 Identificando patrones.	32
2.7.1.2 Clasificación de la Huella.	33
2.7.1.3 Realce de la Huella.	33
2.7.2 Reconocimiento de iris.....	34
2.7.2.1 Funcionamiento.....	35
2.7.3 Geometría de la mano	35
2.7.4 Reconocimiento facial	37
2.7.4.1 Funcionamiento	37
2.7.5 Otros sistemas de reconocimiento facial	38
Capítulo III: La termografía infrarroja	39
3.1 Conceptos básicos de la termografía infrarroja.....	39
3.2. Ondas y espectro electromagnético	39
3.3 Termografía infrarroja.	43
3.4. Radiación electromagnética	45
3.5. Transmisión de calor.....	48
3.6. Emisividad y temperatura reflejada	49
3.7 Temperatura aparente reflejada	49
3.8 Reflexión	50
3.9 Las cámaras infrarrojas como herramientas contra el Covid-19.....	51
3.10 Tipos de cámaras térmicas: refrigeradas o no refrigeradas	52
3.11 Cámaras activas o pasivas	54
3.12 Aplicaciones	55
3.13 Fuentes de error en el análisis termográfico	57

Capítulo IV: Sistema de control de acceso	59
4.1 Definición Control de acceso	59
4.2 Tipos de control de acceso	60
4.2.1. <i>Tipos de control de acceso según el sistema de identificación que utilicen</i>	61
4.2.2. <i>Tipos de control de acceso según la conexión que necesiten</i>	61
4.3 Control de acceso a implementar	62
4.3.1. <i>Control de acceso ASI7213X-T1</i>	62
4.3.2. <i>Sistema de control de acceso ASI7213X-T1</i>	64
4.3.3. <i>Descripción de funcionamiento de sus componentes</i>	66
4.3.3.1 Pantalla.	66
4.3.3.2 Cámara de reconocimiento facial.	67
4.3.3.3 Compensación de luz.	68
4.3.3.4 Monitoreo de temperatura.	68
4.3.3.5 Configuración del monitoreo de temperatura en el control de acceso Dahua.	69
4.3.3.6 Opciones de uso de mascarilla.	71
4.4. Software SMARTPSS-AC	71
4.4.1. <i>Administración de dispositivos</i>	74
4.4.2. <i>Agregar dispositivo</i>	74
4.4.2.1 Adición de dispositivos mediante búsqueda automática.	75
4.4.2.2 Agregar dispositivo manualmente.	75
4.4.2.3. Importación de dispositivos en lotes.	77
4.4.2.4 Eliminación de dispositivo	77
4.5. Registro de usuarios	78
4.5.1 <i>Agregar usuarios en el control de acceso</i>	78
4.5.2 <i>Extraer usuarios al software SmartPPS-AC</i>	80
4.5.3 <i>Diagrama de bloques de la solución</i>	82
Capítulo V: Implementación del proyecto	83
5.1. Procedimiento de instalación y configuración de los controles de acceso	83
5.1.1. <i>Inicialización</i>	83
5.1.2. <i>Menú principal</i>	86
5.1.3. <i>Instalación física de los controles de acceso ASI7213X1-T1</i>	87
5.1.4. <i>Ubicación de geográfica.</i>	88
5.1.5. <i>Diseño arquitectónico</i>	89

5.1.5 Parametrización del sistema	91
5.1.6 Configuración de IP en los controles de acceso	92
5.1.7 Topología de instalación	93
5.1.8. Inversión económica del proyecto.....	94
5.2. Instalación de Software de administración del sistema (SmartPSS-AC).....	95
5.2.1. Requerimientos de sistema para instalación de software.....	95
5.2.2. Instalación de Software SmartPSS-AC.	96
5.3. Configuración de controles de acceso en el Software SmartPSS-AC.	99
5.3.1 Agregar controles de acceso al software SmartPSS-AC.....	100
5.3.2 Configuración de Hora	101
5.3.3 Extraer usuarios	103
5.3.4 Extraer Registros de asistencia.....	104
5.3.5 Creación de Horarios.....	105
5.3.5.1 Periodo de asistencia.	105
5.3.5.2 Turno de asistencia.	107
5.3.5.3 Horario de turno	107
5.3.6 Generación de reportes de asistencia.	108
Conclusiones	110
Recomendaciones	111
Bibliografía	112
Anexos.....	113
Anexo 1 Sensor infrarrojo y cable UTP.....	113
Anexo 2: Plano de instalación	117
Anexo 3: Pruebas efectuadas en los ingresos de las instalaciones	119

Índice de Figuras

Figura 1 Síntomas del Covid-19.....	3
Figura 2: Rasgos biométricos.....	i
Figura 3: Esquema de Sensor CCD.....	18
Figura 4: Sensor Termoeléctrico Fingerchip.....	19
Figura 5: Representación del funcionamiento del sensor termoeléctrico.....	20

Figura 6: Principio funcionamiento del lector capacitivo de huella digital	21
Figura 7: Micrófono óptico unidireccional	23
Figura 8: Esquema de procesamiento de la información	23
Figura 9: Grafica de tasa de error de cruce	29
Figura 10: Esquema de funcionamiento del control de acceso	29
Figura 11: Esquema de los tipos de sistemas biométricos	30
Figura 12: Clasificación de rasgos de una huella dactilar	32
Figura 13 Representación de procesamiento de minutas de la huella dactilar	33
Figura 14: Ojo del ser humano	34
Figura 15: Reconocimiento de la palma de la mano	36
Figura 16 Reconocimiento facial	37
Figura 17: Espectro electromagnético	41
Figura 18: Esquema de metodología de captura termográfica	44
Figura 19: Medición móvil no ionizante	46
Figura 20: Medición realizada con un analizador de espectro	47
Figura 21: Gráfica de longitud de onda	48
Figura 22: Diferencia entre los conceptos de emisividad, transmitancia y reflectancia	49
Figura 23: Reflexión de un haz de luz	50
Figura 24: Refracción de un haz de luz	51
Figura 25: Imágenes térmicas del movimiento en alta velocidad un neumático (Izq.) tomada por una cámara refrigerada y la capturada por una cámara no refrigerada (Der.)	52
Figura 26: Imágenes térmicas del comportamiento de una PCB (Izq.) tomada por una cámara refrigerada y la capturada por una cámara no refrigerada (Der.)	53
Figura 27: Imágenes térmicas de la huella de una mano cámara refrigerada (Izq.) y captura por una cámara no refrigerada (Der.)	54
Figura 28: Control de acceso DAHUA ASI7213X-T1	63
Figura 29: Parámetros de configuración temperatura control de acceso	65
Figura 30: Pagina web de inicio de sesión	66
Figura 31: Sensor capacitivo touch	66
Figura 32: Sensor cámara CMOS	67
Figura 33: Cámara termográfica	69

Figura 34: Parámetros de activación de monitoreo de temperatura	70
Figura 35: Unidades disponibles en el sistema biométrico (°C y °F)	70
Figura 36: Parámetros de activación de máscara en el sistema.....	71
Figura 37: Página principal del Software SmatPSS	72
Figura 38: Búsqueda automática	75
Figura 39: Parámetros de configuración IP.....	76
Figura 40 : Ruta de importación de dispositivos.....	77
Figura 41: Confirmación de borrado de dispositivo.....	78
Figura 42: Interface gráfica del control de acceso ASI7213X-T1	78
Figura 43: Menú principal del control de acceso	79
Figura 44: Parámetros de usuario en el control de acceso	79
Figura 45: Listado de usuarios enrolados en el sistema	80
Figura 46: Extraer usuario.....	81
Figura 47: Selección de dispositivo	81
Figura 48: Información de usuarios en el control de acceso	82
Figura 49 Diagrama de bloques de la solución	82
Figura 50 Inicio de sesión	83
Figura 51 Página principal del Control de acceso DHI-ASI7213X-T1	85
Figura 52 Menú administración	86
Figura 53 Menú principal.....	87
Figura 54 Guía de instalación.....	88
Figura 55 Ubicación geográfica del Campus UTLA.....	88
Figura 56 Ubicación geográfica Laboratorio Especializado	89
Figura 57: Modelo arquitectónico de instalación.....	90
Figura 58: Diseño arquitectónico vista frontal.....	90
Figura 59: Diseño arquitectónico Laboratorio Especializado	91
Figura 60 Topología	93
Figura 61 Topología con enlace entre los dos sitios	94
Figura 62: Carpeta de instalador del Software	96
Figura 63: Ejecutable del Software SmartPSSAC.	97
Figura 64: Acuerdo de Licencia	97

Figura 65: Configuración de contraseña	98
Figura 66: Preguntas de seguridad	98
Figura 67: Pagina de acceso de credenciales Software SmartPSS	99
Figura 68: Página de Inicio del Software SmartPSS	99
Figura 69: Acceso a configuración de dispositivos	100
Figura 70: Lista de dispositivos	100
Figura 71: Configuración IP	101
Figura 72: Estado de dispositivos disponibles	101
Figura 73: Configuración de equipo seleccionado	101
Figura 74: Ventana de configuración de dispositivo	102
Figura 75: Configuración de hora	102
Figura 76: Iconos de extracción de reportes	103
Figura 77: Ventana de extracción de Usuarios	104
Figura 78: Ventana de extracción de registros	105
Figura 79: Ventana de selección de asistencia	106
Figura 80: Periodos de asistencia.	106
Figura 81: Turnos de asistencia	107
Figura 82: Lista de horarios	108
Figura 83: Ventana de informes	109

Índice de tablas

Tabla 1: Comparación de rasgos biométricos generales	31
Tabla 2: Clasificación de la radiación electromagnética según sus características	46
Tabla 3: Emisividad de los materiales	58
Tabla 4 : Descripción de funciones de la página de inicio Software SmartPSS	72
Tabla 5: Descripción de parámetros IP	76
Tabla 6: Iconos comunes del control de acceso	84
Tabla 7: Descripción de partes de la página principal	85
Tabla 8: Parametrización de los sistemas de control de accesos	91
Tabla 9: Configuración IP de los controles de acceso	92

Tabla 10: Listado de costo de equipos y materiales.....95

Tabla 11: Descripción de parámetros hora.....103

Introducción

Nuestro proyecto de investigación consiste en el estudio e implementación de un sistema de control de temperatura y detección de mascarilla, para la prevención de contagios de COVID-19. El objetivo del desarrollo de este sistema es apoyar a la UTLA en el contexto de bioseguridad social que vivimos actualmente.

Un sistema biométrico en general consta de componentes tanto de hardware como de software necesarios para el proceso de tomar datos como temperatura y uso de mascarilla. En el desarrollo capitular del trabajo, escribiremos cada una de las partes que lo conforman, su funcionamiento e implementación.

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, u organismo vivo con un determinado grado de precisión y confiabilidad.

Haciendo uso de estos sistemas, utilizaremos una funcionalidad específica, consistente en la medición de temperatura por medio de cámaras termográficas, siendo estas actualmente muy usadas por su confiabilidad y precisión.

Este sistema será de mucha utilidad para la Universidad Técnica Latinoamericana tanto para la medición de temperatura como para la identificación facial de personas, obviando procedimientos tradicionales que pudieran ser vulnerados. La funcionalidad automática de toma de temperatura y uso correcto de mascarilla, provee una ventaja sobre los mecanismos tradicionales, este sistema almacenará una bitácora electrónica de registro de acceso y datos, este registro ayudará obteniendo un historial de parámetros que apoyaran en la prevención de la pandemia, lo cual actualmente se hace de forma manual en la UTLA.

Capítulo I: Planteamiento del Problema

1.1 Antecedentes

COVID 19: nombre de la enfermedad causada por el virus SARS-CoV-2, según lo acordado por la Organización Mundial de la Salud, la Organización Mundial de Sanidad Animal y la Organización de las Naciones Unidas para la Alimentación y la Agricultura.

SARS-CoV-2: Coronavirus 2 del síndrome respiratorio agudo severo. El nombre formal del coronavirus que causa COVID-19, según lo determinado por el Comité Internacional de Taxonomía de Virus. Anteriormente, este coronavirus se conocía comúnmente como 'nuevo coronavirus 2019 (2019-nCoV)'.

1.1.2 La enfermedad COVID 19.

El SARS-CoV-2 es el agente infeccioso que causa COVID-19. El SARS-CoV-2 es un nuevo coronavirus que se identificó por primera vez en humanos en Wuhan, China, en diciembre de 2019. El SARS-CoV-2 comparte el 80% de la identidad de la secuencia con el SARS-CoV-1. Los coronavirus son una gran familia de virus, algunos causan enfermedades en las personas y otros que circulan entre los animales, incluidos camellos, gatos y murciélagos. Los coronavirus humanos causan enfermedades leves en los seres humanos, como los coronavirus que causan el resfriado común. En raras ocasiones, los coronavirus animales pueden evolucionar e infectar a las personas y luego propagarse entre las personas. Las mutaciones que permiten la transmisión de persona a persona han dado lugar a brotes de enfermedades respiratorias agudas graves debidas al MERS-CoV y al SARS-CoV.

Estudio mundial convocado por la OMS sobre los orígenes del SARS-CoV-2: parte de China, sugiere que los murciélagos y los pangolines pueden ser el reservorio del SARS-CoV-2. Si bien los coronavirus más altamente relacionados con el SARS-CoV-2 se encuentran en murciélagos y pangolines, no son lo suficientemente similares como para confirmarse definitivamente como reservorio. Se requieren más investigaciones para confirmar el origen del SARS-CoV-2.

1.1.3 Cómo se propaga el COVID-19

El COVID-19 se propaga cuando una persona infectada exhala gotitas y partículas respiratorias muy pequeñas que contienen el virus. Estas gotitas y partículas respiratorias pueden ser inhaladas por otras personas o depositarse sobre sus ojos, nariz o boca. En algunas circunstancias, pueden contaminar las superficies que tocan. Quienes están a menos de 6 pies de distancia de una persona infectada tienen mayor probabilidad de infectarse.

Hay tres formas principales en las que se propaga el COVID-19:

- Al inhalar estando cerca de una persona infectada que exhala pequeñas gotitas y partículas respiratorias que contienen el virus.
- Al hacer que estas pequeñas gotitas y partículas respiratorias que contienen el virus se depositen sobre los ojos, nariz o boca, especialmente a través de salpicaduras y aspersiones como las generadas al toser o estornudar.
- Al tocarse los ojos, la nariz o la boca con las manos contaminadas con el virus.

1.1.4 Los síntomas más habituales del COVID-19

Los síntomas más habituales del COVID-19 son la fiebre, la tos seca y el cansancio. Otros síntomas menos frecuentes que afectan a algunos pacientes son los dolores y molestias, la congestión nasal, el dolor de cabeza, la conjuntivitis, el dolor de garganta, la diarrea, la pérdida del gusto o el olfato y las erupciones cutáneas o cambios de color en los dedos de las manos o los pies. Estos síntomas suelen ser leves y comienzan gradualmente. Algunas de las personas infectadas solo presentan síntomas levísimos (OMS, 2020).

Alrededor de 1 de cada 6 personas que contraen la COVID-19 desarrolla una enfermedad grave y tiene dificultad para respirar. Las personas mayores y las que padecen afecciones médicas subyacentes, como hipertensión arterial, problemas cardíacos o diabetes, tienen más probabilidades de desarrollar una enfermedad grave. En torno al 2% de las personas que han contraído la enfermedad han muerto. Las personas que tengan fiebre, tos y dificultad para respirar deben buscar atención médica.

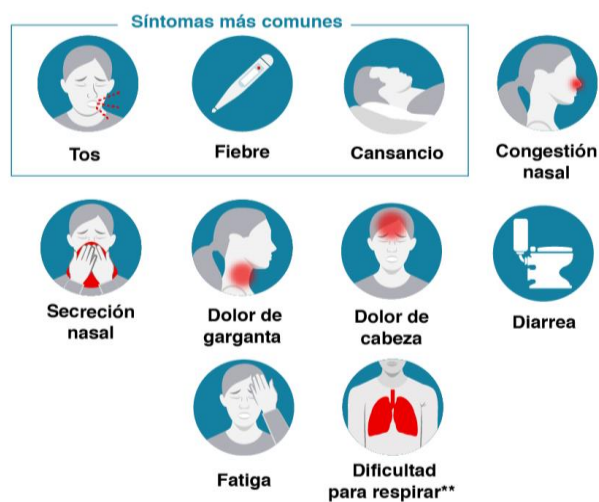


Figura 1 Síntomas del Covid-19

1.1.5 Criterios clínicos del diagnóstico COVID-19

En ciertas enfermedades a las cuales a través del estudio se le establecen signos y síntomas característicos no necesariamente patognomónicos pero que están presentes en las manifestaciones frecuentes de las enfermedades por lo cual a la enfermedad COVID-19 los criterios clínicos de diagnóstico son: fiebre, tos, mialgias y disnea. Sin embargo, siempre los estudios pueden revelar nueva información por lo cual no descartamos que haya manifestaciones atípicas.

1. Tos: suele ser una tos seca, no productiva, irritativa. Es una tos inespecífica que en este tiempo invernal puede ser debida a cualquier proceso infeccioso de vía alta o en una semana a un proceso alérgico. Posiblemente por su inespecificidad no es un síntoma guía.

2. Fiebre: No hay un criterio homogéneo. Según diferentes estudios descriptivos realizados en China se han recogido muestras positivas en pacientes con temperaturas entre 37,3 y 37,5 (sin determinarse la localización de la toma de temperatura). La OMS propone temperaturas a partir de 38°C. Tampoco se trata de un síntoma/signo clave.

3. Disnea: No es necesaria para su diagnóstico, aunque la presencia de disnea es muy frecuente en casos de sospecha de infección por COVID-19. Puede asociar astenia, mialgias, rash cutáneo e incluso clínica digestiva.

Exploración para el diagnóstico COVID-19

En toda investigación sobre patologías debemos realizar un examen médico general debido al grado de transmisibilidad de la enfermedad, el rigor de este examen cambia para preservar la salud del personal y minimizar el contagio por lo cual algunos autores recomiendan que en la exploración hemos de atender a 4 variables fundamentales:

1. Estado general: nivel de conciencia, piel, temperatura corporal.
2. Frecuencia cardiaca y respiratoria.
3. Saturación de oxígeno.
4. Auscultación cardiopulmonar. (ACP).

Diagnóstico de laboratorio

En el caso del diagnóstico de laboratorio algunas fuentes citan que es confirmatorio pero debido a la cantidad de personas expuestas a este nuevo virus se vuelve difícil realizar la prueba de laboratorio a todos los afectados o expuestos, por tal motivo ahora la indicación de una prueba de laboratorio será sobre todo en aquellos casos donde se tenga incertidumbre o como tamizaje para aquellas personas asintomáticas que acudan a los servicios de salud donde se cuente con el método diagnóstico.

Para este fin solo se cuenta con las siguientes pruebas:

- ❖ A. Detección de antígeno y ácido nucleico Los antígenos de coronavirus presentes en las células de secreciones respiratorias pueden detectarse utilizando la prueba de ELISA si se dispone de un antisuero de gran calidad.

Se pueden encontrar coronavirus entéricos con el análisis de muestras de heces en el microscopio electrónico.

Se prefieren los métodos de reacción en cadena de polimerasa (PCR, polymerase chain reaction) para buscar el ácido nucleico del coronavirus en secreciones respiratorias y muestras de heces.

La viremia con los coronavirus SARS y MERS se detecta en el plasma por medio de PCR.

- ❖ B. Aislamiento e identificación del virus El aislamiento de los coronavirus humanos en cultivo celular ha sido difícil. Sin embargo, el virus del SARS se aisló de muestras de la bucofaringe con la utilización de células renales de mono Vero.
- ❖ C. Diagnóstico serológico Dada la dificultad del aislamiento del virus, el diagnóstico serológico utilizando sueros en etapa aguda y convaleciente es el medio práctico de confirmar las infecciones por coronavirus para propósitos epidemiológicos.

Es posible llevar a cabo un enzimoimmunoanálisis de adsorción, métodos indirectos de anticuerpos inmunofluorescentes, y estudios de hemaglutinación. El diagnóstico serológico de las infecciones por la cepa 229E es factible al usar una prueba de hemaglutinación pasiva en la cual los 36 sueros que contienen anticuerpo aglutinan los eritrocitos recubiertos con antígeno de coronavirus.

1.1.6 Prevenciones

En el Protocolo de seguridad sanitaria y contención de COVID-19 de las Instituciones de Educación Superior para una apertura gradual de actividades podemos destacar las siguientes recomendaciones para el personal administrativo, académico y estudiantes:

a. Antes de ingresar a las instalaciones, cada uno de los miembros del personal deberá colocarse la respectiva mascarilla que le sea proveída por la IES. Dicha mascarilla será de uso permanente y obligatorio dentro de las instalaciones; debiéndose observar su uso correcto, esto es, cubriendo completamente nariz y boca.

b. Se les desinfectarán las suelas de los zapatos con una solución de lejía/agua en relación 1:5, o si prefiere amonio cuaternario a razón de 400 ppm. Para lo anterior se contará con pediluvios en todas las entradas de personal desde el exterior y en la entrada de cada uno de los respectivos edificios que constituyen el *campus*; posteriormente habrá una superficie para retirar el exceso de líquido, disminuyendo así el riesgo de caídas.

c. **Se le tomará la temperatura corporal** a cada uno de los empleados antes de su ingreso a las instalaciones, utilizando para ello un termómetro infrarrojo Y SE LLEVARÁ REGISTRO de cada empleado; esto con el propósito de tener una hoja de antecedentes que permita detectar de

manera temprana cambios en la temperatura de un empleado de manera lineal en el tiempo. para la toma de temperatura deberá respetar el distanciamiento social no menor a 2.00 metros. La temperatura puede ser tomada en cualquier parte del cuerpo

d. Inmediatamente después de la toma de temperatura pasará cada uno de los empleados a realizarse un lavado de manos de acuerdo al protocolo establecido para ello.

e. Cuando se esté en los vestidores o en área de baños y lavamanos, habrá un distanciamiento social no menor a 2.00 metros e ingresarán en grupo cuyo número dependerá de las dimensiones del área de baños o lavamanos.

1.2. Generalidades del proyecto

La biometría en su forma elemental existe desde hace varios siglos, se tienen reseñas históricas sobre la época de los faraones la cual se practicaban en el Valle del Río Nilo (Egipto), la biometría constaba en principios básicos para identificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

En la antigüedad, han sido identificadas por diversas características físicas y morfológicas, tales como cicatrices, medidas corporales, color de ojos, tamaño de la dentadura, etc. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenadas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para este efecto las formas de identificación mencionadas las cuales son competencia de la biometría.

La biometría no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En el siglo XIX comienzan las investigaciones científicas acerca de la biometría con el fin de buscar un sistema de identificación de personas con fines judiciales.

En Occidente, la identificación confiaba simplemente en la "memoria fotográfica" hasta que Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló el sistema antropométrico (también conocido más tarde como Bertillonage) en 1883. Este era el primer sistema preciso, ampliamente utilizado científicamente para identificar a criminales y convirtió a la biométrica en un campo de estudio.

Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema - principalmente problemas con métodos distintos de medidas y cambios de medida. Después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar - esencialmente el mismo sistema visto en China cientos de años antes.

En estos últimos años la biométrica ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas físicas y de comportamiento. Las aplicaciones de la biometría también han aumentado - desde sólo identificación hasta sistemas de seguridad y más.

Con los avances en estas investigaciones en el campo de la biometría, se producen importantes avances en la identificación de personas con base en su morfología y se comienzan a surgir aplicaciones relacionadas en este ámbito.

En el siglo XX, la mayoría de los países del mundo utilizan las huellas digitales como sistema práctico y seguro de identificación, esto da inicio al desarrollo de nuevos instrumentos para la verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo, el iris del ojo, el calor facial o la voz.

Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación humana.

Los términos "Biometrics" y "Biometry" se han usado en el siglo XX para referirse al campo de desarrollo de métodos estadísticos y matemáticos aplicables a los problemas de análisis de datos en las ciencias biológicas. Es decir, son métodos estadísticos para el análisis de datos de los experimentos.

Recientemente, el término Biometría también se ha usado para referirse al campo de la tecnología dedicada a la identificación de individuos usando los rasgos biológicos, tales como escaneos de retina o de iris, huellas dactilares y reconocimiento facial.

A finales del año 2019, se dio a conocer una noticia en algunos medios de comunicación en la cual se mencionó que, en Wuhan china, se había descubierto el surgimiento de una nueva enfermedad viral, en nuestro país solo se escuchaba en noticieros internacionales. El 11 de febrero de 2020, la OMS anunció la existencia de la nueva enfermedad mencionada y fue denominada «COVID-19 (por sus siglas en inglés y año de aparición 2019)».

Para evitar la propagación del Covid-19, además del uso de mascarillas y el lavado frecuente de manos, también se aplica la toma de temperatura, ya que la fiebre es uno de los síntomas más comunes en las personas contagiadas. Los expertos en bio seguridad afirman que el uso de termómetros sin contacto, reduce el riesgo de contaminación cruzada y minimiza el riesgo de transmisión de enfermedades. Por esta razón, como estudiantes de ingeniería electrónica, deseamos contribuir con estas medidas, apoyando con herramientas tecnológicas para la prevención de la propagación del virus en nuestra Universidad.

1.3. Formulación del problema

¿De qué forma la Universidad Técnica Latinoamericana puede optimizar el control de la bioseguridad a partir de la medición de temperatura corporal y uso de mascarilla al flujo de personas al ingresar a sus instalaciones con el fin de detectar posibles casos de Covid-19 y contribuir en el control de su propagación?

1.4 Descripción del proyecto.

Implementación de un sistema biométrico de reconocimiento facial, que detecta el uso correcto de mascarilla y control de temperatura, a su vez, nos brindará un registro de ingreso y retiro de las instalaciones del personal administrativo que se presente a las instalaciones del campus universitario de la UTLA.

Este sistema consiste de una pantalla de 7 “pulgadas equipado con sensores y cámaras termográficas que permiten captar datos biométricos ya descritos el usuario solo deberá de colocarse frente al control de acceso y el equipo tomará automáticamente los datos con lo cual se

estaría identificando riesgos de posibles contagios de COVID-19 al restringir el acceso a las instalaciones de personas con sospechas de portar el virus.

1.5 Importancia de la investigación

El 2022 proyecta una progresiva incorporación de, las actividades normales cotidianas en el ámbito social, tales como las actividades comerciales, administrativas, las actividades educativas no son la excepción, de cara a una normalización completa de las clases presenciales, La implementación del sistema mencionado concretizado en los dispositivos mencionados, le dará un valor agregado a la UTLA en su quehacer diario con el flujo de personas concurrentes en las instalaciones (estudiantes, docentes, personal administrativo, visitantes)

1.6 Justificación

La justificación de la implementación de nuestro proyecto radica en “contribuir a evitar la propagación del Covid-19, basándonos en la lectura de la temperatura de cada persona que ingrese a las instalaciones de la UTLA, reforzando las otras medidas implementadas como el uso adecuado de mascarillas y el lavado frecuente de manos, considerando como probable portadora del virus a la persona que refleja una temperatura por encima de los valores normales (36.5 Celsius).

1.7 Alcances del proyecto

La implementación del proyecto está dirigida a la población de la UTLA, estableciendo un control en los puntos de mayor afluencia de personas en el campus universitario, estos son la entrada al campus y el laboratorio especializado, con el fin de cumplir con el protocolo de bioseguridad a través de la medición de temperatura corporal denegando el ingreso al detectar temperatura anormal considerando que puede tratarse de un caso potencial del COVID-19 contribuyendo de esta manera a evitar su propagación.

1.8 Limitaciones

La delimitación de la investigación se basa en dos tipos, los cuales se presentan a continuación:

1.8.1. Delimitaciones Espacial.

El proyecto se implementó en dos espacios geográficos. La finalidad es poder tener monitoreado a visitantes en las distintas instalaciones de la Universidad Técnica Latinoamericana UTLA según se detalla a continuación:

Universidad Técnica Latinoamericana EDIFICIO A-B-C-D, 3ª Avenida Norte, 1501 - Santa Tecla, Departamento de La Libertad, Ubicación Geográfica Latitud: 13.677979668948687, Longitud: -89.28590085898509, Datos de contacto: Teléfono +503 22284775, +503 22284380. Correo Electrónico: comunicaciones@utla.edu.sv

Laboratorios especializados de la Universidad Técnica Latinoamericana UTLA, 3ª Avenida Norte Y 7ª Calle Oriente No. 5-1, - Santa Tecla, Departamento de La Libertad, Ubicación Geográfica Latitud: 13.679121156248451, Longitud: -89.28921875150377. Datos de contacto: Teléfono +503 22284775, +503 22284380. Correo Electrónico: comunicaciones@utla.edu.sv

1.8.2. Delimitación Temporal

La implementación se desarrolló en el periodo comprendido de mayo a noviembre del 2022

1.9 Objetivos

1.9.1 *Objetivo general*

- Implementar un sistema de control biométrico para monitorear la temperatura y uso de mascarilla en puntos estratégicos de afluencia de personas para el ingreso a las instalaciones de la UTLA; personal administrativo, población estudiantil y visitantes.

1.9.2. *Objetivos específicos*

- Instalar en el acceso principal de la UTLA un control de acceso con tecnología de reconocimiento facial y medición térmica y uno en el acceso principal del Laboratorio Especializado.
- Configurar los controles de accesos para su correcta identificación del personal enrolado al sistema acceso.
- Instalar en un ordenador el software para la administración de los usuarios y generación de reportes de asistencia de personas enrolado.
- Describir las diferentes tecnologías utilizadas en la Bioseguridad aplicada en la medición de temperatura corporal.

1.10 Marco de referencia

1.10.1 Antecedentes del tema de estudio.

Una de las formas para identificar a posibles portadores del COVID-19 es la toma de temperatura corporal, está en muchos lugares se hace de forma manual o automática usualmente sin contar con registros y controles de acceso. En el caso de la UTLA, esto se hace actualmente de forma manual.

En la actualidad, las tecnologías biométricas se presentan como las soluciones favoritas de las compañías para el control de accesos, en lo referente al COVID-19, estas son utilizadas para identificar riesgos de posibles contagios en las instalaciones.

Con la implementación de sistemas biométricos en los controles de acceso, las instituciones están haciendo una verificación rápida y segura de la temperatura corporal de su personal, determinando así, a portadores de temperaturas altas de manera ágil.

La precisión que tiene este equipo en sus mediciones de temperatura es de $\pm 0,5^{\circ}\text{C}$, sin contacto ni manipulación manual, lo cual hace a esta opción, más eficiente que la manual

Con la utilización de estas soluciones biométricas aplicadas en los accesos, se contribuye en la identificación de riesgos de contagios de COVID-19 y, por ende, en la prevención de la diseminación de este, en los espacios de trabajo y grupos familiares asociados.

Capítulo II: Generalidades, conceptos básicos.

2.1. Concepto de biometría

El término biometría deriva de las palabras griegas bio, que significa vida, y metro, que significa medir. La biometría es la medición y el análisis estadístico de las características físicas y de comportamiento únicas de las personas. Esta tecnología se utiliza principalmente para la identificación y el control de acceso o para la identificación de individuos que están bajo vigilancia. La premisa básica de la autenticación biométrica es que toda persona puede ser identificada con precisión por sus rasgos físicos o de comportamiento intrínsecos.

La biometría trabaja en función del tipo de rasgo en cuestión. Pueden ser fisiológicas, como la huella dactilar, el rostro, el iris o la retina; o conductuales, como la voz, la firma o la forma de moverse, entre otros. Cabe destacar que las mediciones fisiológicas se consideran más confiables, puesto que no cambian (o no suelen hacerlo).

2.2. Evolución histórica de la biometría

La biometría se remonta siglos atrás donde se encontraron hallazgos arqueológicos en la época de los faraones, en el Valle del Nilo ya se utilizaban los principios básicos de la identificación biométrica para verificar a las personas que participaban en diferentes actividades comerciales y judiciales del antiguo Egipto.

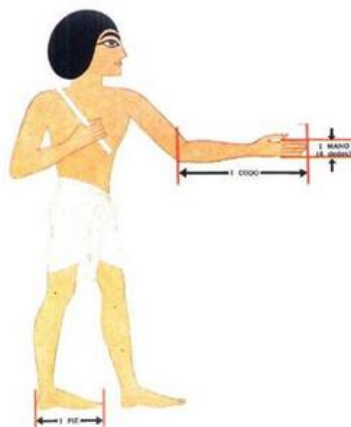


Figura 2: Rasgos biométricos

2600 A.C. En el antiguo Egipto, los trabajadores que construían las pirámides, medían a las personas para identificarlas (antropometría). Esta manera rudimentaria de identificación se basaba en las medidas de algunas partes del cuerpo y sigue siendo utilizada desde entonces.

Muchas son las referencias de personas que, en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura...Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenadas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como eran sus rasgos físicos.

500 A.C. Babilonia donde los reyes firmaban las tabletas de arcilla grabando las yemas de sus dedos antes de cocerlas. Más tarde, en China, durante la Dinastía Tang en el año 650 de nuestra era, se estableció que, para divorciarse de una mujer, el marido debía exponer siete motivos y firmar el documento con las huellas dactilares.

La biometría no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

Desde el siglo XVI los estudios de Malpighi sobre las capas de la piel, Purkinje con su clasificación de 9 tipos de formas de huellas dactilares, Faulds con la inmutabilidad de las huellas e impresión con tinta, Vucetich creador del primer método de clasificación de ficheros de huellas dactilares el cual fue utilizado para esclarecer un crimen, Galton con la confirmación de que las huellas dactilares son únicas y que no cambiaban a lo largo de la vida del individuo, enunció las tres leyes fundamentales de la Dactiloscopia: perennidad, inmutabilidad y diversidad infinita. Su hijo, quien continuó su investigación, estableció el cálculo de probabilidad de que dos huellas sean iguales en 1 en 64.000 millones. Henry en 1896 desarrolló en Scotland Yard e impuso el método de clasificación e identificación de huellas dactilares, en reemplazo de la antropometría, versión avanzada del método Galton, actualmente en uso en Europa y Norteamérica.

El FBI en 1969 contrató al Buró Nacional de Estándares (NBS), ahora Instituto nacional de Estándares y Tecnología (NIST), para estudiar el proceso automatización de la clasificación, búsqueda y concordancia de las huellas dactilares. Esta misma, institución en 1975 fundó el desarrollo de escáneres de huella dactilar para clasificadores automatizados y tecnología de extracción de minucias, lo cual condujo al desarrollo de un lector prototipo.

Conforme a la necesidad de un sistema de identificación integrado en la comunidad de la justicia criminal de los Estados Unidos se volvió rápidamente evidente, la próxima fase en la automatización de huellas dactilares ocurrió al finalizar la competencia de sistemas automatizados de identificación de huellas dactilares (Automated Fingerprint Identification System, IAFIS). La competencia identificó e investigó tres desafíos principales:

- A. Adquisición de huellas dactilares digitales
- B. Extracción de características de crestas locales.
- C. Concordancia de patrones de características de crestas

En el siglo XX, la mayoría de los países del mundo utilizan las huellas digitales como sistema práctico y seguro de identificación, esto da inicio al desarrollo de nuevos instrumentos para la verificación de huellas digitales. También se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo, el iris del ojo, el calor facial o la voz.

Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación humana.

Los términos "Biometrics" y "Biometry" se han usado en el siglo XX para referirse al campo de desarrollo de métodos estadísticos y matemáticos aplicables a los problemas de análisis de datos en las ciencias biológicas. Es decir, son métodos estadísticos para el análisis de datos de los experimentos.

Recientemente, el término Biometría también se ha usado para referirse al campo de la tecnología dedicada a la identificación de individuos usando los rasgos biológicos, tales como escaneos de retina o de iris, huellas dactilares y reconocimiento facial.

2.3. Necesidad de la Biometría

Durante todo el siglo pasado han sido muchas las empresas que han concentrado sus esfuerzos en desarrollar sistemas biométricos para garantizar su seguridad, así como lo han hecho los propios Departamentos de Defensa de varios países.

La biometría es un sistema automatizado, basado en el reconocimiento de las características físicas de determinadas partes del cuerpo de las personas, que son únicas e intransferibles como la huella dactilar, el iris o el rostro y es una forma de validar la identidad para prevenir fraudes.

Encontrar un sistema infalible e inequívoco para reconocer personas es el objetivo primordial de la biometría. Hoy en día contamos con una gran variedad de equipos capaces de identificar a las personas a partir de la información de alguna parte de su cuerpo como las manos, la retina, el iris, los dedos, las huellas dactilares, la voz, o la firma. Incluso se está investigando en la posibilidad de crear un sistema basado en el ADN.

Para los expertos, “la biometría es ideal para la autenticación porque los usuarios no necesitan recordar contraseñas complicadas. La biometría también impide que se compartan las credenciales de autenticación, a diferencia de otros factores que no están vinculados de manera exclusiva a la persona”.

De esta forma con los sistemas biométricos que reconocen las características singulares de las huellas digitales, por ejemplo, se logra evitar fraudes en la banca, en el sistema de salud por suplantación de pacientes, controlar el acceso en el desplazamiento de seres humanos al interior de las empresas, tiempos desperdiciados, accesos no deseados; sin necesidad de utilizar contraseñas, carnés, tarjetas magnéticas u otros medios de identificación vulnerables. Esto hace que los sistemas biométricos sean el medio, más rápido y seguro mediante la utilización de la huella digital como validador de operaciones y de control de acceso.

La autenticación biométrica y sus usos en la tecnología moderna y las aplicaciones digitales tienen una serie de ventajas:

1. Alta seguridad y fiabilidad.
2. Experiencia de usuario: Práctica y rápida.

3. No es transferible: Cada persona tiene acceso a un conjunto de datos biométricos único.
4. A prueba de suplantación de identidad: Es difícil falsificar o robar datos biométricos.

A pesar del aumento de la seguridad, la eficacia y la comodidad, la autenticación biométrica y sus usos en las aplicaciones digitales y tecnológicas actuales también tienen desventajas:

1. Costos: Es necesario hacer una inversión significativa en biometría para seguridad
2. Violación de datos: Las bases de datos biométricas pueden ser hackeadas
3. Monitorización y datos: Los dispositivos biométricos, como los sistemas de reconocimiento facial, pueden limitar la privacidad de los usuarios.
4. Fallo: El aprendizaje automático y los algoritmos tienen que ser muy avanzados para minimizar el fallo demográfico biométrico.
5. Positivos falsos e imprecisiones: Es posible que ocurran falsos rechazos y falsas aceptaciones que impidan a los usuarios acceder al sistema.

2.4. Funcionamiento de un sistema biométrico

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad.

La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas, passwords, pin numbers, códigos u otros que sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos.

El funcionamiento de estos sistemas implica la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje. Éstas son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptografía se limita a un uso secundario como el cifrado de los datos biométricos almacenados en la base de datos o la transmisión de los mismos.

Los escáneres de huellas digitales y equipos de medición de geometría de la mano son los dispositivos más corrientemente utilizados. Independientemente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico.

2.5. Sensores biométricos

Un sensor biométrico es un transductor que transforma un rasgo físico y concreto de un ser humano en una señal eléctrica. Por lo general, el sensor interpreta o mide aspectos como la luz, la temperatura, la velocidad (en el caso de una voz, por ejemplo), y otro tipo de estímulos energéticos. Esto se consigue mediante sofisticadas combinaciones de redes de sensores y cámaras digitales o micrófonos cuya imagen o sonido son de alta precisión.

A continuación, se muestran diferentes tipos de sensores:

2.5.1 Sensores Ópticos

El método óptico es uno de los más comunes que suele estar formado por cámaras de vídeo de tipo CCD. Estos sensores se emplean tanto en reconocimiento de huella dactilar como de ojo.

El corazón de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada). Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI.

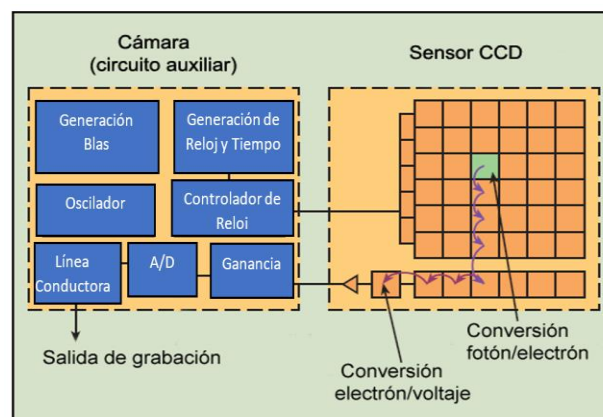


Figura 3: Esquema de Sensor CCD

Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la cámara), almacenando una pequeña carga de electricidad. Los píxeles se

encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

2.5.2 Sensores Termoeléctricos

El método termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip™ para reconocimiento de huella dactilar.

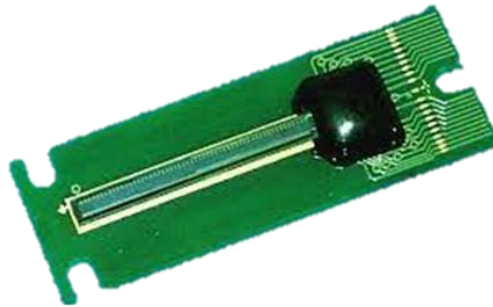


Figura 4: Sensor Termoeléctrico Fingerchip

El Fingerchip™ utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip™ obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris. El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran calidad incluso cuando las huellas dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

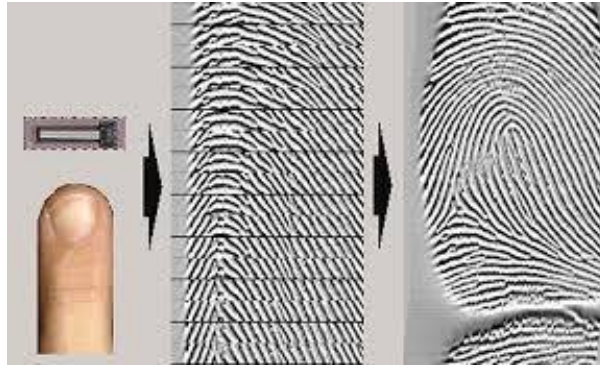


Figura 5: Representación del funcionamiento del sensor termoeléctrico

Además, también cuenta con la ventaja de autolimpieza del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores, sino que permite que se copie la huella para falsificar y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip™ funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta calidad y siempre un sensor limpio. La desventaja es que la calidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente.

Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar. El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona.

2.5.3 Sensores Capacitivos

El método capacitivo es uno de los más populares para reconocimiento de huella dactilar. Al igual que otro escáner, genera una imagen de las crestas y valles del dedo. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato.

Principio de funcionamiento del lector capacitivo de huella digital



Figura 6: Principio funcionamiento del lector capacitivo de huella digital

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor, tendremos un efecto de solapamiento sobre los platos (píxel) vecinos, lo que provocará que el área sensor aumente de tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen.

Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos óptimas en la piel. Cuando el dedo está sucio, con frecuencia no existirán aberturas de aire en los valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento. Entre las empresas líderes en este sector se encuentran: Infineon, Vericon, Sony y STMicroelectronics.

2.5.4 Sensores E-Field (de Campo Eléctrico)

El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del "mundo real", como por ejemplo piel húmeda, seca o dañada.

Esta tecnología para reconocimiento de huella dactilar origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador under-píxel para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma.

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Desde hace poco existe también un sensor más fuerte basado en esta tecnología que saldrá al mercado en pocos meses. Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

2.5.5 Sensores sin contacto

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico con la correspondiente distorsión de la imagen. Otro punto es que las huellas escaneadas son esféricas lo que origina un complejo algorítmico mucho más complejo.

2.5.6 Micrófonos ópticos unidireccionales

La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada. Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido. Es utilizado en reconocimiento de voz.

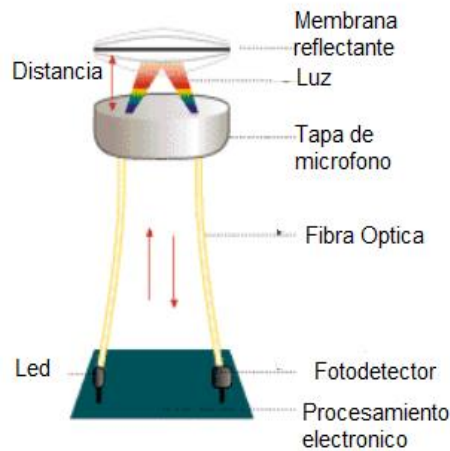


Figura 7: Micrófono óptico unidireccional

2.6 Procesamiento de la información

Los sistemas biométricos se basan en distintos procesos: registró, captura en vivo y la extracción y comparación de plantillas. El propósito del registro consiste en recoger y archivar las muestras biométricas y generar plantillas numéricas para futuras comparaciones. Esto, a su vez, es especialmente importante para la identificación biométrica en la búsqueda de “uno a muchos”.

Se puede considerar un sistema biométrico genérico de identificación, dividido en cinco subsistemas: recolección de datos, transmisión, procesamiento de la señal, decisión y almacenamiento de datos.

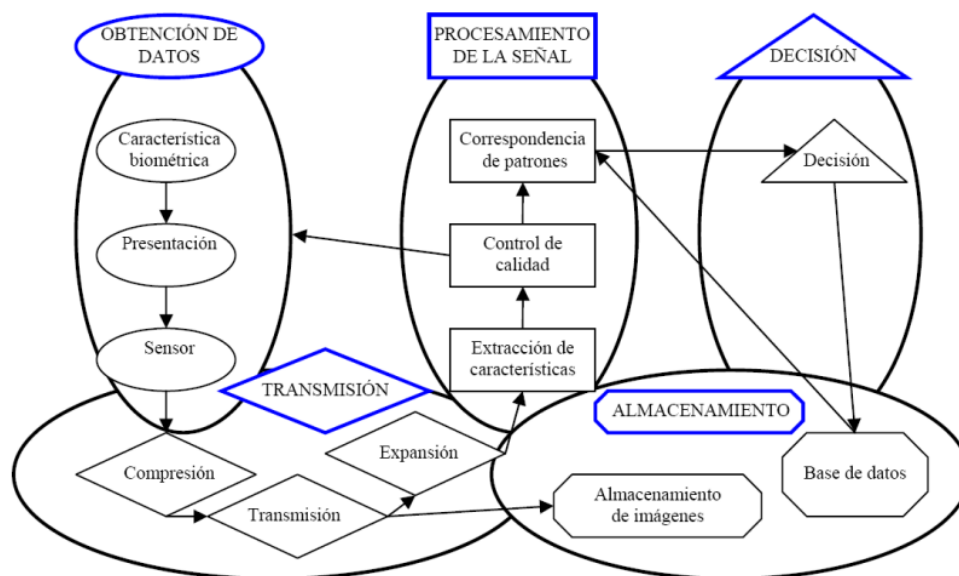


Figura 8: Esquema de procesamiento de la información

2.6.1 *Recolección De Datos*

Los sistemas biométricos comienzan con la medida de una característica del comportamiento o fisiológica. La clave de todos los sistemas es la hipótesis subyacente que la característica biométrica medida es distintiva entre los individuos y en un cierto plazo repetible para el mismo individuo.

Es decir, las características deben variar en gran magnitud entre individuos, pero deben variar muy poco para cada individuo de medida a medida. Los problemas en medir y controlar estas variaciones comienzan en el subsistema de la colección de datos. La característica del usuario se debe presentar a un sensor. Según lo observado ya, la presentación de la característica biométrica al sensor introduce un componente del comportamiento.

Los cambios inevitables en el comportamiento afectarán la capacidad de repetición y la distinción de la medida.

Si un sistema pretende ser abierto, presentación y sensor deben ser estandarizados para asegurar que la característica biométrica recogida sea la misma que recogería otro sistema para el mismo individuo.

2.6.2 *Transmisión*

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

El cuadro anterior muestra la compresión y la transmisión que ocurren antes de procesar la señal y del almacenamiento de la imagen.

En tales casos, los datos comprimidos transmitidos o salvados se deben descomprimir antes de que sean usados. El proceso de la compresión y de la descompresión causa generalmente pérdida de la calidad en la señal restablecida.

La técnica de compresión usada dependerá de la señal biométrica. Un campo de investigación interesante consiste en encontrar, para una técnica biométrica dada, métodos de compresión con impacto mínimo en el subsistema del proceso de señal.

Si un sistema es abierto, los protocolos de la compresión y de la transmisión deben ser estandarizados de modo que cada usuario de los datos pueda reconstruir (aunque con pérdida de la calidad) la imagen original.

Los estándares existentes actualmente son: para la compresión de la huella digital (WSQ)¹, de las imágenes faciales (JPEG)², y de los datos de la voz (CELP)³.

2.6.3 *Procesado De Señal*

Adquirida y transmitida una característica biométrica, debemos prepararla para corresponder con otra. El cuadro anterior divide el subsistema de proceso de señal en tres tareas: extracción, control de calidad, y concordancia con el modelo.

La primera meta es analizar el modelo biométrico verdadero de la presentación y las características del sensor, en presencia de las pérdidas por ruido y de señal impuestas por la transmisión.

La segunda meta, es preservar el modelo biométrico para que esas calidades que sean distintivas y repetibles, y desechar las que no lo sean, o sean redundantes.

En un sistema de reconocimiento de la voz, se deseará encontrar las características, tales como los lazos armónicos en las vocales, que dependen solamente del hablante y no de las palabras que son habladas.

Y, desearemos centrarnos en esas características que deberán ser invariantes incluso si el hablante está resfriado o no está hablando directamente en el micrófono.

Hay muchos acercamientos matemáticos para realizar estos procesos. En general, la extracción de la característica es una forma de compresión irreversible, significando esto que la imagen biométrica original no se puede reconstruir de las características extraídas.

En algunos sistemas, la transmisión ocurre después de la extracción de la característica para reducir el requisito de mínimo ancho de banda.

Después de la extracción de la característica, o quizá antes o durante, desearemos controlar si la señal recibida del subsistema de recolección de datos tiene la calidad requerida, a fin de solicitar si es necesario una nueva muestra del usuario.

El desarrollo de este proceso de "control de calidad" ha mejorado sensiblemente el funcionamiento de los sistemas biométricos en los últimos años.

¹ WSQ: Wavelet Scalar Quantization por sus siglas en ingles.

² JPG: Joint Photographic Experts Group por sus siglas en ingles.

³ CELP: Code Excited Linear Prediction por sus siglas en ingles.

El propósito del proceso de concordancia con el modelo es comparar una muestra actual con la característica de una muestra salvada, llamada un modelo, y enviar al subsistema de decisión la medida cuantitativa de la comparación.

Las distancias raramente, serán fijadas en cero, pues siempre habrá alguna diferencia relacionada con el sensor o relacionada con el proceso de transmisión o con el comportamiento propio del usuario.

2.6.4 Decisión

La política del sistema de decisión dirige la búsqueda en la base de datos, y determina los "coincidencia" o los "no-coincidencia" basándose en las medidas de la distancia recibidas de la unidad de procesamiento de señal.

Este subsistema toma en última instancia una decisión de "acepta/rechaza" basada en la política del sistema. Tal política podría ser declarar un "coincidencia" para cualquier distancia más baja que un umbral fijo y "validar" a un usuario en base de este solo "coincidencia", o la política podría ser declarar una "coincidencia" para cualquier distancia más baja que un umbral dependiente del usuario, variante con el tiempo, o variable con las condiciones ambientales.

Una política posible es considerar a todos los usuarios por igual y permitir sólo tres intentos con una distancia alta para la "coincidencia" para luego volver una medida baja de la distancia.

La política de decisión empleada es una decisión de la gerencia que es específica a los requisitos operacionales y de la seguridad del sistema. En general, bajar el número de no-coincidencia falsas se puede negociar contra levantar el número de coincidencias falsas.

La política óptima del sistema depende de las características estadísticas de las distancias de comparación que vienen de la unidad de "coincidencia" del modelo y de las penas relativas para la coincidencia falsa y la no-coincidencia falsa dentro del sistema.

En cualquier caso, en la prueba de dispositivos biométricos, es necesario evaluar el funcionamiento del subsistema de procesamiento de señal con independencia de las políticas puestas en ejecución mediante el subsistema de decisión.

2.6.5 Almacenamiento

El subsistema restante que se considerará es el del almacenamiento. Habrá una o más formas de almacenamiento a usar, dependiendo del sistema biométrico. Los modelos de la característica serán salvados en una base de datos para la comparación en la unidad de concordancia.

Para los sistemas que realizan solamente una correspondencia "uno a uno", la base de datos se puede distribuir en las tarjetas magnéticas llevadas por cada usuario. Dependiendo de la política del sistema, no es necesaria ninguna base de datos centralizada.

Aunque, en esta aplicación, una base de datos centralizada se puede utilizar para detectar tarjetas falsificadas o para reeditar tarjetas perdidas sin recordar el modelo biométrico.

Los requisitos de velocidad del sistema dictan que la base de datos esté repartida en subconjuntos más pequeños, tales que cualquier muestra de la característica necesita solamente ser correspondida con la de los modelos salvados en una partición. Esta estrategia tiene el efecto de aumentar velocidad del sistema y de disminuir concordancias falsas a expensas de aumentar la tasa de no-concordancias falsas. Esto significa que las tasas de error del sistema no son constantes con el aumento del tamaño de la base de datos y, además, esta relación no es lineal.

Por lo tanto, las estrategias para particionar la base de datos representan una decisión bastante compleja.

Si existe la posible necesidad de reconstruir los modelos biométricos a partir de los datos salvados, será necesario el almacenamiento de datos sin procesar.

El modelo biométrico, en general, no es reconstruirle a partir de los datos salvados. Además, los modelos son creados usando algoritmos propietarios de extracción de características, propios de cada fabricante. El almacenamiento de informaciones en bruto permite cambios en el sistema o de equipamiento sin que sea necesario registrar nuevamente a todos los usuarios.

Estos cinco pasos se refieren a la captación y verificación de una característica biométrica determinada de una persona, pero para que el sistema sea capaz de verificar dicha característica es necesario un paso previo a estos cinco en el que la persona debe registrarse en el sistema ("enroll en inglés"). Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como, por ejemplo, la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia ("reference template" en inglés.) El modelo de referencia debe ser guardado en una base de datos, una tarjeta inteligente ("smart card" en inglés), o en algún otro lugar del cual será extraído en cualquier ocasión futura para realizar la verificación.

A pesar de que es poco probable obtener dos tomas iguales aún del mismo individuo, a causa de diferencias ambientales y otras condiciones en el momento de la captura, el sistema aún debe poder funcionar correctamente. La mayoría de los algoritmos de comparación generan un ámbito para cada ensayo de comparación el cual es cotejado dentro de determinados umbrales antes de ser aceptados o rechazados.

Es en este punto donde entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Cada proveedor de tecnología biométrica configura la/el falsa/o aceptación / rechazo de forma diferente.

La figura siguiente muestra esta relación de compromiso.

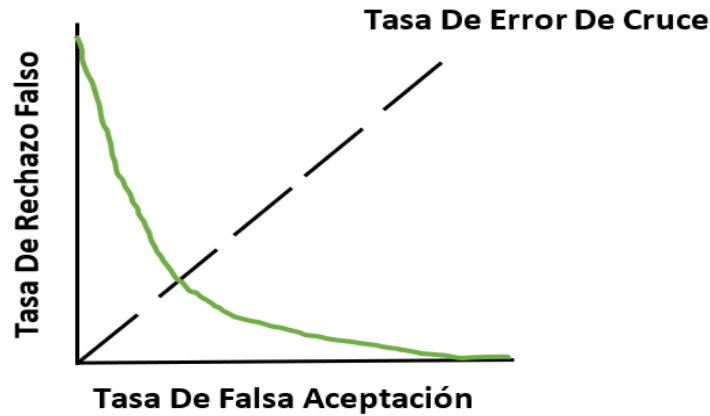


Figura 9: Grafica de tasa de error de cruce

Como puede observarse, si el umbral es demasiado bajo, se vuelve demasiado fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas.

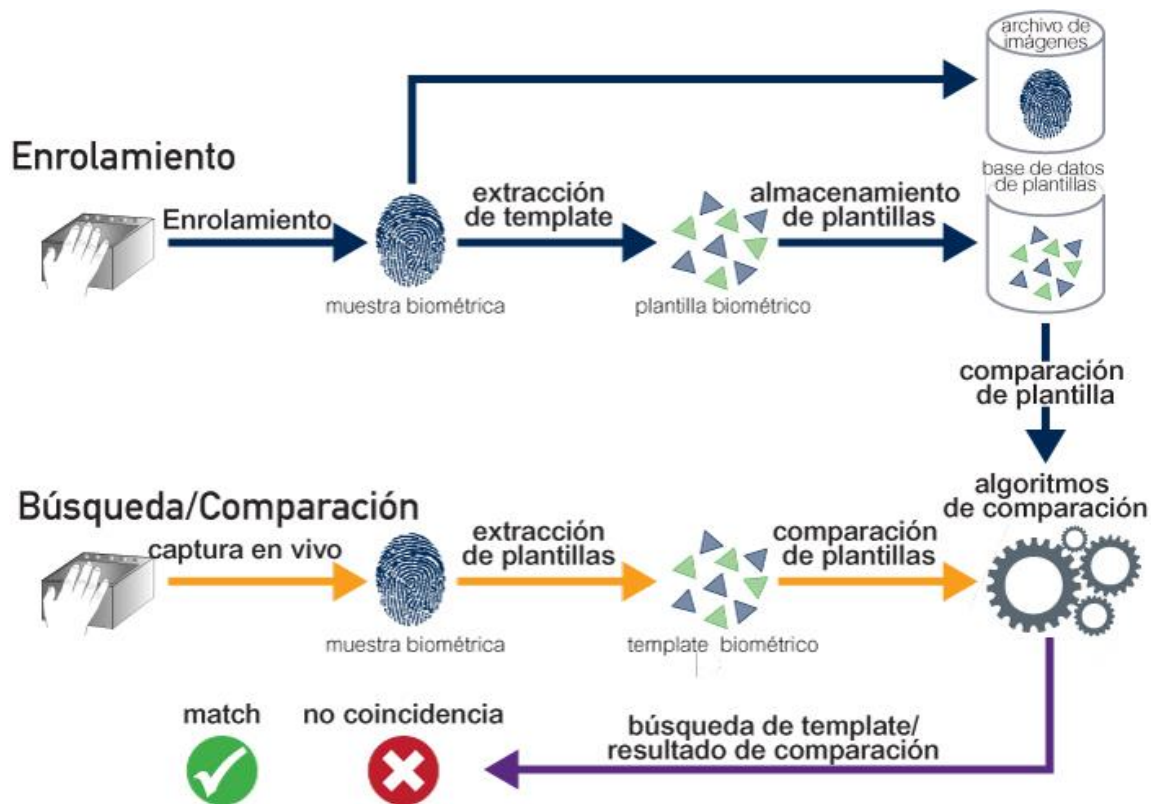


Figura 10: Esquema de funcionamiento del control de acceso

2.7 Clasificación de los sistemas biométricos

Aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento (por ejemplo, la medición de la biometría basada en huella digital variará de acuerdo a la manera en que se coloca el dedo), la clasificación de las técnicas biométricas facilita su estudio. La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual

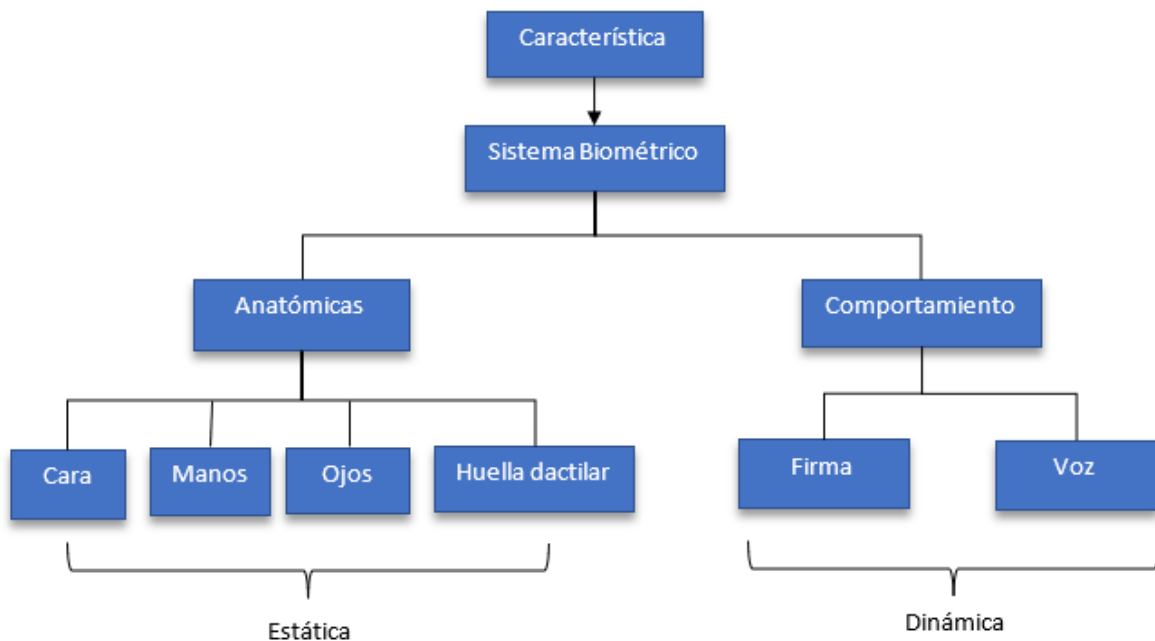


Figura 11: Esquema de los tipos de sistemas biométricos

Las técnicas biométricas se pueden clasificar atendiendo a cuál es la característica observada y aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y medible del individuo (esto incluye desde la forma de teclear ante un

ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en seis grandes grupos:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autenticación de la voz
- Reconocimiento de la firma

Cada sistema biométrico utiliza una cierta clase de interfaz para recopilar la información sobre la persona que intenta acceder. Un software especializado procesa esa información en un conjunto de datos que se pueden comparar con los modelos de los usuarios que se han introducido previamente al sistema. Si se encuentra un "concordancia" con la base de datos, se confirma la identidad de la persona y se concede el acceso.

En la siguiente tabla se muestra una comparativa de sus rasgos más generales:

Tabla 1: Comparación de rasgos biométricos generales

	Ojo - iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Fiabilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy Alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy Alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándares	-	-	ANSI/NIST , FBI	-	-	SVAPI

Interferencias	Gafas	Irritaciones	Suciedad	Artritis	Firmas	Ruido
Utilización	Instalaciones nucleares, Servicios médicos, centros penitenciarios	Instalaciones nucleares, Servicios médicos, centros penitenciarios	Policía, Industria	General	Industria	Accesos remotos en bancos o bases de datos

2.7.1 Huella dactilar

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos Inter papilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

2.7.1.1 Identificando patrones.

A simple vista, el patrón que siguen las líneas y surcos de una huella se puede clasificar según tres rasgos mayores: arco, lazo y espiral. Cada dedo presenta al menos una de estas características. Por otro lado, en determinados puntos las líneas de la huella dactilar se cortan bruscamente o se bifurcan. Estos puntos reciben el nombre de minucias, y juntos suman casi el 80% de los elementos singulares de una huella.

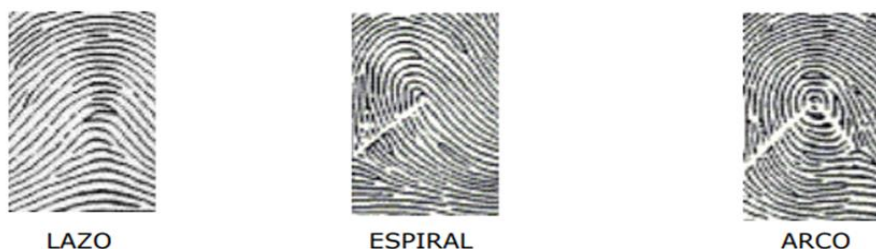


Figura 12: Clasificación de rasgos de una huella dactilar

2.7.1.2 Clasificación de la Huella.

La clasificación de las huellas dactilares es una técnica consistente en asignar a una huella uno de los varios tipos previamente especificados en la literatura y registrarla con un método de indexación de las direcciones. Una huella dactilar de entrada es primeramente clasificada a un nivel grueso en uno de los tipos:

- Whorl
- Lazo derecho
- Lazo izquierdo
- Arco
- Tented el arco

2.7.1.3 Realce de la Huella.

Un paso crítico en la clasificación automática de la huella dactilar está en extraer mediante un algoritmo las minutias de las imágenes de la huella dactilar de la entrada. El funcionamiento de un algoritmo de extracción de las minucias confía totalmente en la calidad de las imágenes de la huella dactilar de la entrada. Para asegurarse de que el funcionamiento de un sistema automático de identificación/verificación de huella dactilar sea robusto con cierta independencia de la calidad de las imágenes de la huella dactilar, es esencial incorporar un algoritmo del realce de la huella dactilar en el módulo de la extracción de las minucias. De este modo se puede mejorar de forma adaptativa la claridad de las estructuras de la cresta y el surco de las imágenes de las huellas dactilares de entrada.

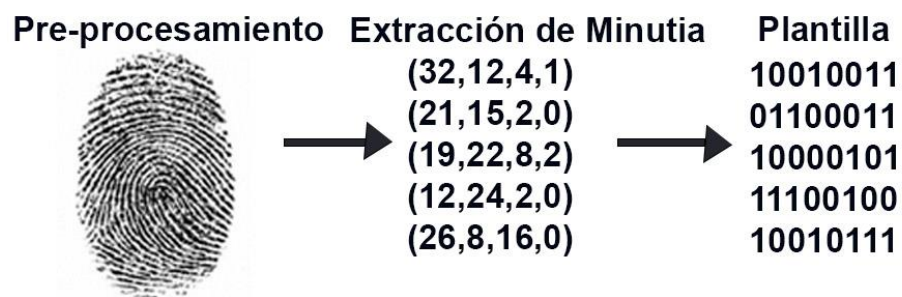


Figura 13 Representación de procesamiento de minutias de la huella dactilar

2.7.2 Reconocimiento de iris

El iris es una membrana coloreada y circular que separa las cámara anterior y posterior del ojo. Posee una apertura central de tamaño variable, la pupila. Las fibras musculares del iris la constituyen dos músculos, el esfínter del iris y el dilatador de la pupila.

Dos regiones del ojo pueden ser utilizadas por un sistema biométrico para identificar a un individuo: la red venosa de la retina y el iris.

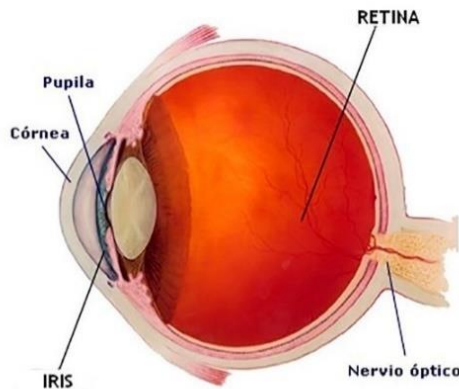


Figura 14: Ojo del ser humano

El iris está constantemente activo permitiendo así a la pupila dilatarse (midriasis) o contraerse (miosis). Esta función tiene su objetivo en la regulación de la cantidad de luz que llega a la retina.

Se trata de la estructura indivisible del cuerpo humano más distintiva matemáticamente. En sus 11 milímetros de diámetro cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag,). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar.

Hay que tener en cuenta que el iris no cambia a lo largo de la vida, y que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes. Asimismo, se trata de un órgano interno protegido -por la córnea y el humor acuoso- pero visible externamente a una distancia de hasta un metro. Las lentes de contacto y las gafas no afectan a la identificación. Y, por si todo esto fuera poco, los sistemas basados en el reconocimiento de iris son veinte veces más rápidos que cualquier otro sistema biométrico.

2.7.2.1 Funcionamiento.

El procedimiento, base de los dispositivos actuales, resulta extraordinariamente sencillo. Basta con colocarse frente a una cámara, con los ojos correctamente alineados en su campo de visión. La cámara genera una imagen que es analizada por medio de los algoritmos de Daugman para obtener el IrisCode personal, un patrón único del iris que apenas ocupa 256 bytes de información. Tan reducido tamaño permite una rápida búsqueda de su homólogo en una base de datos hasta identificar a su propietario.

Para la codificación del patrón del iris, usualmente se realiza una conversión de la imagen del iris de coordenadas cartesianas a polares para facilitar la extracción de información, al pasar de una forma circular a una rectangular. A la nueva representación, se le aplican filtros multicanal, ya sean de Gabor, Fourier o Wavelet, para extraer los coeficientes que finalmente conformarán el código del iris.

2.7.3 Geometría de la mano

La forma de la mano puede ser de gran valor en biometría. A diferencia de las huellas dactilares, la mano humana no es única, y sus características individuales no son suficientes para identificar a una persona. Sin embargo, su perfil resulta útil si el sistema biométrico lo combina con imágenes individuales de algunos dedos, extrayendo datos como las longitudes, anchuras, alturas, posiciones relativas, articulaciones. Estas características se transforman en una serie de patrones numéricos que pueden ser comparados. Su principal aplicación es la verificación de usuario.

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura.

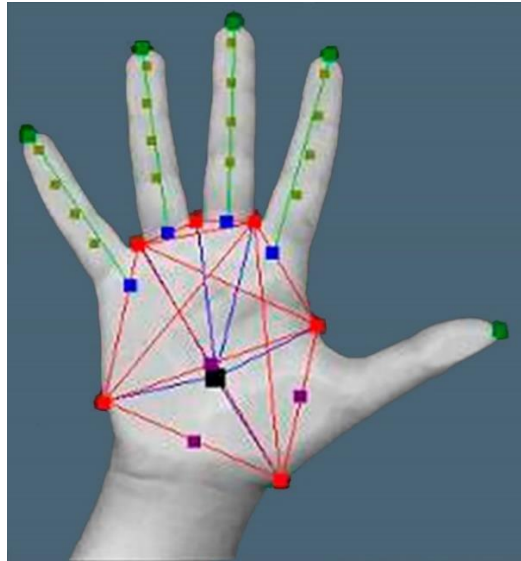


Figura 15: Reconocimiento de la palma de la mano

Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones.

Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualiza su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

2.7.4 Reconocimiento facial

Un sistema de reconocimiento facial es una aplicación dirigida por ordenador para identificar automáticamente a una persona en una imagen digital mediante la comparación de determinadas características faciales en la imagen y en la base de datos facial.

El reconocimiento facial automatizado es relativamente un concepto nuevo. Desarrollado en los años 60, el primer sistema semiautomático para reconocimiento facial requería del administrador para localizar rasgos (como ojos, orejas, nariz y boca) en las fotografías antes de que este calculará distancias a puntos de referencia en común, los cuales eran comparados luego con datos de referencia.

El método más común utiliza una cámara para capturar una imagen de nuestra cara, que es analizada en función de ciertos 'puntos clave', como la distancia entre los ojos o la anchura de la nariz.

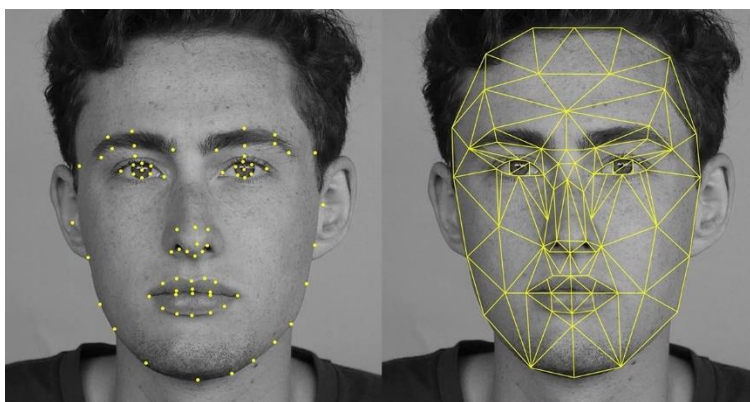


Figura 16 Reconocimiento facial

2.7.4.1 Funcionamiento

El primer paso en el reconocimiento facial es la adquisición de una imagen real o una imagen bidimensional del objetivo. El sistema determina la alineación de la cara basándose en la posición de la nariz, la boca, etc. En una imagen en 2D no debe estar más desplazada de 35 grados. Después de la alineación, orientación y ajuste de tamaño, el sistema genera una plantilla facial única (una serie de números) de modo que pueda ser comparada con las de la base de datos.

Un factor importante en los sistemas de reconocimiento facial es su capacidad para distinguir entre el fondo y la cara. El sistema hace uso de los picos, valles y contornos dentro de

un rostro (los denominados puntos duros del rostro) y trata a estos como nodos que puedan medirse y compararse contra los que se almacenan en la base de datos del sistema. Hay aproximadamente 80 nodos en un rostro de los que el sistema hace uso (entre ellos se incluye el largo de la línea de la mandíbula, la profundidad de los ojos, la distancia entre los ojos, la forma del pómulo, la anchura de la nariz...).

Los nuevos sistemas de reconocimiento facial hacen uso de imágenes tridimensionales, y por lo tanto son más precisos que sus predecesores. Al igual que en los sistemas de reconocimiento facial en dos dimensiones, estos sistemas hacen uso de distintas características de un rostro humano y las utilizan como nodos para crear un mapa del rostro humano en tres dimensiones de la cara de una persona. Empleando algoritmos matemáticos similares a los utilizados en búsquedas de Internet, la computadora mide las distancias entre determinados puntos de la muestra en la superficie del rostro. Estos sistemas en 3D tienen la capacidad de reconocer una cara incluso cuando se encuentra girada 90 grados. Por otra parte, no se ven afectados por las diferencias en la iluminación y las expresiones faciales del sujeto.

2.7.5 Otros sistemas de reconocimiento facial

Ciertos softwares interpretan cada imagen facial como un conjunto bidimensional de patrones brillantes y oscuros, con diferentes intensidades de luz en el rostro. Estos patrones, llamados eigenfaces, se convierten en un algoritmo que representa el conjunto de la fisionomía de cada individuo. Cuando un rostro es escaneado para su identificación, el sistema lo compara con todas las imágenes guardadas en la base de datos.

Este tipo de sistemas está sujeto a limitaciones, como las condiciones ambientales en el momento de capturar la imagen. Así, aunque normalmente interpreta correctamente los cambios de luz en interiores, su funcionamiento al aire libre, con luz natural, es todavía una asignatura pendiente. También la posición de la cabeza y la expresión del rostro pueden influir en el "veredicto".

Capítulo III: La termografía infrarroja

3.1 Conceptos básicos de la termografía infrarroja

Como bien es sabido, la termografía infrarroja se basa en la captación de imágenes térmicas, sin contacto, mediante las cuales se puede hacer un análisis en profundidad según la cantidad de radiación infrarroja emitida por un cuerpo u objeto en el que nos enfoquemos.

En cuanto a los orígenes de esta técnica, son atribuidos al astrónomo de nacionalidad alemana William Herschel. Herschel, además de realizar experimentos con luz solar, fue un astrónomo y músico germano-británico, descubridor del planeta Urano y de otros numerosos objetos celestes. En uno de sus experimentos, hizo incidir la luz solar a través de un prisma, formando a su paso el conocido fenómeno llamado arcoíris, al dividirse el haz de luz recibido; al observar este fenómeno, realizó mediciones de temperatura en cada zona de color mediante un termómetro, observando que iba incrementando razonablemente incluso una vez superada la región roja del espectro visible, a la que bautizó como luz infrarroja

3.2. Ondas y espectro electromagnético

Para comprender la naturaleza del espectro electromagnético y de la radiación infrarroja antes vamos a introducir el concepto de onda. ¿Qué es una onda? Pues según la RAE encontraríamos diferentes definiciones para la misma palabra, pero, para la física, es “la propagación de energía (y no de masa) en el espacio debido a la perturbación de alguna de sus propiedades físicas, como son la densidad, presión, campo eléctrico o campo magnético. Este fenómeno puede darse en un espacio vacío o en uno que contenga materia (aire, agua, tierra, etc.)”. Además de esto, se sabe que tienen lugar debido a oscilaciones de la materia que se ven continuadas en el tiempo. Teniendo en cuenta todo lo anterior, nos podemos encontrar diferentes tipos de ondas, con variaciones entre las mismas:

Según el medio en el que se propagan nos encontramos con:

- **Ondas mecánicas** son aquellas que necesitan un medio material y una serie de parámetros de temperatura y presión para propagarse. Un ejemplo de las mismas podrían ser las ondas sonoras (que a su vez también sabemos que se trata de ondas longitudinales).

- **Ondas electromagnéticas** a diferencia de las mecánicas, son capaces de propagarse en el vacío, sin necesidad de la presencia de un medio material. Como ejemplo y, al contrario del sonido, nos encontramos con la luz, que bien es sabido que es una onda transversal.

- **Ondas gravitacionales** estas últimas han sido reciente y frecuentemente publicadas por la prensa (con anterioridad al año 2019) y, aunque ya se sabía de las mismas, se ha confirmado que se tratan de una serie de alteraciones espacio-temporales.

Otra de las características de las mismas es la periodicidad:

- **Ondas periódicas** son aquellas que, como su propio nombre indica, presentan ciclos en un periodo de tiempo que se repiten continuamente.

- **Ondas no periódicas** en contraste a las periódicas, muestran ciclos que no se repiten o con variaciones que no tienen por qué ser muy significativas.

A continuación, hablaremos de las propiedades de direccionamiento dimensional:

- **Ondas unidimensionales** son aquellas que se desplazan a través del espacio, pero en una sola dimensión (de las tres espaciales que conocemos).

- **Ondas bidimensionales** como el prefijo “bi” indica, actúan en dos dimensiones espaciales, y también reciben el nombre de ondas superficiales.

- **Ondas tridimensionales** éstas son las capaces de moverse en las tres dimensiones espaciales conocidas y, son usualmente conocidas como ondas esféricas.

Finalmente, las ya mencionadas con anterioridad, y que dependen del movimiento del medio:

- **Ondas longitudinales** son aquellas que se caracterizan por la singularidad de que la dirección de la onda es la misma que la del desplazamiento de las partículas del medio.

- **Ondas transversales** en este caso, el movimiento de las partículas se produce de forma ortogonal a la dirección del vector de propagación de la onda.

En cuanto a las ondas electromagnéticas y, según el físico James Clerk Maxwell, “las cargas aceleradas o las corrientes eléctricas variables dan lugar a campos eléctricos y magnéticos”, que, al moverse con rapidez, se les denomina ondas electromagnéticas; estas representan la energía emitida por la materia que se obtiene por la variación en las configuraciones electrónicas de los átomos o moléculas. Además, se caracterizan por su frecuencia (f) o longitud de onda (λ), las cuales vienen vinculadas por la siguiente ecuación: $c=f\cdot\lambda$

Así, la velocidad de la onda viene dada en hercios (Hz, que es equivalente a la inversa del tiempo) por μm (micrómetros, donde la denominación de “micro” es equivalente a 10^{-6} m), lo que supone una unidad de velocidad, que en el SI (sistema internacional) se rige como m/s (metros por segundo).

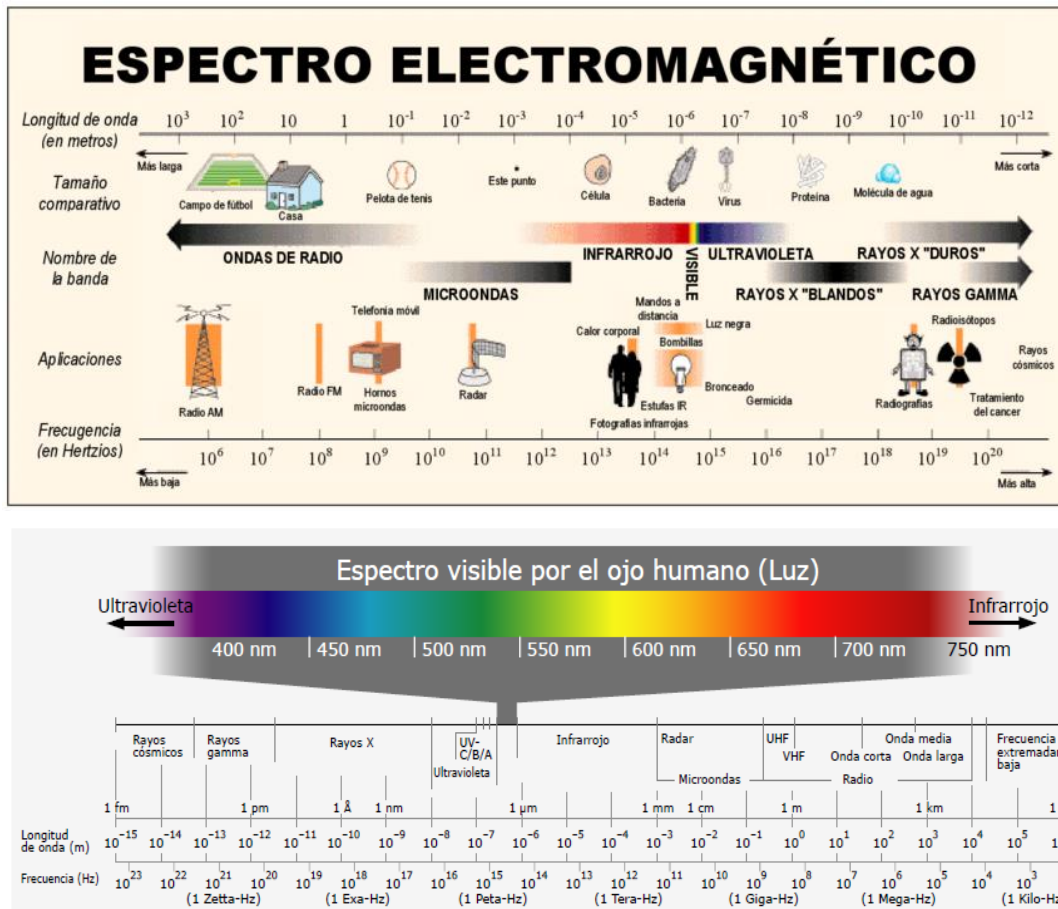


Figura 17: Espectro electromagnético

En la Figura 17 está representado el espectro electromagnético (EM). Entre los 700 nm (nanómetros) y los 1000 nm se encuentra la región del espectro electromagnético conocida como radiación infrarroja (la luz infrarroja como la denominó Herschel), que es de menor energía que la radiación visible que abarca de los 380 nm a los 780 nm, que es el rango de radiación EM donde la visión de los seres humanos está especializada y que coincide con las longitudes de onda donde el Sol emite la mayor parte de su radiación.

Las cámaras térmicas trabajan en la región de onda larga del espectro electromagnético, es decir, entre los 7 y los 14 μm .

El resto del espectro electromagnético está compuesto por diferentes regiones donde la radiación puede tener más o menos energía en función de la longitud de onda (λ).

En primer lugar, empezando por las ondas con menor λ , visualizamos los Rayos Gamma (γ), están caracterizados por tener una frecuencia superior a los 10 EHz (Exa Hercios) y tienen lugar en las reacciones nucleares.

En segundo lugar, los Rayos X tan conocidos por películas de ciencia ficción, y que se generan por el choque de electrones de alta energía con metales como el tungsteno.

Además, son capaces de atravesar la materia (con una longitud de onda incluso inferior a los nanómetros) y tienen diversos usos en la medicina como son las radiografías.

Posteriormente, la luz o radiación UV (Ultravioleta), que es muy comúnmente conocida ya que, día a día se habla del agujero de la capa de ozono producido por la contaminación, y que poco a poco nos hemos estado viendo afectados en mayor cantidad por estas ondas electromagnéticas.

Justo antes de alcanzar las frecuencias del espectro infrarrojo nos encontramos con la luz visible, que ya hemos comentado y que como su propio nombre dice, es la que somos capaces de observar.

Así pues, queda reflejado que el ojo humano no es capaz de percibir ni siquiera un 1% del espectro electromagnético conocido.

Finalmente, con una longitud de onda bastante mayor a las infrarrojas, localizamos las microondas, que se generan por tubos de vacío teniendo en cuenta el movimiento del electrón o por semiconductores como son los transistores del tipo FET (Efecto campo) y BJT (Unión bipolar); y con las ondas de radio, que se caracterizan por la excitación de cristales o por el paso de corriente alterna a través de conductores eléctricos.

Sabiendo todo lo anterior, hay que destacar que el infrarrojo térmico se encuentra entre los 0,9 μm (0'9·10⁻⁶m) y los 1.4 μm de longitud de onda.

Debido a este rango de longitudes de ondas, el vidrio entre 7 μm y 14 μm , es opaco para las cámaras infrarrojas; de ahí la prohibición de llevar puestas cualquier tipo de gafas oculares, ya que nos impide la medición de temperatura en el lagrimal del ojo.

La teoría dice que todo cuerpo con una temperatura superior a los 0 K (-273,15°C), emite radiación infrarroja (y radiación electromagnética) y, por tanto, es visible para una cámara termográfica.

3.3 Termografía infrarroja.

Con respecto a la termografía, cabe destacar que es la ciencia de adquisición y análisis de información térmica a partir de dispositivos sin contacto directo, los cuales son capaces de captar la radiación infrarroja emitida por un cuerpo.

Por otro lado, la termografía infrarroja, y más concretamente las cámaras termográficas, nos aportan la siguiente información:

- Permite realizar la medida de temperatura con facilidad a objetos móviles y de difícil acceso.
- No produce interferencias con el funcionamiento y/o comportamiento propio del elemento a medir. Esto es debido a que se trata de una técnica sin contacto, con la caracterización de que no existe inercia térmica.
- Nos da la posibilidad de realizar la medida de grandes superficies con facilidad y rapidez.
- Admite la captación de la temperatura de varios objetos de forma simultánea, en los que cada píxel de la imagen facilita sensores de temperatura independientes.
- Aportan un tiempo de respuesta en el orden de los milisegundos. Además, otorga la observación de fenómenos transitorios de temperatura mediante cámaras de alta velocidad.
- Proporciona una precisión de monitoreo de 0.1°C [4] y una alta fiabilidad en todas y cada una de sus mediciones, la cual es una característica clave en la medición de procesos febriles, que es en lo que se enfoca este trabajo.

⁴ Dato obtenido de la ficha técnica del Control de acceso ASI-7213X-T1 Anexo 2

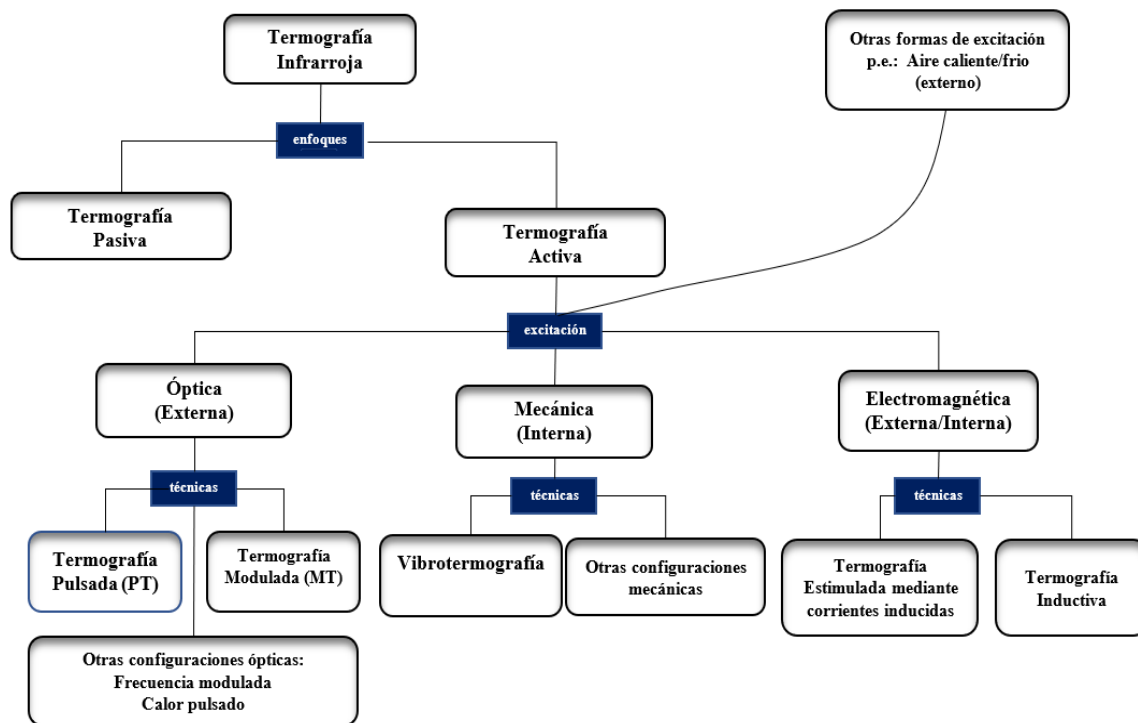


Figura 18: Esquema de metodología de captura termográfica

Como podemos observar en la Figura, hay diferentes metodologías y formas de captura que varían según la aplicación que le queramos dar a la cámara. Es por ello que, si queremos detectar ciertos fallos y anomalías en nuestro objetivo, o queremos profundizar en los mismos y averiguar propiedades más específicas de esos defectos, tenemos que clasificar la termografía en dos grupos: Por un lado, la termografía cualitativa, esta técnica se basa en el diagnóstico de anomalías a partir de una imagen térmica. Además, puede ser útil en aplicaciones como la vigilancia y detección de fugas, aquellos lugares en los que no es necesaria una medida precisa de la temperatura. Por otro lado, la termografía cuantitativa, la cual es capaz de estimar la gravedad de un defecto a partir de una medida de temperatura precisa, en actividades como el mantenimiento preventivo o ensayos no destructivos (END). Así pues, los caracteriza de la siguiente manera:

- Estima la temperatura.
- Determina el tamaño y la forma del problema a revisar.
- Calcula la profundidad y/o localización en la que se encuentra la anomalía.
- Evalúa las propiedades térmicas del defecto (resistencia térmica, dilatación).

Para realizar un contraste más exhaustivo entre éstas, hay que tener en cuenta que la termografía cualitativa sólo mide temperaturas aparentes para determinar si existen o no esas anomalías y analizar los patrones. En cambio, la termografía cuantitativa no es necesaria en todos y cada uno de los procesos, así como implica una medida de temperatura más exacta para realizar un equilibrio de temperaturas.

Es por ello que, hay actividades en las que ambos análisis son requeridos para el correcto funcionamiento del proceso.

3.4. Radiación electromagnética

La radiación electromagnética como tal es emitida por muchos dispositivos de los que nos rodeamos hoy en día, la mayoría de ellos electrónicos simples como por ejemplo un sensor de temperatura o complejos como un ordenador, pero ondas como la luz también componen lo que es llamado radiación electromagnética.

Pero, ¿cuáles son los componentes de este fenómeno? Pues principalmente una partícula llamada fotón, que se encarga de emitir la energía en forma de señales electromagnéticas, la cual es un proceso indispensable en nuestra naturaleza.

Por otro lado, todo este tipo de radiación está caracterizado por ciertos parámetros como son la frecuencia y la energía. Según estos aspectos, y teniendo en cuenta si la radiación es ionizante o no ionizante (produce la ionización de ciertos átomos o moléculas del elemento con el que interacciona), podemos clasificarlos mediante la tabla mostrada N° 2.

Tabla 2: Clasificación de la radiación electromagnética según sus características

	DENOMINACIÓN	LONGITUD DE ONDA	FRECUENCIA	ENERGÍA
Radio	Radio Onda Muy Larga	> 10Km	< 30KHz	$< 1^{-10}eV$
	Radio Onda Larga	650m-10Km	30-650KHz	$1.24^{-10} - 1.9^{-10}eV$
	Radio de Onda Media (AM)	180-650m	650KHz-1.7MHz	$1.9^{-9} - 6.9^{-9}eV$
	Radio de Onda Corta	10-180m	1.7-30MHz	$6.9^{-9} - 1.24^{-7}eV$
	Muy Alta Frecuencia Radio (VHF)	1-10m	30-300MHz	$1.24^{-7} - 1.24^{-6}eV$
	Ultra Alta Frecuencia Radio (UHF)	30cm-1m	300MHz-1GHz	$1.24^{-6} - 4.14^{-6}eV$
Microondas	Microondas	1mm-30cm	1GHz-300GHz	$4.14^{-6} - 0.001 eV$
Luz Infrarroja	Infrarrojo Lejano	50µm-1mm	300GHz-6THZ	$0.001 - 0.02 eV$
	Infrarrojo Medio	2.5-50µm	6THZ-120THZ	$0.02 - 0.5 eV$
	Infrarrojo Cercano	780nm-2.5µm	120THZ-384THZ	$0.05 - 1.6 eV$
Luz Visible	Rojo	625-740nm	384THZ-480THZ	$0.5 - 0.5 eV$
	Naranja	590-625nm	480THZ-508THZ	$0.02 - 0.5 eV$
	Amarillo	565-590nm	508THZ-531THZ	$0.02 - 0.5 eV$
	Verde	520-565nm	531THZ-577THZ	$0.02 - 0.5 eV$
	Celeste	500-520nm	577THZ-600THZ	$0.02 - 0.5 eV$
	Azul	450-500nm	600THZ-666THZ	$0.02 - 0.5 eV$
	Añil	430-450nm	666THZ-698THZ	$0.02 - 0.5 eV$
	Violeta	380-430nm	698THZ-790THZ	$0.02 - 0.5 eV$
Luz Ultravioleta	Ultravioleta Cercano (UVA)	315-380nm	790THZ-952THZ	$3.3 - 4 eV$
Radiacion Indirectamente Ionizante	Ultravioleta Medio (UVB)	280-315nm	952THZ-1THZ	$4 - 4.4 eV$
	Ultravioleta Extremo	10-280nm	1THZ-30PHZ	$4.4 - 124 eV$
	Rayos x	10pm-10nm	30PHZ-30EHZ	$124 - 124 MeV$
	Rayos Gamma	<10pm	>303HZ	$> 124 MeV$

En la figura N°19 se muestra el resultado de una medición móvil (realizadas sobre carreteras) de radiaciones no Ionizantes (RNI) en la ciudad de San Salvador, en banda ancha entre los 100kHz y 8GHz.



Figura 19: Medición móvil no ionizante

Para describir los parámetros de una señal cualquiera dentro del espectro electromagnético se muestra una medición realizada en la banda de 850MHz a 960MHz, tomada con un analizador de espectro. En esta podemos apreciar el parámetro frecuencia (MHz) en el eje X y el parámetro intensidad de señal en el eje Y utilizando una escala logarítmica (dBm, 0dBm = 1mW).

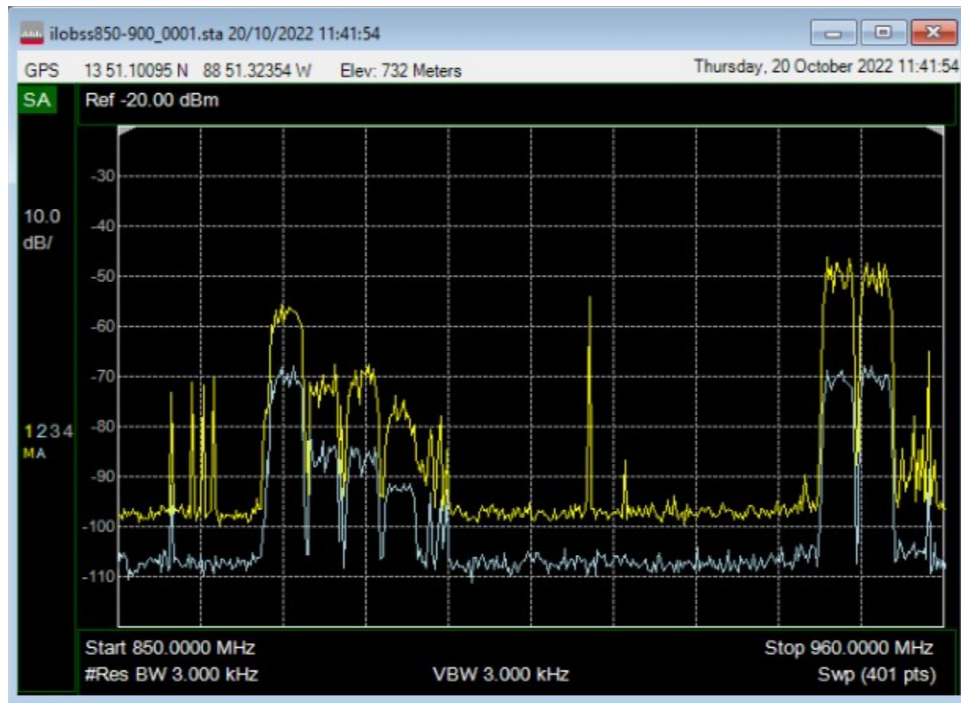


Figura 20: Medición realizada con un analizador de espectro

Continuando con la fundamentación relacionada con este trabajo mencionamos otro concepto vinculado, este es la Ley de Wien la cual establece que existe una relación entre la temperatura y la longitud de onda de una emisión electromagnética la cual expresa de manera cuantitativa la relación inversamente proporcional entre el pico o máximo de emisión en el espectro de un cuerpo negro y las longitudes de onda, a medida que la temperatura aumenta se tiene un espectro de frecuencia con menores longitudes de onda. (Ecuación. 2)

$$\lambda_{max}=0,002898/T \quad (\text{Ec. 2})$$

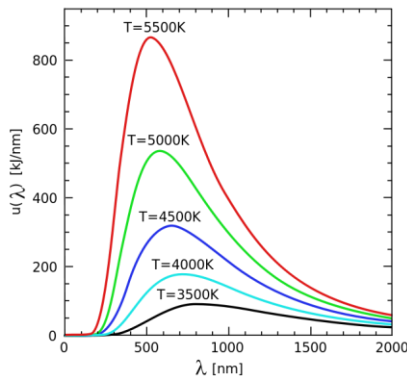


Figura 21: Gráfica de longitud de onda

Así pues, el producto de la longitud de onda (λ) en metros de una radiación electromagnética y la temperatura (T) en Kelvin del cuerpo negro el cual tiene por principal propiedad la absorción de toda la energía radiante incidente, comportándose de manera plana para cualquier frecuencia. Por otro lado, uno de los aspectos más importantes de esta propiedad es que, a partir de la radiación emitida por una estrella, se puede hacer una estimación de la temperatura a la que se encuentra la misma y, por tanto, obtener datos como la masa y la energía del cuerpo analizado o incluso de la propia estrella, sin importar la distancia a la que se encuentre.

3.5. Transmisión de calor

Mientras que la transferencia de energía a partir de los otros dos mecanismos que dictamina la física tiene lugar con una dependencia del material y los fluidos que intervienen, la transmisión de calor por radiación no necesita medio material alguno para desarrollarse.

¿Esto qué quiere decir? Pues básicamente que esa transferencia de energía se lleva a cabo a partir de ondas electromagnéticas, las cuales se propagan con mayor facilidad a través del vacío, como lo demuestra la principal fuente de energía que recibe el planeta Tierra, el Sol. Esta estrella proyecta su energía a partir de ondas que calientan nuestra superficie mediante radiación, y proyecta, además, cierta radiación dañina de la que hemos hablado con anterioridad, como la radiación ultravioleta.

Una vez hemos introducido la manera de actuación, hay que hablar de las formas por las pueden actuar los objetos o elementos que reciben esta radiación. Así, una proporción de estas ondas electromagnéticas puede ser absorbida, reflejada o transmitida, y estos factores los destacaremos en profundidad en los siguientes puntos.

3.6. Emisividad y temperatura reflejada

En este apartado, encontramos tres conceptos claves a definir: en primer lugar, la emisividad, que es la relación entre la radiación emitida por un cuerpo real y la radiación emitida por un cuerpo negro, el cual se encuentra a la misma temperatura y longitud de onda.

En segundo lugar, la transmitancia, que es la fracción de radiación incidente transmitida por una superficie analizada.

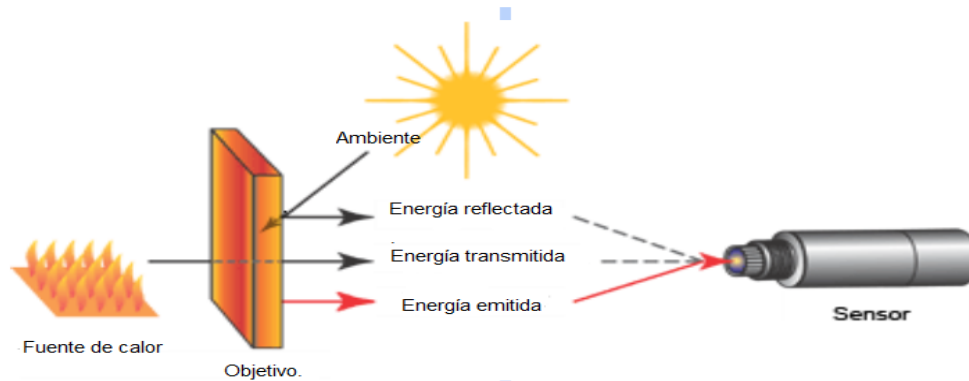


Figura 22: Diferencia entre los conceptos de emisividad, transmitancia y reflectancia

En tercer lugar, la reflectancia, que es la fracción de radiación incidente reflejada por una superficie.

Teniendo en cuenta estas definiciones previas y, realizando un experimento práctico, suponiendo que todos los objetos se consideran opacos; es decir que, en condiciones de idealidad, no se produce transmitancia, provocando que, al aplicar las leyes de Kirchhoff, la suma de las proporciones de la emisividad y la reflectancia de una superficie es igual a uno.

3.7 Temperatura aparente reflejada

El calor reflejado procede normalmente de lo que se encuentra enfrente y, muchas veces incluye al propio operador. Pero, cuando realizamos estas mediciones, tenemos que tener en cuenta factores como la temperatura reflejada (RTC).

Además, es importante establecer correctamente, de forma manual, la RTC⁵ para el cálculo de la temperatura porque, cuando el objeto a analizar dispone de una baja emisividad, aumenta paulatinamente la proporción de radiación reflejada.

⁵ RTC (Reflective temperature correction por sus siglas en ingles)

Por otro lado, en muchas ocasiones se suele definir y establecer la temperatura reflejada como la temperatura ambiente. Sin embargo, cuando se encuentra una gran diferencia de temperatura entre los objetos alrededor y el objeto a medir (por ejemplo, en mediciones exteriores bajo una intensa luz solar), es difícil estimar el valor de la temperatura reflejada.

Es por ello que se recomienda el uso de un radiador Lambert, para realizar una medida de la temperatura aparente reflejada en paralelo a la de la cámara termográfica. El método de trabajo de este radiador, se basa en reflejar la radiación que incide en el mismo, con la intensidad más próxima a la recibida, y en la dirección que nos interese.

3.8 Reflexión

Una vez hemos hablado de la temperatura aparente reflejada, tenemos que destacar dos fenómenos que ocurren cuando una onda choca contra una superficie. En estos dos factores, la frecuencia es constante, pero, la velocidad de la onda y, por tanto, la longitud de onda, varían al producirse refracción.

Aunque sean conceptos similares que se estudian en la rama óptica dentro de la física, son muy diferentes entre sí, ya que, cuando la onda se propaga, puede atravesar o no la superficie del otro medio al que se enfrenta. En el caso en el que, al menos una parte de la onda no traspase esa especie de barrera, y simplemente cambie de dirección, se llamará reflexión (Figura 5).

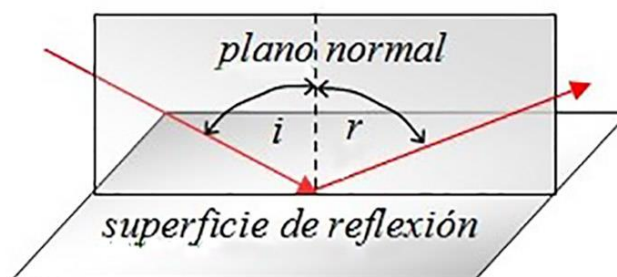


Figura 23: Reflexión de un haz de luz

Como vemos en la imagen mencionada, la reflexión va a variar según el ángulo con el que se produzca; así pues, en el caso de que la superficie disponga de irregularidades, la reflexión podría no ser uniforme, y en ese caso se llama reflexión difusa. Además, si el medio dispone de

irregularidades más pequeñas que la longitud de onda, se le llama reflexión especular, ya que no produce esa variación tan significativa que encontramos en la difusa.

Por otro lado, cuando, al menos una fracción de la onda, pasa de un medio a otro y, además de la dirección de la misma, cambia su velocidad, se le llama refracción.

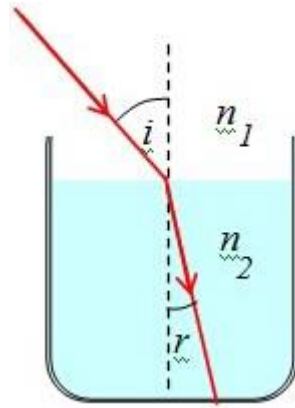


Figura 24: Refracción de un haz de luz

Una propiedad a destacar, acerca del índice de refracción, es que depende de la longitud de onda de la, valga la redundancia, onda que choca con esa superficie que hace de barrera entre un medio u otro. Este factor de refracción, es muy común también a la hora de analizar las lentes necesarias para corregir enfermedades que afecten a la visión ocular de los humanos.

3.9 Las cámaras infrarrojas como herramientas contra el Covid-19

Tras la declaración del estado de alarma por la emergencia sanitaria en nuestro país (y a nivel mundial) debido a la pandemia que ha afectado gravemente a la humanidad, se ha priorizado la detección precoz de los síntomas de esta enfermedad. Como hemos hablado en la introducción del trabajo, nuestro enfoque será la detección de estados febriles mediante la actuación de cámaras termográficas.

Además, aunque conocemos todos los síntomas que se pueden presentar, se sabe también el orden en el que se manifiestan y uno de los síntomas más frecuentes y que se manifiestan de forma precoz es la fiebre. Es por ello que, mediante el uso de la termografía infrarroja como herramienta, resulta fundamental detectarla con anterioridad, para poder facilitar el monitoreo del virus Covid-19 y colaborar en su erradicación.

En este apartado estudiaremos los diferentes tipos de cámaras térmicas, sus características principales y algunas de sus aplicaciones. Además, analizaremos las fuentes de error más habituales y las consideraciones fundamentales a tener en cuenta para su utilización como herramienta de detección de estados febriles.

3.10 Tipos de cámaras térmicas: refrigeradas o no refrigeradas

Las cámaras que disponen de un sensor refrigerado aportan una serie de características que las diferencian de las de sensor no refrigerado. Aquellas que son refrigeradas, tienen la capacidad de disminuir la temperatura del sensor responsable de la generación de las imágenes mediante, como su propio nombre indica, un refrigerador criogénico. Gracias al efecto del mismo, se consiguen minimizar las desviaciones térmicas generadas, facilitando así la medida a realizar.

Este dispositivo requiere de una gran precisión en su fabricación y, debido a su función, es necesaria su reposición tras un tiempo preestablecido de trabajo cuyo promedio anda alrededor de tres años.

Una vez introducido este aspecto, llevaremos a cabo una comparación entre las condiciones de funcionamiento de las cámaras térmicas con sensor refrigerado y las de sensor no refrigerado, ya que, según la aplicación que se le quiera dar, tendrán un comportamiento mejor unas u otras:

- Medidas en alta velocidad como podemos observar en la imagen a continuación y, sabiendo que la captura de la izquierda ha sido tomada por una cámara con sensor refrigerado y la de la derecha por una sin refrigeración podemos concluir lo siguiente.



Figura 25: Imágenes térmicas del movimiento en alta velocidad un neumático (Izq.) tomada por una cámara refrigerada y la capturada por una cámara no refrigerada (Der.)

La grafica anterior se observa que la velocidad de captura de los detectores refrigerados es mucho mayor, ya que se aprecia perfectamente la rueda en estático, mientras que en la no refrigerada no podemos apreciar los radios de la misma y, por tanto, la medida será de más baja calidad.

Resolución espacial en este apartado visualizaremos las diferencias entre el tamaño del punto de medición y la posibilidad de ampliación de las mismas.

Por un lado, las cámaras refrigeradas son capaces de detectar longitudes de onda de infrarrojos más cortas, característica que observamos perfectamente en las imágenes mostradas, con una mayor definición y calidad al ampliar las zonas de calor.

Además, “como las cámaras refrigeradas tienen mayores características de sensibilidad, lentes con más elementos ópticos o elementos más gruesos que pueden utilizarse sin degradar la relación de señal y ruido por arriba de los 20 db, lo que permite un mejor rendimiento de ampliación”, es por ello que, aunque las zonas de trabajo de una PCB (Por sus siglas en ingles Printed Circuit Board) sean más o menos distribuidas uniformemente, en la cámara no refrigerada sólo se percibe un punto de calor.

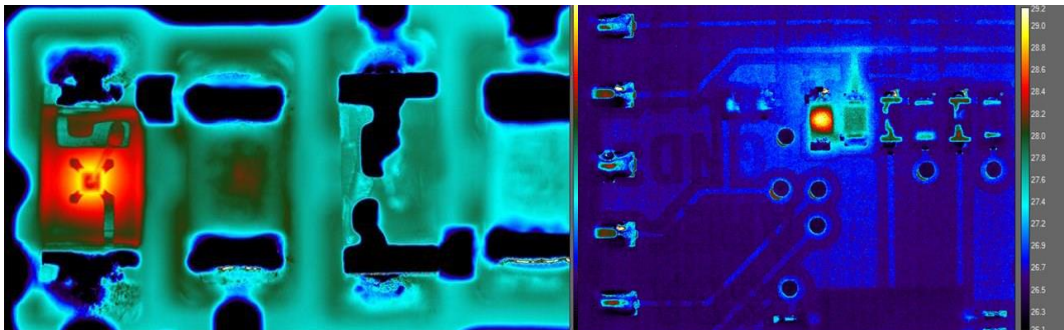


Figura 26: Imágenes térmicas del comportamiento de una PCB (Izq.) tomada por una cámara refrigerada y la capturada por una cámara no refrigerada (Der.)

Sensibilidad en las siguientes ilustraciones mostraremos, en la parte superior la captura instantánea tras retirar la mano y, en la parte inferior, la huella térmica que ha permanecido después de un cierto período de tiempo (siempre teniendo en cuenta que las imágenes de la izquierda corresponden a las cámaras refrigeradas).

Así pues, podemos obtener dos conclusiones significativas: en primer lugar, la calidad y precisión de la medida es bastante mayor en las refrigeradas, además de que se proporciona menor ruido; y, en segundo lugar, la detección en el tiempo es bastante más extensa, permitiendo una mejor detección de diferencias de temperatura con una medición más estable y duradera.

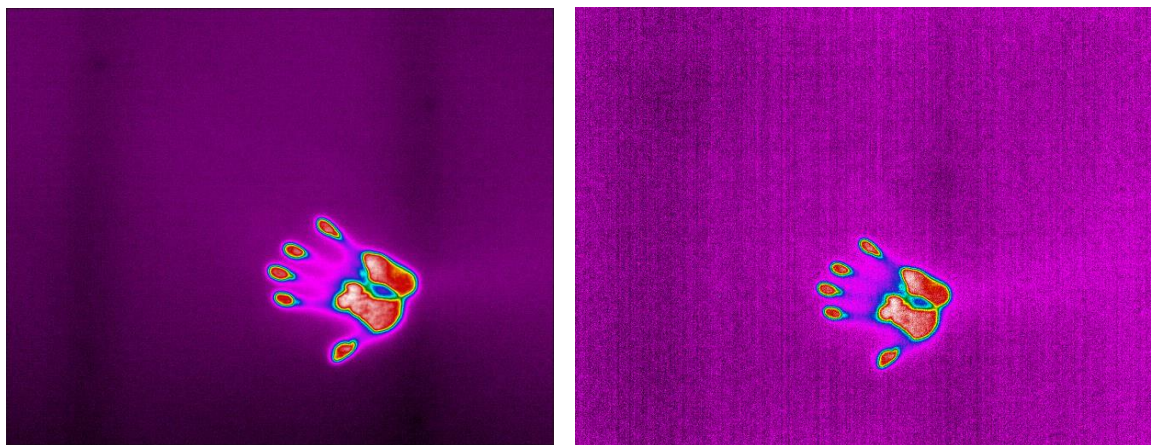


Figura 27: Imágenes térmicas de la huella de una mano cámara refrigerada (Izq.) y captura por una cámara no refrigerada (Der.)

Filtrado espectral a continuación veremos una de las propiedades más ventajosas de las cámaras con sensor refrigerado, ya que, las no refrigeradas no tienen la capacidad de realizar un filtrado espectral.

3.11 Cámaras activas o pasivas

En relación a la termografía pasiva, hay que destacar que está concebida con el objetivo de generar una imagen infrarroja a partir del contraste térmico entre el elemento a medir y el entorno que lo rodea, es decir, sin emplear un estímulo de calentamiento externo que provoque un flujo de calor en el cuerpo a inspeccionar.

Al producirse el estudio del objeto, se contempla que, si nos encontramos con una pequeña diferencia de temperatura respecto a la que presenta habitualmente en condiciones de trabajo, es posible que la medida en tiempo real nos haya facilitado la detección de un comportamiento inusual de la maquinaria o región.

Así pues, aunque la termografía más utilizada es la activa, este tipo de termografía es muy útil en aplicaciones industriales que disponen de una gran cantidad de energía, así como la monitorización de procesos de soldadura y en mantenimiento predictivo de instalaciones, o también en inspecciones de defectos o anomalías en viviendas y a nivel medicinal en detección de cáncer de seno.

Por otro lado, la termografía activa se emplea para detectar detalles específicos que no son posibles de ver debajo de la superficie de un objeto. De esta manera, se trata de calentar las zonas de interés, afectando así a la temperatura superficial con el objetivo de detectar anomalías transitorias y poder captarlas con las cámaras termográficas.

Una vez se ha transmitido el calor necesario a través de la fuente de excitación, debemos tener en cuenta que se puede aplicar tanto de forma transitoria (mediante impulsos) o en régimen permanente (realizándose de forma periódica). A partir de este proceso en el que conocemos la temperatura superficial, podremos obtener datos que detallen lo que sucede en el interior del objeto.

El principio de detección de defectos consiste en lo siguiente: la relación de difusión varía cuando se producen imperfecciones en la propagación térmica de un pulso de temperatura. Esto quiere decir que, si las condiciones fueran ideales, es decir que el material al que nos enfrentemos y el aporte de energía sean uniformes, al medir la temperatura en la superficie del mismo también obtendríamos unos resultados bastante similares a lo largo de la misma. Es por eso que cualquier oscilación puede afectar de lleno en la medida y/o alertarnos de una anomalía en el sistema.

3.12 Aplicaciones

En este apartado describiremos y ejemplificaremos la gran variedad de aplicaciones en las que las cámaras pueden ser de utilidad además de la medicina, tanto a nivel industrial como en temas de mantenimiento, detección de fugas, ensayos, etc.:

- **Industria electrónica** (disipaciones en PCBs, diseño). Dentro del análisis de las PCB, son muy útiles para visualizar qué elementos están más calientes y, por tanto, están trabajando en mayor medida comparado con los otros elementos, además de poder detectar fallos si los componentes alcanzan o superan sus temperaturas límites de operación.

- **Aeronáutica** (pruebas funcionales de motores y/o turbinas, aplicaciones de alta velocidad). En las aplicaciones de alta velocidad, las cámaras infrarrojas tendrían la misma función que un termopar, pero sin contacto; además, ofrecen la ventaja de medir una gran cantidad de puntos con precisión y aportar datos como el origen del calor o la rapidez con la que aparece.

- **Automoción** (asientos calefactados). En este caso, su utilidad sería para comprobar si la distribución de calor es uniforme en todo el asiento, o si no están funcionando de una forma eficiente.

- **Medicina** (detección de cáncer al alertar de zonas con temperaturas corporales anómalas). Esta es una de las funciones más eficaces dentro de la medicina, ya que, mediante las tonalidades de colores que aportan las imágenes térmicas, se pueden llevar a cabo diagnósticos de detección precoz de enfermedades tan graves e influyentes como el cáncer.

Así pues, permite al personal médico la inspección de zonas corporales específicas solamente con una captura térmica, pudiendo ser determinante en este aspecto. Por curiosidad, para visualizar el gran calibre de esta utilidad, según una noticia que publicó el medio CNN en octubre de 2019, una cámara térmica fue capaz de detectar cáncer de seno en una mujer que se encontraba en un parque de atracciones.

-**Veterinaria** (diagnósticos en animales, zoológicos, con animales exóticos para no alterarlos por el contacto directo; por ejemplo, con la medición, sin contacto, en el ojo del número de latidos de un ave).

- **Industria alimentaria** (comprobación de la temperatura en cada alimento para diagnosticar un posible mal estado, distribución homogénea de temperatura, termocompresión de envasado, verificación de termosellado).

- **Mantenimiento preventivo y correctivo** en la industria, monitorización de equipos/máquinas rotativas y elementos eléctricos. Monitorización continua de un equipo crítico.

- **Niveles de llenado** en tanques, detección de fugas.

- **Ensayos de tracción**, fuerzas aplicadas sobre probetas, esfuerzos.

- **Metalurgia** (medición de metalíquidos, integridad de los hornos, tratamientos térmicos, inspección continua de los moldes, inspección de calidad en planchones revisando grietas, nivel de llenado).
- **Siderurgia** (colada continua, control y observación del planchón, ver temperaturas de rodillos y cada colada individualmente, detección de escoria). Componentes automotrices, cabinas de inspección, fundición de aluminio.
- **Medio Ambiente** (detección de posibles puntos calientes en incendios forestales). Se han instalado en hidroaviones, con la función de detectar esas zonas con mayor riesgo de expandir el fuego, en el incendio forestal del pasado 23 de agosto de 2020 en la isla de La Palma.

3.13 Fuentes de error en el análisis termográfico

En cuanto a las fuentes de error en el análisis termográfico, podemos enumerar las siguientes:

- **Viento** puede interferir entre el objeto y la cámara. Además, reduce la temperatura del objeto con una relación directamente proporcional a la velocidad del mismo. Para solucionarlo, existen factores de corrección, en los cuales nos enfocamos para suavizar este efecto meteorológico.
- **Lluvia** reduce la temperatura del objeto a medir. Permite el correcto funcionamiento y cálculo de la cámara, siempre y cuando la lluvia no sea muy abundante.
- **Distancia al objeto** es uno de los factores más determinantes ya que, si se reduce el tamaño de medición, tienes una menor referencia de puntos, perdiendo fiabilidad de la medición. Aunque sea un aspecto importante a tener en cuenta, usualmente no modifica sensiblemente la medida.
- **Tamaño del objeto** para obtener una buena medida, se requiere una resolución con un área mínima de 3x3 píxeles, nunca por debajo de esa superficie, ya que sería físicamente implementable y aportaría una medida totalmente errónea.
- **Tipo de material** para este aspecto hay que tener en cuenta que, las cámaras infrarrojas tienen preestablecido un valor de emisividad, el cual varía suficientemente según el material en el que

estamos midiendo, pudiendo realizar un análisis erróneo. Es por ello, que, en materiales como los metales, hay que tenerlo en cuenta, debido a su baja emisividad.

-Emisividad superficial como ha sido indicado anteriormente, depende directamente del tipo de material.

Tabla 3: Emisividad de los materiales

Materiales	Emisividad	Materiales	Emisividad
Madera	0.85	Papel negro	0.86
Agua	0.96	Polycarbonato	0.8
Ladrillo	0.75	Hormigón	0.97
Acero inoxidable	0.14	Oxido de cobre	0.78
Cinta	0.96	Hierro fundido	0.81
Placa de aluminio	0.09	Oxido	0.8
Placa de cobre	0.06	Yeso	0.75
Aluminio negro	0.95	Pintura	0.9
Piel humana	0.98	Goma	0.95
Asfalto	0.96	Tierra	0.93
PVC	0.93		

- **Temperatura ambiente** no es un fenómeno que influya, pero para tener una correcta medición debe estar en el rango no superior al +15°C a +32°C.

- **Absorción atmosférica** que se define como la disminución de la intensidad luminosa de una fuente celeste, causada por los gases que componen la atmósfera. Es quizás el menor factor a tener en cuenta, sin embargo, la radiación se reduce levemente.

Capítulo IV: Sistema de control de acceso

4.1 Definición Control de acceso

La definición más generalizada de un sistema de control de acceso hace referencia al mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos. Básicamente encontramos sistemas de controles de acceso en múltiples formas y para diversas aplicaciones.

Por ejemplo, encontramos sistemas de controles de acceso por software cuando digitamos nuestra contraseña para abrir el correo, otro ejemplo es cuando debemos colocar nuestro usuario y contraseña al iniciar el sistema operativo Windows en nuestras PC, estos son ejemplos que permiten el acceso a datos. Sin embargo, nuestro enfoque es en la seguridad electrónica que está relacionada al acceso de recursos, en la toma de temperatura, verificación del uso de mascarilla, y registro de ingreso del personal universitario.

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de proximidad o biometría) y a su vez controlando el recurso (puerta, torniquete) por medio de un dispositivo eléctrico como cerradura eléctrica.

El control de acceso de personas se realiza con una serie de objetivos:

- Restringir o permitir el acceso de personas a determinadas áreas o departamentos de unas instalaciones.
- Restringir o permitir el acceso a sistemas informáticos, bases de datos y otros servicios de información.
- Proteger los bienes físicos, equipos o datos de las organizaciones ante robos o accesos de terceros sin permiso.
- Detectar accesos no autorizados y poner en marcha mecanismos para evitarlos.
- Registrar y revisar eventos críticos realizados por los usuarios en los sistemas.
- Facilitar la organización de la empresa y el control de los trabajadores.

- Medición sin contacto de temperatura corporal.

Principios básicos

Los tres principios básicos que rigen un **control de acceso y seguridad** son la identificación, la autenticación y la autorización. A continuación, vemos en qué consiste cada uno de ellos.

Identificación

Esta consiste en la identificación del usuario o trabajador. Existen diversos métodos para identificar a una persona, como pueden ser las huellas dactilares, las tarjetas de identificación o el reconocimiento facial, entre muchos otros.

Autenticación

Esta consiste en una validación del usuario en la base de datos y si cuenta con los permisos necesarios para acceder, es decir, consiste en la verificación de la identidad del usuario según los valores almacenados comparándolos con los valores obtenidos por el sensor biométrico.

Autorización

Una vez que el sistema ha identificado y verificado la identidad del usuario, se procede a autorizar o denegar su acceso a las instalaciones o a los sistemas informáticos. Es habitual que la autorización esté limitada a determinados recursos o instalaciones. Por ejemplo, en un control de acceso al trabajo, la entrada al almacén puede estar restringida a los operarios o a los transportistas.

4.2 Tipos de control de acceso

Una forma de clasificar los controles de acceso es mediante la descripción en la forma en que se implementan. Dentro de la clasificación que hemos preparado, vamos a distinguir entre los tipos de control de acceso según la forma de identificación que utilicen, y también según el tipo de conexión que necesiten para cumplir sus funciones.

4.2.1. Tipos de control de acceso según el sistema de identificación que utilicen

Un sistema de control de acceso tiene tres funciones principales: la autenticación que permite la identificación de las personas o vehículos que solicitan acceder a una empresa o a una zona concreta; la autorización que gracias al software del sistema realiza las comprobaciones y envía la orden de abrir o no un acceso; y la trazabilidad que facilita la obtención de listados de las personas presentes en una zona o lugar.

En base a esto podemos encontrar diferentes tipos de control de acceso según el sistema de identificación que utilicen:

Sistema de proximidad: permite la utilización de tarjetas u otros objetos que al acercarlos al terminal inicia la autenticación. En este tipo de control de acceso tenemos que destacar la innovadora tecnología RFID, que además de ofrecer una alta seguridad, es precisa, fiable y cuenta con una gran capacidad de almacenamiento de datos.

Sistemas biométricos: que se basan en el reconocimiento de una característica física de la persona que solicita el acceso para que pueda ser verificada de forma automática e instantánea. El más utilizado en las empresas es el lector de huella digital, que cuenta con numerosas ventajas como evitar la suplantación de identidad, acabar con los problemas de olvido de tarjetas, además de ser un sistema sencillo y eficaz.

Sistemas de reconocimiento de matrícula o TAG: Controlan el acceso mediante la identificación de la persona, del vehículo o la combinación de ambas. Los vehículos pueden identificarse por tarjeta/TAG o por lectura de matrícula.

4.2.2. Tipos de control de acceso según la conexión que necesiten

En segundo lugar, podemos distinguir los tipos de control de acceso según la conexión que necesiten para cumplir con sus funciones. Pueden ser:

Sistemas de acceso autónomos: son los que no se requiere ningún tipo de conectividad ya que los propios terminales disponen de memoria para la gestión de los usuarios. Se trata de un sistema que varía según la implementación y requerimientos del proyecto ya que está limitado a la administración de uno a uno y del nivel de acceso que requiera.

Sistemas de acceso en red: son los que utilizan herramientas como los softwares de control de acceso y que ofrecen un alto nivel de seguridad. Se pueden controlar a la vez infinitas zonas

diferentes de la empresa, acotar los accesos por horarios y permisos, y además cuentan con la ventaja de que pueden englobar otras soluciones importantes para toda empresa como el control horario.

4.3 Control de acceso a implementar

En nuestro trabajo describiremos un sistema que contempla las dos clasificaciones antes descritas, ya que es un sistema que puede trabajar de manera autónoma y también en red, por tener la capacidad de ser administrado desde el mismo dispositivo y desde un software de administración por medio de la red. Este Software permite a la vez administrar más de dos dispositivos aplicando diferentes reglas y privilegios de acceso como también la generación de reportes de asistencia del personal.

En nuestro sistema propuesto describiremos cada uno de los componentes que lo conforman y sus características aplicándolo a la medición de temperatura corporal y detección de portación de mascarilla, el sistema está compuesto de control de acceso marca DAHUA, modelo ASI7213X-TI, y el software de administración SmartPSS-AC.

4.3.1. Control de acceso ASI7213X-T1

El control que estaremos utilizando para dar solución a nuestra problemática planteada en nuestro trabajo de investigación es el ASI7213X-TI marca Dahua, que es un equipo biométrico de reconocimiento facial y con la integración de una cámara térmica para la toma de temperatura corporal.

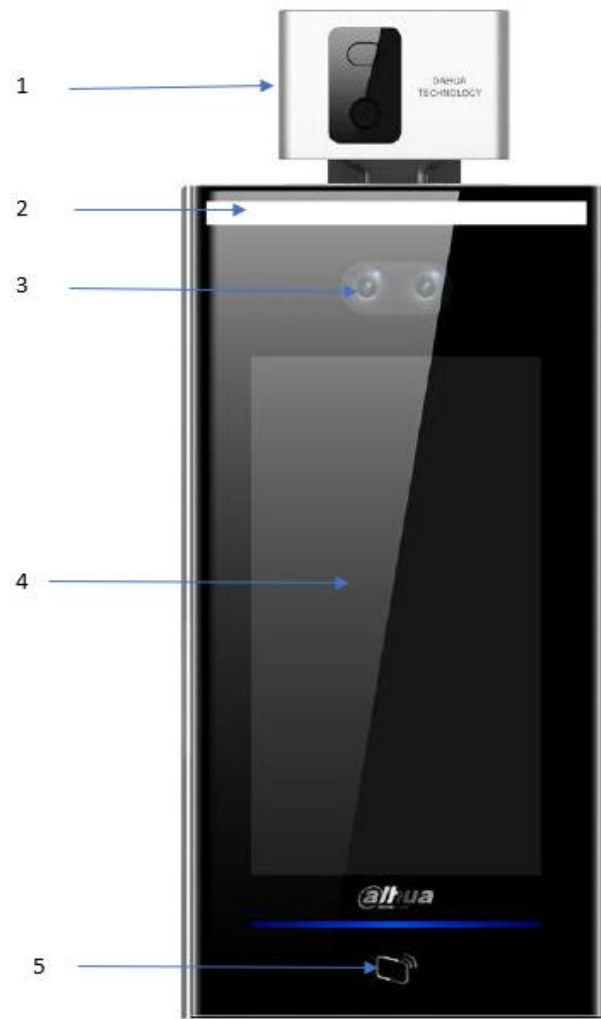


Figura 28: Control de acceso DAHUA ASI7213X-T1

En la figura podemos ver cada uno de los componentes del cual consta el control de acceso o los más importantes para nuestra solución:

1- Cámara térmica: Esta permite el monitoreo de temperatura corporal, en el rango de temperatura de 30°C. a 50° C.⁶

2: Luz de llenado automática: Esta reduce la contaminación lumínica.

⁶ Ficha técnica Serie ASI7 DHI-ASI7213X-T1 página N° 2, en anexos

3: Cámara de reconocimiento facial de tecnología CMOS⁷ de 2MP⁸, WDR⁹, que es utilizada para la detección de rostros y para la identificación de mascarilla, si esta última opción está habilitada, informara si la portación de mascarilla es correcta o incorrecta.

Con el algoritmo de reconocimiento facial, el controlador de acceso puede reconocer más de 360 posiciones en el rostro humano. Permite detección de vida en rostros humanos.

4: Pantalla LCD de 7 pulgadas con resolución de 600 X 1024, la cual permite la visualización de la captura de imagen del usuario y de las mediciones hechas por el equipo. También por ser una pantalla táctil nos permite ingresar a las configuraciones del equipo y parametrizar sus funciones sin la necesidad de estar conectado a una PC.

5: Lector de tarjetas IC de proximidad con capacidad de 100,000 tarjetas.

4.3.2. Sistema de control de acceso ASI7213X-T1

El control de acceso ASI7213X-T1 está conformado por un procesador incorporado que permite hacer todo el tratamiento de la imagen y de las mediciones de temperatura, este hace todas las comparaciones con las cuales está parametrizado y de acuerdo al proceso de las señales realizado, se genera una señal de alerta en el caso que se superen los parámetros permitidos, como ejemplo podemos decir que si el límite de temperatura está configurado en 36.5°C y una persona ingresa con una temperatura superior, el equipo alertará en su pantalla con un mensaje configurado por el administrador del sistema por ejemplo: “La Temperatura es alta”,

⁷ CMOS: Complementary Metal Oxide Semiconductor por sus siglas en ingles.

⁸ MP: Mega, Pixel: Elemento más pequeño de una imagen reproducida digitalmente.

⁹ WDR: Wide Dynamic Range por sus siglas en ingles.

Umbral de reconocimiento facial: 85

Ángulo máx. de reconocimiento facial: 90

Umbral de anti-falsificación: ☐ Activar ☒ Cerrar

Config. del brillo de la luz de relleno: 30

Config. del modo de luz de relleno: ☐ NA ☐ NC ☒ Auto

Luz infrarroja: 40

Se agotó el tiempo de espera de(S): 3 (1-6)

Tiempo de intervalo de rostro inválido(S): 3 (1-6)

Distancia pupilar: 45 (0-500)

ID del Canal: 1

Activar exposición de rostro: ☒ Activar ☐ Cerrar

Brillo objetivo de rostro: 50

Tiempo de detección del intervalo de exposición de rostro (S): 10 (1-28800)

Monitoreo de la temperatura: ☒ Activar ☐ Cerrar

Unidad de temperatura: °C

Área de detección: ☒ Activar ☐ Cerrar

Distancia de monitoreo de TEMP (cm): 0 (0-200)

Umbral de temperatura: 36.50 (0-70)

Valor de corrección de temperatura: 0.00 (-70-70)

Modo máscara: Interceptar máscara

Figura 29: Parámetros de configuración temperatura control de acceso

El Control de acceso ASI7213X-T1 cuenta con protocolo de internet IPv4¹⁰, RTSP¹¹, RTP¹², TCP¹³ el cual nos permite la administración del mismo de forma web a través de unos de sus puertos de comunicación LAN¹⁴ y por la IP¹⁵ que está configurada en ese puerto.

¹⁰ IPv4: Internet Protocol version 4

¹¹ RTSP: Real Time Streaming Protocol

¹² RTP: Real Time Transport Protocol

¹³ TCP: Transmission Control Protocol

¹⁴ LAN: Local Area Network

¹⁵ IP: Internet Protocol

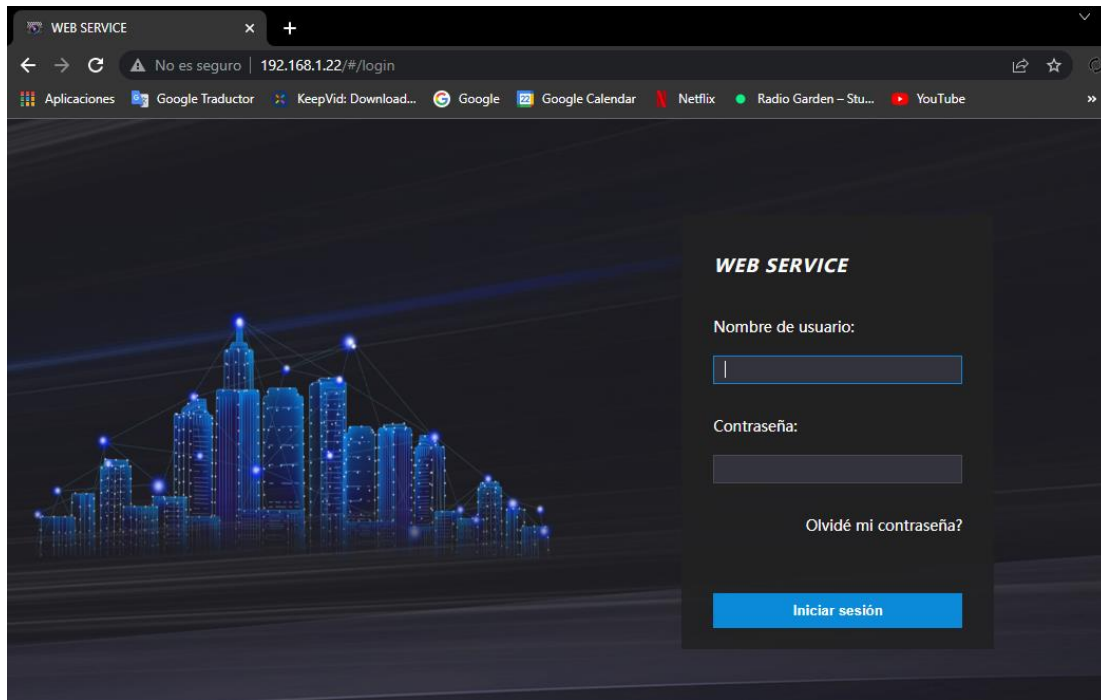


Figura 30: Pagina web de inicio de sesión

4.3.3. Descripción de funcionamiento de sus componentes

4.3.3.1 Pantalla.

Estos dispositivos constan de una pantalla de 7 pulgadas con sensores capacitivos que contienen electrodos X e Y con una capa de aislamiento entre ellos. Los electrodos transparentes normalmente se fabrican en forma de diamante con ITO y con puente de metal.

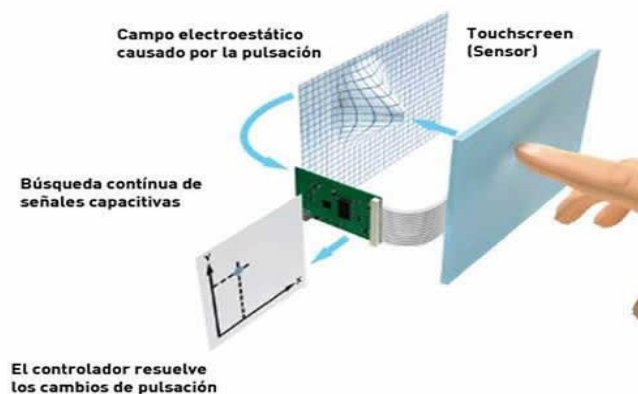


Figura 31: Sensor capacitivo touch

El cuerpo humano es conductor porque contiene agua. La tecnología capacitiva proyectada hace uso de la conductividad del cuerpo humano. Cuando un dedo desnudo toca el sensor con el

patrón de los electrodos X e Y, ocurre un acoplamiento de capacitancia entre el dedo humano y los electrodos que cambia la capacitancia electrostática entre los electrodos X e Y. El controlador de pantalla táctil detecta el cambio de campo electrostático y la ubicación. La pantalla cuenta con una resolución de 600h y 1024 v esto significa que los números de los píxeles o las nomenclaturas que utilizamos para referirnos a ellos son muy similares en las pantallas y en los vídeos. Esto es útil, porque una pantalla no puede aprovechar la máxima calidad de un vídeo que tenga una resolución mayor.

A la hora de referirnos a las resoluciones solemos utilizar dos números, como por ejemplo 600 H x 1024 V que indican la cantidad de píxeles que se muestran en la pantalla. El primero de estos números indica la cantidad de píxeles horizontales y en el segundo número se indican los píxeles verticales.

4.3.3.2 Cámara de reconocimiento facial.

La cámara que posee este dispositivo cuenta con tecnología de captación llamada CMOS¹⁶ (Por siglas en ingles), conformado por pixeles independientes donde la digitalización se realiza internamente en unos transistores. Una de las grandes ventajas es que los sensores CMOS son más sensibles a la luz, por lo que en condiciones pobres de iluminación se comportan mucho mejor. Por lo que hace que el equipo tenga un menor consumo de energía haciéndolo más eficiente.

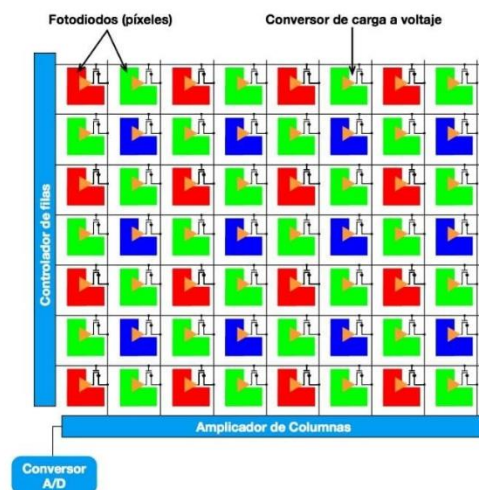


Figura 32: Sensor cámara CMOS

¹⁶ CMOS: Complementary Metal Oxide Semiconductor

Otra de las ventajas que posee este sistema es que cuenta con la tecnología WDR¹⁷, esto ayuda a compensar los problemas que surgen con la exposición a la luz. Con la tecnología WDR, la cámara compensa las imágenes donde existen zonas oscuras y brillantes, en las que se produce una gran descompensación y no podemos ver las imágenes nítidas si empleamos una cámara normal.

Con esta tecnología, se consigue un equilibrio entre el brillo y la oscuridad mejorando notablemente la calidad de la imagen y obteniendo un resultado más uniforme, gracias a ese tratamiento dinámico de la luz.

4.3.3.3 Compensación de luz.

Para una mejor detección de escaneo facial, el sistema cuenta con una luz blanca automática, con el objetivo de mejorar el reconocimiento facial cuando la luminosidad del rostro es muy baja, reduciendo el porcentaje de error en el reconocimiento facial.

Otra de las funciones posee este dispositivo es la luz IR (Luz Infrarroja es un tipo de luz electromagnética y térmica) para realizar el reconocimiento facial en total ausencia de luz.

4.3.3.4 Monitoreo de temperatura.

El dispositivo cuenta con una cámara termográfica con capacidad de leer un rango de temperatura de 30° a 50° C. Su resolución es de 120 * 90 píxeles, la precisión con que está diseñada por el fabricante es de 0.1°C. Para dispositivo las distancias mínimas y máximas para el monitoreo de temperatura son de 30cm a 180 cm respectivamente para que las lecturas sean correctas o evitar falsas lecturas. Considerando los conceptos vistos en el capítulo II podemos decir que la cámara infrarroja utilizada en el equipo propuesto es una cámara no refrigerada ya que para esta aplicación no se requiere de alta precisión y como cámara activa ya que necesita de una fuente de calor IR para hacer la comparación térmica del cuerpo a medir. (Rostro)

¹⁷ WDR: Wide Dynamic Range por sus siglas en ingles



Figura 33: Cámara termográfica

La cámara térmica detecta la temperatura capturando diferentes niveles de luz infrarroja, invisible a la vista humana, que es irradiada por el sensor que incluye dicha cámara. Cuanto más caliente es un objeto, más radiación infrarroja produce. La cámara térmica detecta la radiación y esta información la procesa presentando en pantalla el valor obtenido.

4.3.3.5 Configuración del monitoreo de temperatura en el control de acceso Dahua.

Para esta configuración se tiene dos opciones, ingresando desde el equipo como usuario administrador y la otra opción es desde su administración web.

Explicaremos la segunda opción ya que es más práctica la interacción de con el equipo y se puede hacer desde un ordenador.

Paso 1 Ingresamos mediante la IP configurada en el equipo en navegador.

Paso 2 Ingresamos con usuario admin para tener acceso a estos parámetros.

Paso 3 En la opción “Detección de caras” encontraremos la opción de activar o desactivar el monitoreo de temperatura. En nuestro caso se activará para que el equipo pueda hacer el monitoreo de temperatura mediante la cámara térmica.

Monitoreo de la temperatura ☒ Activar ☐ Cerrar

Unidad de temperatura °C

Área de detección ☒ Activar ☐ Cerrar

Distancia de monitoreo de TEMP (cm) 0 (0-200)

Umbral de temperatura 36.90 (0-70)

Valor de corrección de temperatura 0.00 (-70-70)

Modo máscara Interceptar máscara

Figura 34: Parámetros de activación de monitoreo de temperatura

Paso 4 En el parámetro Unidad de temperatura seleccionamos la unidad en Centígrados (C°) o Fahrenheit (F°).

Monitoreo de la temperatura ☒ Activar ☐ Cerrar

Unidad de temperatura °C

Área de detección ☒ Activar ☐ Cerrar

Distancia de monitoreo de TEMP (cm) 0 (0-200)

Umbral de temperatura 36.90 (0-70)

Valor de corrección de temperatura 0.00 (-70-70)

Modo máscara Sin detectar

Figura 35: Unidades disponibles en el sistema biométrico (°C y °F)

La distancia de monitoreo de temperatura es otra opción de configuración que nos ayuda al momento de la instalación del equipo, permitiendo establecer una distancia en la que el fabricante recomienda que es entre 0.30m a 1.8m para mejorar las lecturas hechas por la cámara.

Umbral de temperatura, con esta opción podemos configurar el equipo con una temperatura umbral, orientada a reconocer la presencia de procesos febriles, de acuerdo al MINSAL (Ministerio de Salud Republica de El Salvador), este umbral es de 37.1 °C, siguiendo esta normativa, debemos configurar este valor en esta casilla, así, cuando un usuario supere este valor el equipo nos alerta en pantalla indicando que la temperatura supera el umbral ayudando a identificar posibles casos de COVID y tomar los protocolos que la Universidad tenga establecidos, entre estos, restringir el

acceso a las instalaciones. En caso contrario de temperatura normal solo se mostrará en pantalla la temperatura registrada dando como acceso permitido.

La siguiente opción “Valor de corrección de temperatura” mostrada en la imagen N° 35 que va de un rango de -70 a 70 se utiliza para compensar la lectura de acuerdo a la temperatura ambiente.

4.3.3.6 Opciones de uso de mascarilla.

Se tienen tres opciones de configuración que serán tomadas en consideración según se requiera, a continuación, se describirán cada una de ellas:

- Sin detectar: el sistema omite la portación de mascarilla por el usuario, si el usuario no la porta, el siempre permitirá el acceso.
- Recordatorio de máscara¹⁸: El sistema detecta si el usuario porta o no porta máscara, permitiendo el acceso en ambos casos
- -Interceptar mascarilla: Para nuestra aplicación es la opción principal ya que el sistema igual

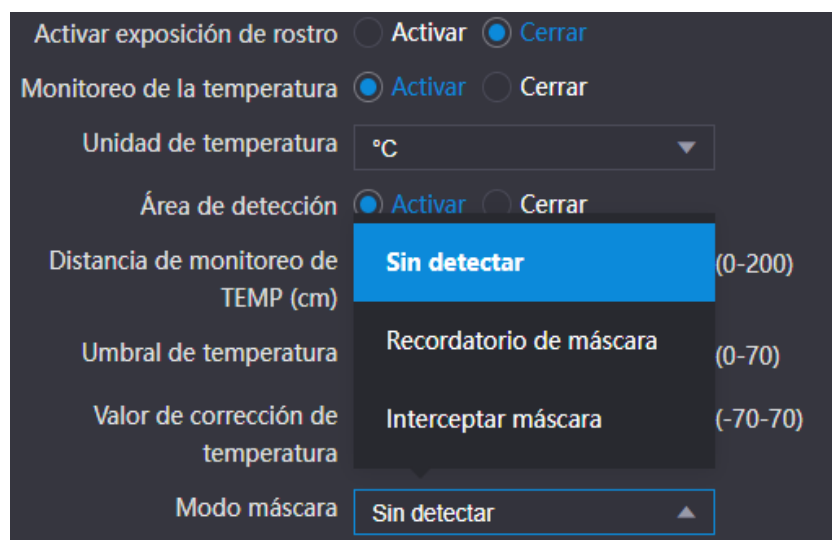


Figura 36: Parámetros de activación de máscara en el sistema

que en la opción anterior detecta la portación de la máscara, restringiendo el acceso al no detectarla, mostrando alarma de portación de máscara.

4.4. Software SMARTPSS-AC

Smart PSS-AC es un software cliente, desarrollado para administración de dispositivos de control de acceso y monitoreo de temperatura, este software nos permite la administración de uno

¹⁸ El termino máscara equivalente de mascarilla es utilizado por el fabricante del control de acceso.

a varios dispositivos, administración de usuarios, horarios de trabajo, niveles de acceso a áreas de ingreso restringido y exportación de reportes.

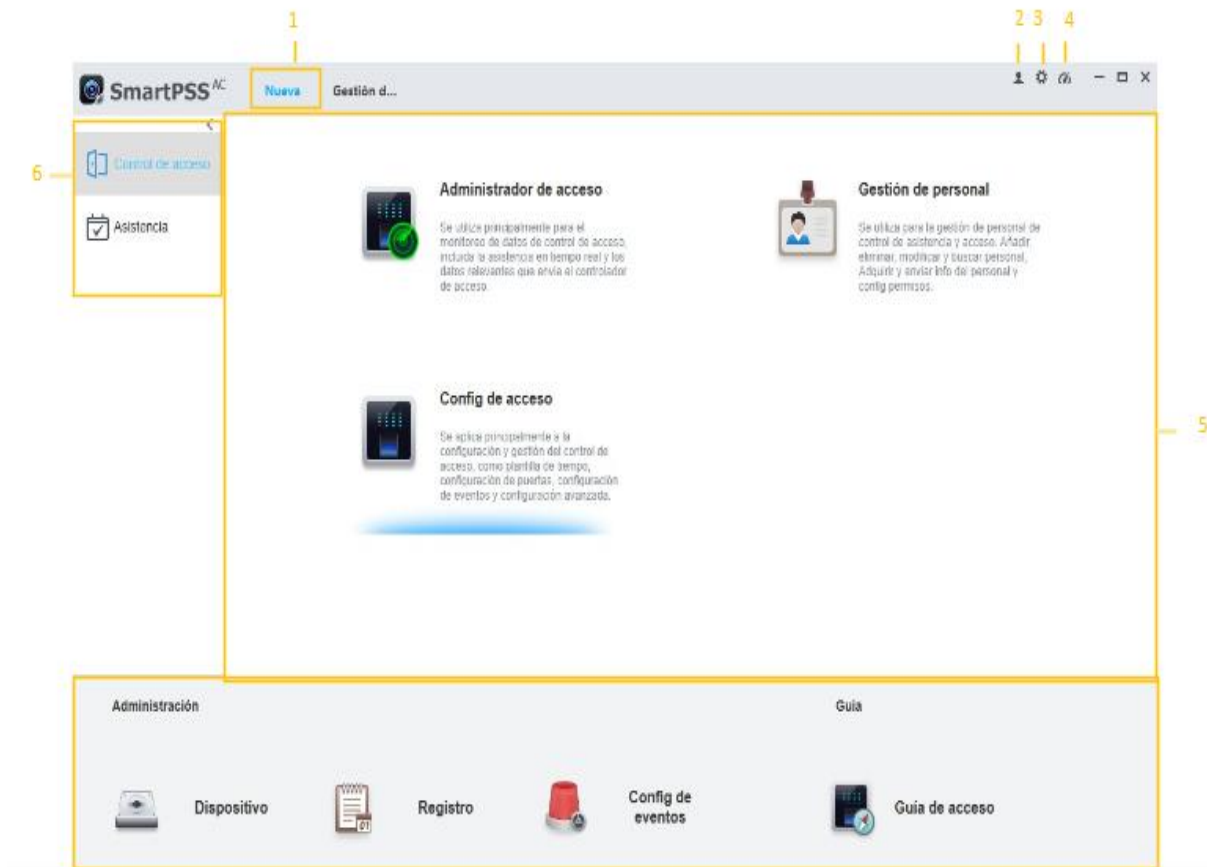


Figura 37: Página principal del Software SmatPSS

Tabla 4 : Descripción de funciones de la página de inicio Software SmartPSS

No.	Parámetro	Descripción
1	Pestaña Función	Mostrar la página de inicio por defecto. Cuando hace clic en una función por primera vez, la pestaña de función se agrega aquí
		- Click  y seleccione Cambiar usuario para volver a la interfaz de inicio de sesión. Puede iniciar sesión con una nueva cuenta. - Click  y seleccione Pantalla de bloqueo para bloquear la pantalla. Ingrese la contraseña de la cuenta de inicio de sesión cuando desee desbloquear.

2	Gestión de usuarios	• Click  y seleccione Cambiar usuario para volver a la interfaz de inicio de sesión. Puede iniciar sesión con una nueva cuenta. • Click  y seleccione Manual de ayuda para obtener el manual del usuario. • Click  y seleccione Acerca de para ver la versión y la fecha del sistema. Habilite Abrir registro de depuración para que los registros de depuración se guarden automáticamente en una ruta local, para localizar y resolver problemas.
3	Configuración del sistema	• Configuración básica ○ Temporización: habilite la verificación automática de la hora todos los días y configure la verificación de la hora para que los dispositivos verifiquen la hora automáticamente en el momento establecido. ○ Idioma: muestra el idioma que se activa después de reiniciar. ○ Hora de guardado del registro: establezca la hora de guardado del registro y luego se guardarán los registros desde hoy hasta la hora establecida. Esta función se activa después de reiniciar. Por ejemplo, establezca el tiempo de guardado en 30 y luego se guardarán los registros de los últimos 30 días. ○ Formato de datos: seleccione el formato de visualización de datos. ○ Formato de hora: seleccione el formato de visualización de la hora. ○ Capacidad de la red: seleccione la capacidad de la red de acuerdo con la condición de su red. Por ejemplo, cuando la condición de la red es fluida, se recomienda seleccionar Alta. ○ Máscara: seleccione la máscara que se activa después de reiniciar. La configuración predeterminada es blanco grisáceo. • Evento ○ Habilite el bucle de sonido del evento. ○ Seleccione el sonido del evento. Puede seleccionar el sonido necesario o agregar los sonidos personalizados en la ruta. ○ Habilitar y configurar SMTP. • Camino local Las rutas de almacenamiento. • Gestión de datos

		○ Extraer regularmente: Configure el tiempo de extracción regular para que los datos de asistencia de los dispositivos se extraigan en un tiempo predefinido. Por ejemplo, si configura las 8:00 de todos los días como hora de extracción regular, el SmartPSS-AC extraerá automáticamente los datos de asistencia desde las 8:00 del día anterior hasta las 8:00 de hoy a las 8:00 de la mañana. ○ Borrar regularmente: establece el tiempo de ahorro para datos e imágenes. SmartPSS-AC borra automáticamente los datos y las imágenes que exceden el tiempo de ahorro. Se activa a las 00:00 todos los días o cuando se inicia el software. • Copia de seguridad: soporte para realizar copias de seguridad de forma automática y manual. ○ Manual: seleccione la ruta de la copia de seguridad y haga clic en Copia de seguridad manual. ○ Automático: seleccione la ruta de la copia de seguridad y habilite la copia de seguridad automática. • Restaurar: haga clic en Restaurar y seleccione el archivo de respaldo que necesita. Las configuraciones restaurarán las configuraciones del archivo.
4	Estado del Sistema	Click  Haga clic para ver el estado de uso de la CPU y la RAM. Si el uso de la CPU es alto, el ícono se vuelve rojo.
5	Módulo de función	Haga clic en el icono de función para ir a la interfaz de función.
6	Módulo de solución	Seleccione la solución necesaria. Haga clic  para mostrar u ocultar soluciones.

4.4.1. Administración de dispositivos

El SmartPSS-AC permite agregar dispositivos. Puede configurar y operar los dispositivos de forma remota después de agregarlos mediante SmartPSS-AC.

4.4.2. Agregar dispositivo

Hay varios métodos para agregar dispositivos. Seleccione el método más adecuado según las situaciones, como la dirección IP y el segmento de red.

-Búsqueda automática

-Agregar manualmente

-Importar en lotes

4.4.2.1 Adición de dispositivos mediante búsqueda automática.

Se recomienda agregar dispositivos mediante búsqueda automática cuando necesite agregar dispositivos en lotes dentro del mismo segmento de red, o cuando el segmento de red está claro, pero la dirección IP del dispositivo no está clara.

Paso 1 Haga clic en Búsqueda automática en la interfaz del Administrador de dispositivos.

Paso 2 Configure el rango del segmento de red y luego haga clic en Buscar.

N...	IP	Tipo de dispositivo	Dirección MAC	Puerto	Estado de inicialización
1	192.168.1.21	DHI-ASI7213X-T1	08:ed:ed:f0:8b:ed	37777	Iniciado

Figura 38: Búsqueda automática

Paso 3 Haga clic en los dispositivos necesarios y luego haga clic en Agregar.

Paso 4 Ingrese el nombre de usuario y la contraseña de inicio de sesión y luego haga clic en Aceptar para confirmar.

La interfaz de búsqueda automática aún se muestra después de agregar dispositivos. Puede continuar agregando o haciendo clic en Cancelar para salir.

Los dispositivos se registran automáticamente después de agregarlos. Si el inicio de sesión es exitoso, el estado se muestra como en línea; de lo contrario, fuera de línea.

4.4.2.2 Agregar dispositivo manualmente.

Se recomienda agregar dispositivos manualmente cuando necesite agregar un solo dispositivo con cierta dirección IP o nombre de dominio.

Paso 1 Seleccione Agregar en la interfaz del Administrador de dispositivos.

Paso 2 Configure los parámetros del dispositivo.

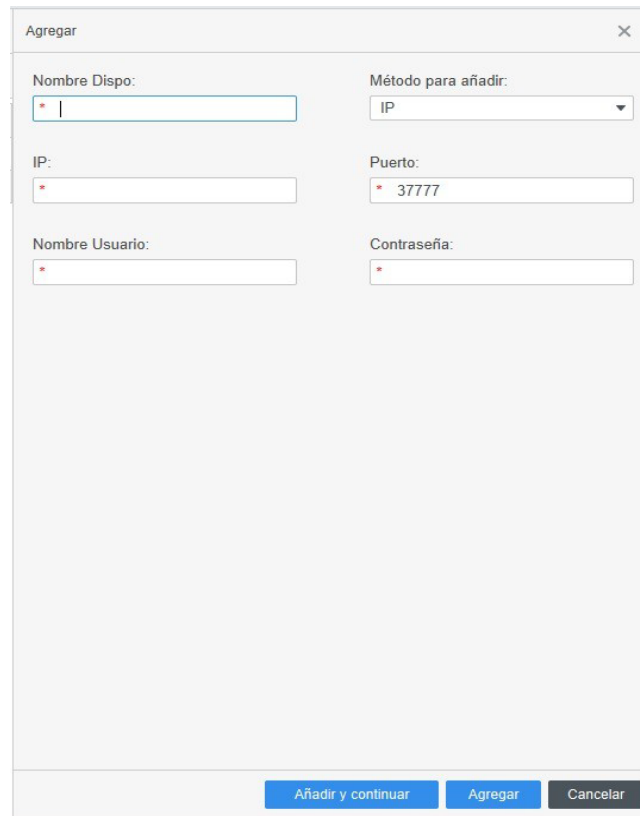


Figura 39: Parámetros de configuración IP

Tabla 5: Descripción de parámetros IP

Parámetro	Descripción
Nombre del dispositivo	Se recomienda nombrar los dispositivos con el área de monitoreo para una fácil identificación.
Método para agregar	Seleccione el método para agregar.
IP	Ingresa la dirección IP del dispositivo aquí cuando seleccione IP como el método para agregar.
Puerto	Ingresa el número de puerto, y el número de puerto es 37777 por defecto. Prevalecerá el número de puerto real.
Nombre de usuario	Introduzca el nombre de usuario de inicio de sesión.
Contraseña	Introduzca la contraseña de inicio de sesión.

Paso 3 Haga clic en Agregar para agregar el dispositivo y cerrar la interfaz Agregar dispositivo; o haga clic en Agregar y continuar para agregar el dispositivo y permanezca en la interfaz Agregar dispositivo para que pueda agregar otro dispositivo convenientemente.

4.4.2.3. Importación de dispositivos en lotes.

Se recomienda agregar dispositivos importando cuando necesite agregar dispositivos en lotes, pero no están en el mismo segmento de red. Organice la información del dispositivo como un archivo en formato .XML y luego importe el archivo.

Puede exportar la plantilla de información del dispositivo. Seleccione un dispositivo y haga clic en Exportar.

Paso 1 Haga clic en Administrador de Paso 1 dispositivos > Importar.

Paso 2 Seleccione el archivo de información y haga clic en Importar.

Los dispositivos se iniciarán automáticamente después de agregarlos. Si el inicio de sesión es exitoso, el estado se muestra como en línea; de lo contrario, está fuera de línea.

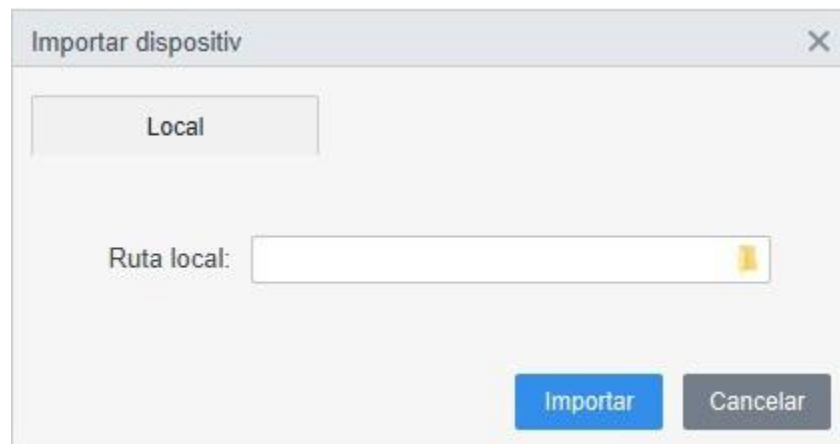


Figura 40 : Ruta de importación de dispositivos

4.4.2.4 Eliminación de dispositivo

Paso 1 Seleccione Administrador de dispositivos en la página de inicio.

Paso 2 Seleccione el dispositivo que ya no necesita y luego haga clic en Eliminar que está en el lado derecho del dispositivo.

Paso 3 (Opcional) seleccione Al mismo tiempo eliminar la instantánea y el video del dispositivo si no necesita esas instantáneas y videos; de lo contrario, no lo marque.

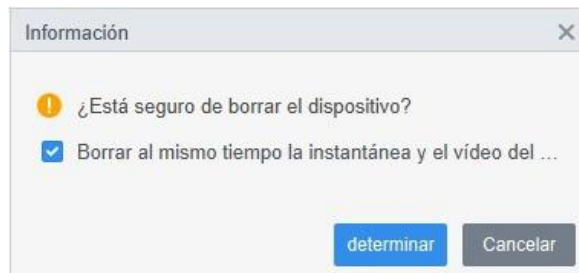


Figura 41: Confirmación de borrado de dispositivo

Paso 4 Haga click en Determinar.

4.5. Registro de usuarios

Nuestra solución es completamente funcional sin que un usuario esté registrado sin embargo el sistema está equipado para poder administrar 100,000 usuarios que estén ingresados o enrolados en el sistema, en este apartado detallaremos el procedimiento para dar ingreso a usuarios que se requieran o sean parte de la institución.

4.5.1 Agregar usuarios en el control de acceso

En el control de acceso ASI7213X-T1 ingresamos a la administración

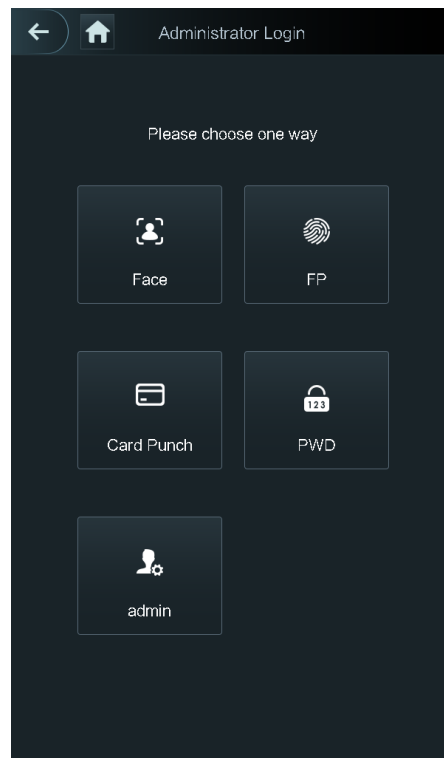


Figura 42: Interface gráfica del control de acceso ASI7213X-T1

Luego seleccionamos el icono de usuario



Figura 43: Menú principal del control de acceso

Luego, en opción de usuarios podemos configurar cada uno de los parámetros que hace único a cada usuario como por ejemplo Id, Nombre y datos biométricos como el reconocimiento facial

The image shows a 'New User' configuration screen with a dark background. At the top, there is a back arrow, the title 'New User', and a checkmark icon. Below the title, there is a list of parameters and their values:

User ID	3
Name	
Face	0
Card	0
PWD	
User Level	User
Period	255-Default
Holiday Plan	255-Default
Valid Date	2037-12-31
User Level	General
Use Time	Unlimited

Figura 44: Parámetros de usuario en el control de acceso

En esta etapa se establece el nivel o perfil de usuario ya que de esto dependerá si tendrá permisos para poder ingresar a las configuraciones del equipo, Se tienen dos opciones: Usuario y Administrador.

Usuario: Solo tendrá permisos para ingresar

Administrador: Podrá ingresar y también tendrá permisos a las configuraciones de los parámetros del equipo.

4.5.2 Extraer usuarios al software SmartPPS-AC

Una vez ingresado los usuarios en el control de acceso (Enrolado), es necesario realizar la importación al software que se encarga de la administración y asignación de los diferentes horarios que se pueden crear en el mismo.

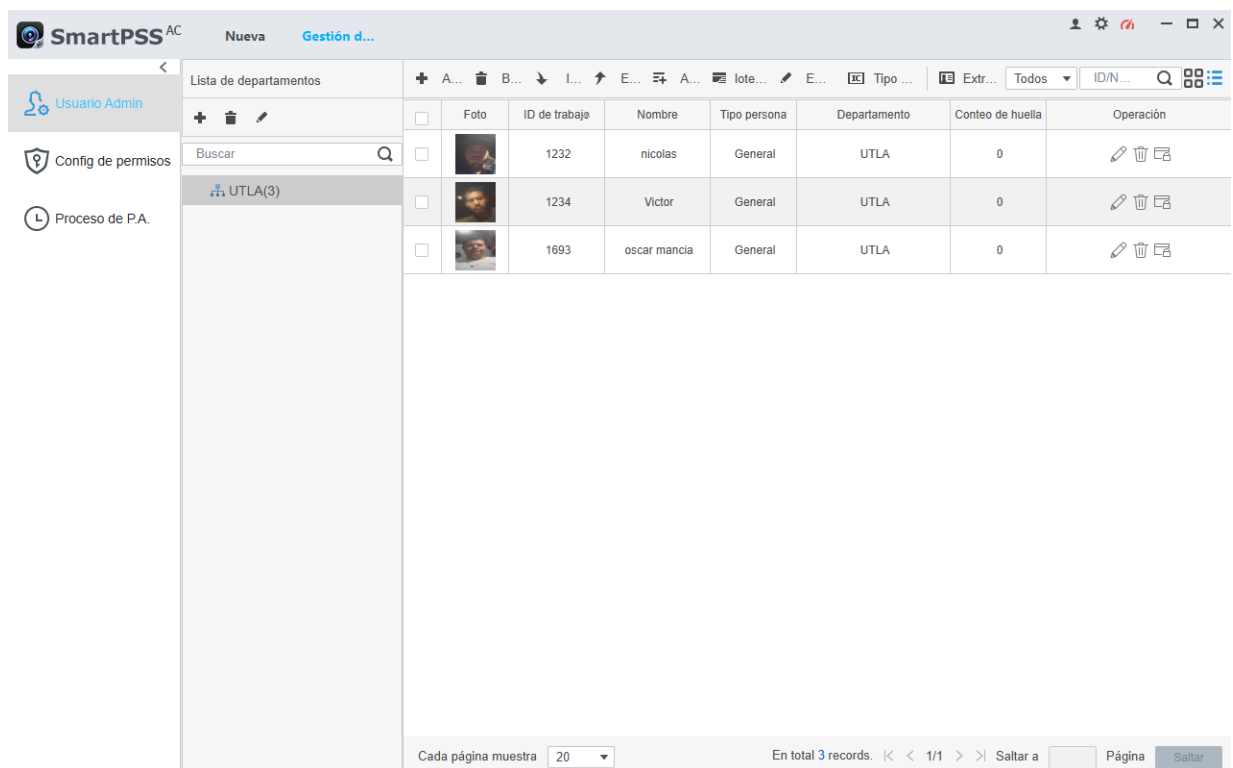


Foto	ID de trabajo	Nombre	Tipo persona	Departamento	Conteo de huella	Operación
	1232	nicolas	General	UTLA	0	  
	1234	Victor	General	UTLA	0	  
	1693	oscar mancia	General	UTLA	0	  

Figura 45: Listado de usuarios enrolados en el sistema

- Seleccionamos la opción extraer en la parte superior



Figura 46: Extraer usuario

- Se nos presentará la lista de dispositivos disponibles con su dirección IP, seleccionamos en el cual se efectuó el enrolamiento de los usuarios y damos click en determinar.

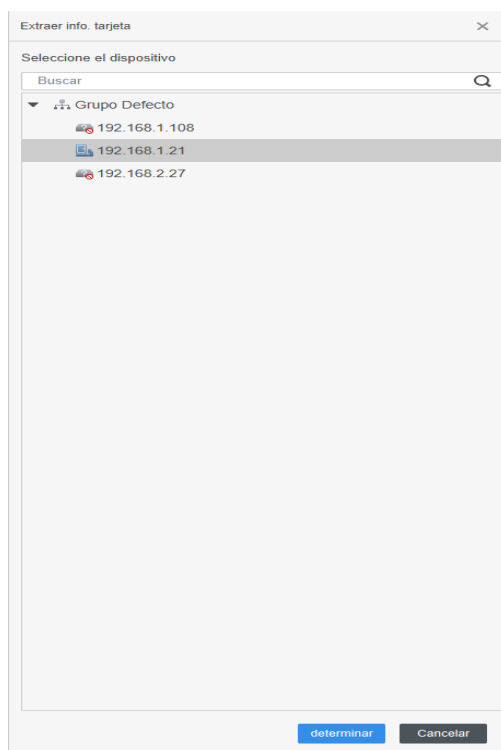


Figura 47: Selección de dispositivo

- El sistema inicia la descarga de todos los usuarios disponibles mostrando en una lista como se ve en la imagen siguiente.

Seleccionamos todos o solo los usuarios que se necesiten importar al software y damos click en Extraer, iniciara la descarga de los usuarios al sistema según los datos ingresados en el procedimiento de enrolamiento que ingresamos en el equipo.

Extraer info. tarjeta

IP de dispositivo:192.168.1.21

ID/Nombre/Tarjeta

☐	Num.	ID de usuario	Nombre	Nº de tarjeta	Tipo persona	Departamento	Recuento de huellas
☐	1	1693	oscar mancia		General		0
☐	2	1234	Victor		General		0
☒	3	1232	nicolas		General		0

Extraer

Exportar

Cancelar

Figura 48: Información de usuarios en el control de acceso

4.5.3 Diagrama de bloques de la solución

En el siguiente diagrama de bloques representamos los componentes principales del sistema para la comprensión del sistema.

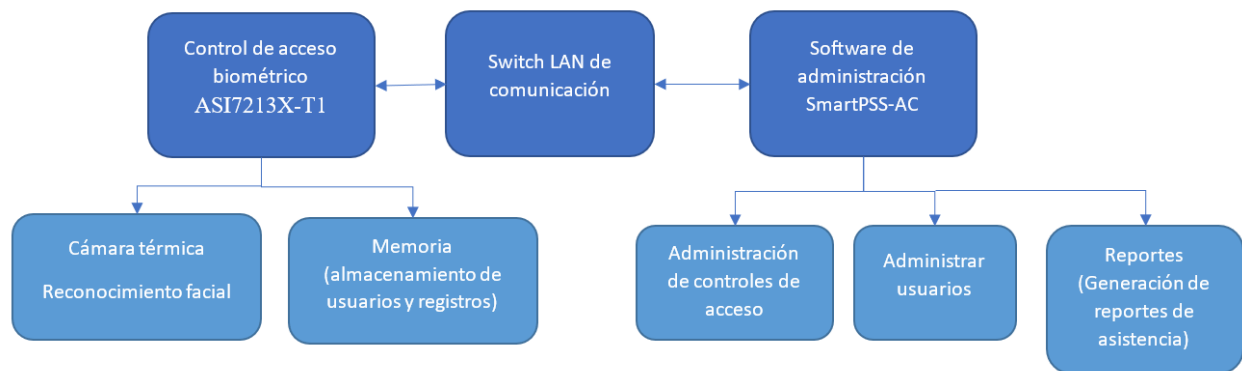


Figura 49 Diagrama de bloques de la solución

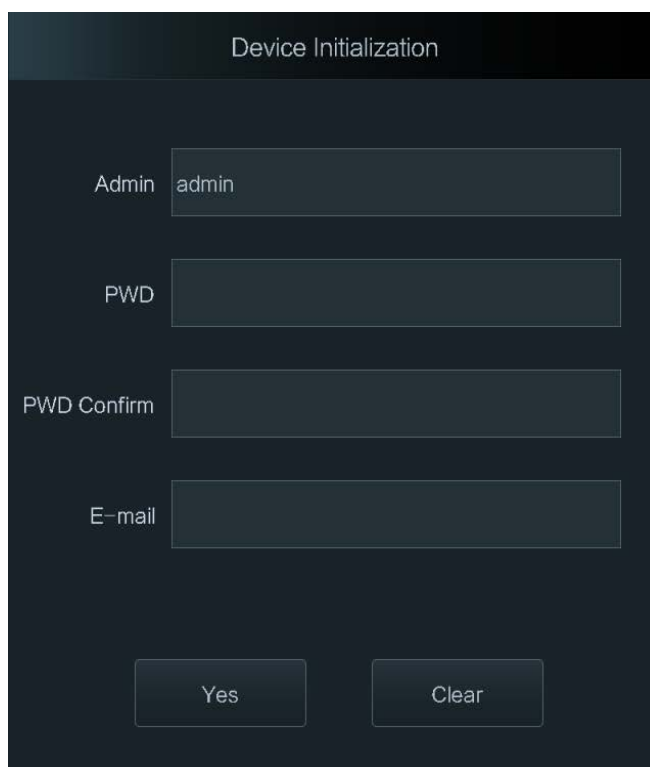
Capítulo V: Implementación del proyecto

5.1. Procedimiento de instalación y configuración de los controles de acceso

En este apartado explicaremos los requisitos y pasos para la implementación del sistema de control de temperatura y detección de mascarilla, que estarán ubicados en el ingreso principal de la Universidad Técnica Latinoamericana campus edificios A-B-C-D y puerta de ingreso de los laboratorios especializados de la UTLA.

5.1.1. Inicialización

La contraseña de administrador y un correo electrónico deben configurarse la primera vez que se enciende el controlador de acceso o después de reiniciarlo; de lo contrario, no se puede utilizar el controlador de acceso.



Device Initialization

Admin admin

PWD

PWD Confirm

E-mail

Yes Clear

Figura 50 Inicio de sesión

- El administrador y la contraseña establecidos en esta interfaz se utilizan para iniciar sesión en la plataforma de administración web¹⁹.

¹⁹ World Wide Web

- La contraseña del administrador se puede restablecer a través de la dirección de correo electrónico que ingresó si el administrador olvida la contraseña.
- La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excepto '“; &).

Tabla 6: Iconos comunes del control de acceso

Icono	Descripción
	Icono del menú principal.
	Confirmar icono.
	Pase a la primera página de la lista.
	Pase a la última página de la lista.
	Vaya a la página anterior de la lista.
	Pase a la página siguiente de la lista.
	Vuelve al menú anterior.
	Habilitar.
	Deshabilitar.



Figura 51 Página principal del Control de acceso DHI-ASI7213X-T1

Tabla 7: Descripción de partes de la página principal

No.	Descripción
1	Métodos de desbloqueo: Tarjeta, rostro y contraseña. (Cuando la tarjeta, el rostro y la contraseña están configurados como modo de desbloqueo, el ícono de la contraseña no se mostrará en la esquina superior izquierda del controlador de acceso.)
2	Fecha y hora: Muestra la fecha y hora en tiempo real.
3	Muestra el estado de la red y el estado del USB.
4	Icono del menú principal. (Solo los usuarios con permiso de administrador pueden ingresar al menú principal.)
5	Icono de desbloqueo de contraseña.
6	Icono de desbloqueo de contraseña de administrador.

5.1.2. Menú principal

En el menú principal los administradores pueden agregar usuarios de diferentes niveles, establecer parámetros relacionados con el acceso, configurar la red, ver registros de acceso e información del sistema.

Paso 1 Toque en la interfaz de espera.



Paso 2 Seleccione un método de entrada del menú principal.

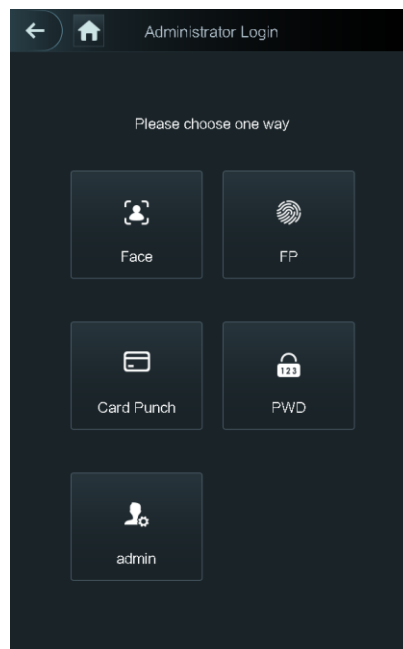


Figura 52 Menú administración

Después de seleccionar el método de desbloqueo, el equipo nos muestra el menú principal



Figura 53 Menú principal

5.1.3. Instalación física de los controles de acceso ASI7213X1-T1

En la Universidad Técnica Latinoamericana se ha definido el siguiente procedimiento para la instalación física del control de acceso ASI7213X1-T1.

1. Instalación de punto de red desde el Laboratorio de Informática ubicado en el segundo nivel del edificio “B” desde el cual hay una distancia de alrededor de 50 metros a la ubicación seleccionada para el control de acceso. La trayectoria del cable UTP²⁰ utilizado se canalizará con tecno-ducto cumpliendo con la normativa de instalación de red en intemperie.
2. Instalación de punto de red desde la entrada principal del laboratorio hacia la oficina de administración que está a una distancia de alrededor 10m a la ubicación seleccionada para el control de acceso.
3. Instalación de toma de alimentación 110VAC²¹ para la alimentación de la fuente de poder con que cuenta el control de acceso.
4. Instalación de acrílico para la protección de salpicaduras de agua y polvo del ambiente.

²⁰ Unshielded twisted pair (UTP) o cable de par trenzado no apantallado

²¹ VAC: Voltaje de corriente continua

Se ha definido instalar instaló el control de acceso a una altura de 1.4 metros del piso cumpliendo con las recomendaciones que sugiere el fabricante para las lecturas correctas de temperatura, mascarilla y de reconocimiento facial (ver figura 52).

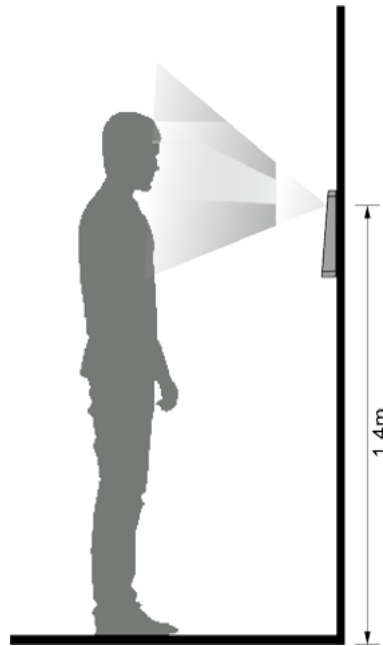


Figura 54 Guía de instalación

5.1.4. Ubicación de geográfica.

El control de acceso se tiene proyectado instalar en el ingreso principal de la Universidad Técnica Latinoamericana campus edificios A-B-C-D, 3ª Avenida Norte, 1501 - Santa Tecla, Departamento de La Libertad, Ubicación en coordenadas geográficas decimales 13.677979, - 89.285900.

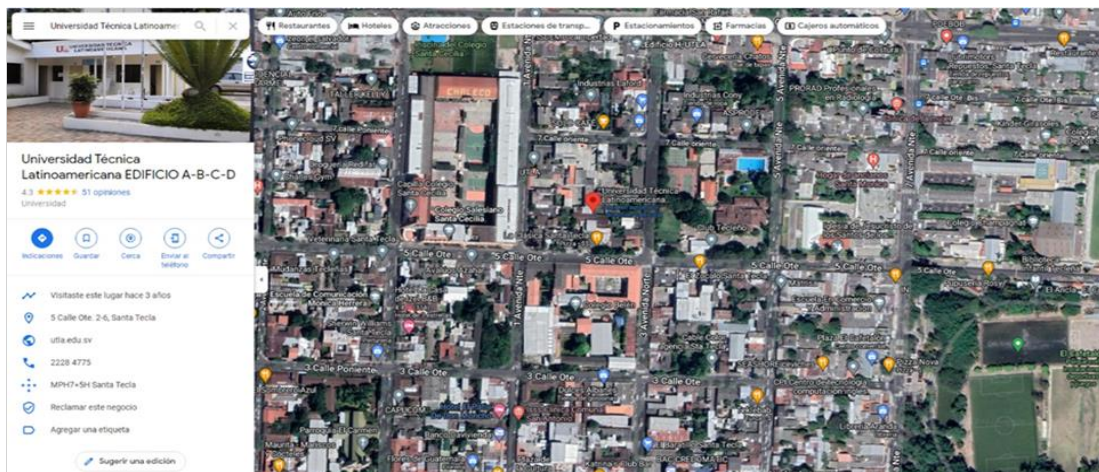


Figura 55 Ubicación geográfica del Campus UTLA

El control de acceso se instaló en el pasillo de ingreso de los laboratorios especializados de la UTLA, ubicados en 3ª Avenida Norte Y 7ª Calle Oriente No. 5-1, - Santa Tecla, Departamento de La Libertad, Ubicación en coordenadas geográficas decimales 13.679121, -89.289218.

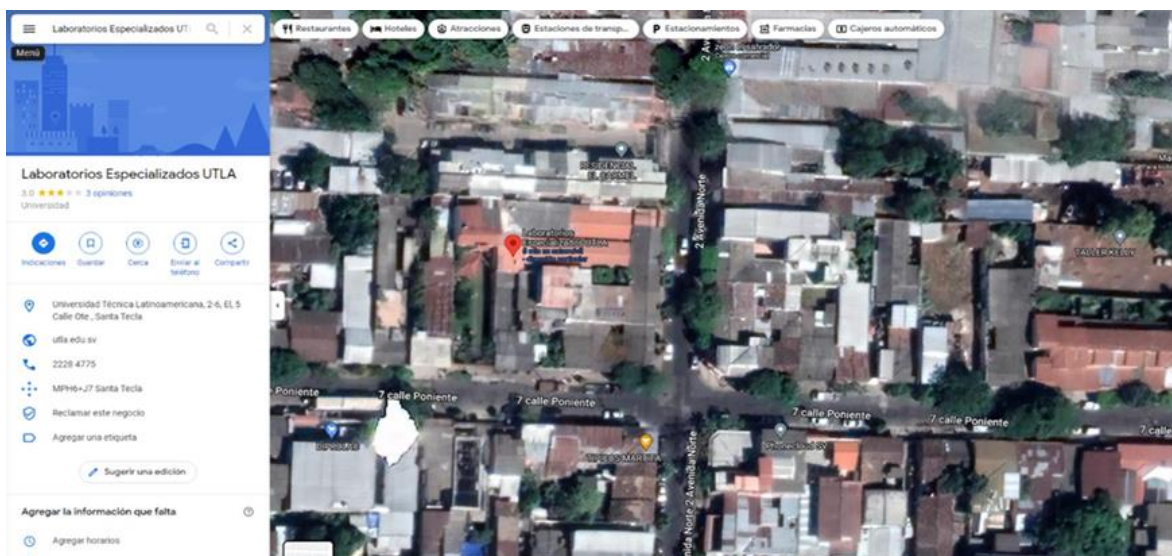


Figura 56 Ubicación geográfica Laboratorio Especializado

5.1.5. Diseño arquitectónico

En las figuras N°57 y 58 se muestran esquemas ilustrativos de la adecuación del área donde se instalará el equipo la cual tiene una superficie de 9 m², estará protegida con un acrílico que servirá como protección contra salpicaduras de agua y partículas de polvo. En anexo 1 se encuentra el diagrama de cableado UTP²².

²² UPT: Unshielded Twister Pair por sus siglas en ingles



Figura 57: Modelo arquitectónico de instalación

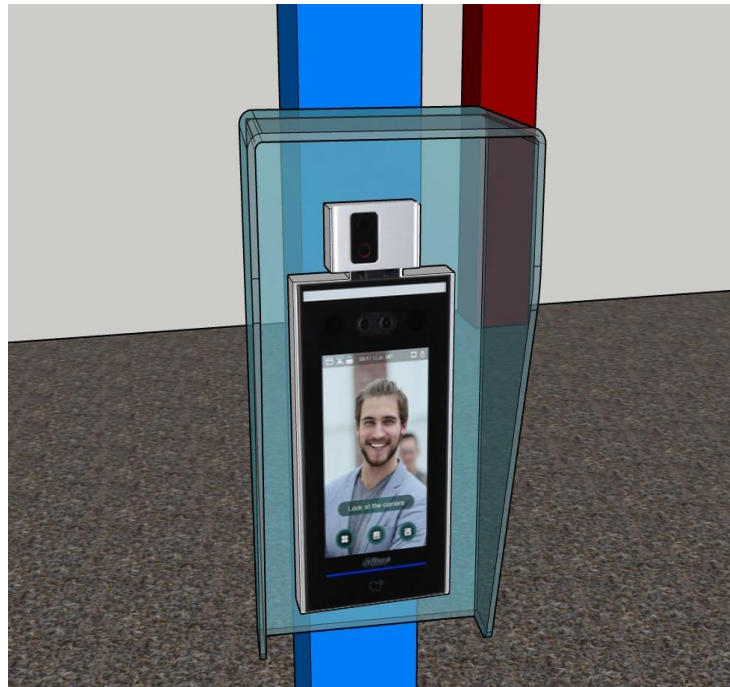


Figura 58: Diseño arquitectónico vista frontal

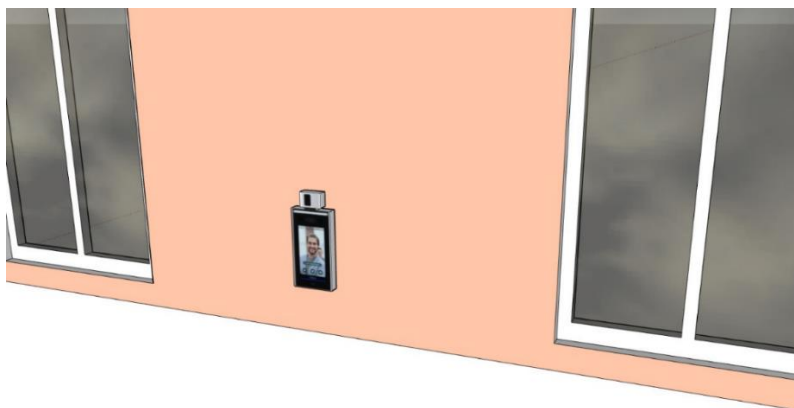


Figura 59: Diseño arquitectónico Laboratorio Especializado

5.1.5 Parametrización del sistema

Para el ingreso de la Universidad Técnica Latinoamericana y para el Laboratorio se ha determinado la configuración de parámetros detallada en la tabla N° 8 basada en la idea de mejorar el resultado del reconocimiento facial en función de la iluminación natural.

Tabla 8: Parametrización de los sistemas de control de accesos

Parámetros	Valor configurado	
	Campus universitario	Laboratorio especializado
Umbral de reconocimiento facial	20	85
Ángulo máximo de reconocimiento facial	90	90
Umbral de anti falsificación	Cerrar	Cerrar
Configuración del modo de luz de relleno	Auto	Auto
Luz Infrarroja	40	40
Se agotó el tiempo de espera (s)	3	3
Tiempo de intervalo de rostro invalido (s)	3	3
Distancia pupilar	45	45
ID del canal	1	1
Activar exposición del rostro	Activar	Activar

Brillo objetivo de rostro	50	50
Tiempo de detección del intervalo de exposición de rostro (s)	5	5
Monitoreo de temperatura	Activar	Activar
Unidad de temperatura	°C (Celsius)	°C (Celsius)
Área de detección	Activar	Activar
Distancia de monitoreo de TEMP (cm)	0	0
Umbral de temperatura	36.50	36.50
Valor de corrección de temperatura	0.00	0.00
Modo máscara	Interceptar máscara.	Interceptar máscara.

5.1.6 Configuración de IP en los controles de acceso

Para la comunicación del control de acceso DHI-ASI7213X-T1 y el software de administración SmartPSS-AC se estableció la siguiente configuración IP.

Se ingresó a la configuración del control de acceso como usuario administrador en la opción de conexión, configuración de red y seleccionamos la opción dirección IP, seleccionamos el puerto NIC 100MBPS, en la tabla N° 9 se detallan los parámetros de la configuración a implementar.

Tabla 9: Configuración IP de los controles de acceso

Parámetro	Valor Configurado	
	Campus Universitario	Laboratorio especializado
Dirección IP	192.168.1.22	192.168.1.21
Máscara Subred	255.255.255.0	255.255.255.0
Dirección IP Gateway	192.168.1.1	192.168.1.1
DHCP	Apagado	Apagado
P2P	Apagado	Apagado

5.1.7 Topología de instalación

En la figura 60 se describe la topología utilizada en la instalación en cada uno de las áreas, estos están de forma aislada ya que la Universidad Técnica Latinoamericana no cuenta con enlace de red entre el campus universitario y el laboratorio especializado.

En el caso de contar con el enlace de red ²³ el control de acceso DHI-ASI7213X-T1 se pudiesen administrar desde una sola computadora, mejorando la administración por ser centralizada para ambos equipos y unificando reportes de los registros que se obtendrían de cada uno de ellos, para este esta configuración se tiene que considerar un incremento en el costo del proyecto por adicionar el pago del servicio que se tiene que adquirí con un proveedor tercero para realizar el enlace, considerando que nuestro proyecto consta de solo dos equipo se tiene que evaluar el ventajas en costo veneficio, si considera un crecimiento en equipos a instalar en los dos ubicaciones tanto como el campus universitario y el laboratorio, el beneficio seria notable por que se pudiese tener una mejor supervisión en el funcionamiento, administración centralizada de los usuarios, unificación de reportes y la supervisión de alertas que pueden generar en el caso de detección de temperaturas altas y no portación de mascarillas.

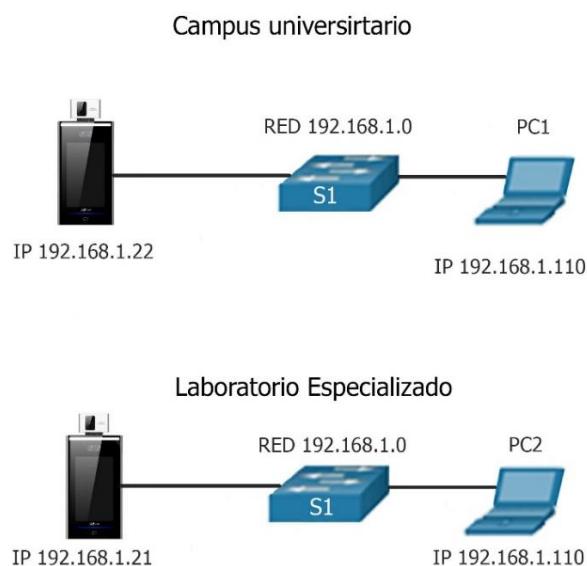


Figura 60 Topología

²³ Figura 60 Topología con enlace entre los dos sitios

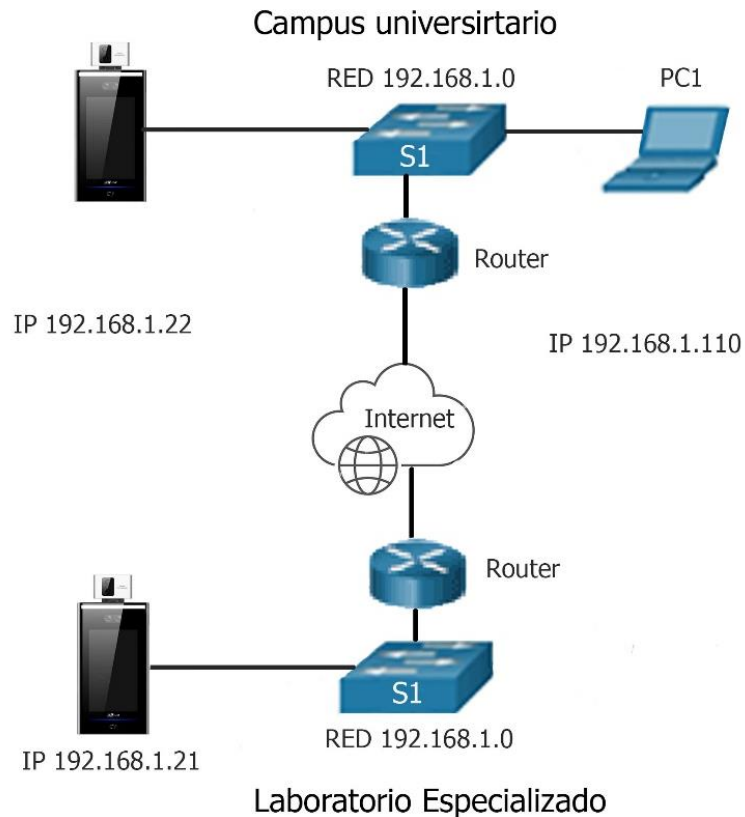


Figura 61 Topología con enlace entre los dos sitios

5.1.8. Inversión económica del proyecto

La inversión económica necesaria para la implementación del proyecto, se evaluaron en dos ejes fundamentales, el primero, la adquisición de los dos controles de acceso con capacidad de medición térmica y detección de mascarilla a instalar y la segunda en los materiales necesarios para la instalación de dichos equipos.

En la tabla No 10 se detalla el costo de cada uno de los elementos utilizados en la implementación del proyecto, valorando el monto total viable económicamente, considerando que la marca DAHUA ofrece mejores características técnicas y la integración de acceso y lectura de temperatura corporal.

Tabla 10: Listado de costo de equipos y materiales

Ítem	Descripción de materiales.	Cant.	Unidad	Precio unitario.	Precio total.
Control de Acceso					
1	Control de acceso ASI7213X1-T1	2	Unidad	\$1,400.00	\$2,800.00
Listado de materiales					
2	Cable UTP	60	Metros.	\$0.56	\$33.60
3	Tecno ducto	50	Metros.	\$0.80	\$40.00
4	Abrazadera para tecno-ducto	15	Unidad	\$0.13	\$1.95
5	Tornillos	65	Unidad	\$0.15	\$9.75
6	Resguardo de acrílico	1	Unidad	\$45.00	\$45.00
7	Toma hembra 110 VAC	2	Unidad	\$1.40	\$2.80
8	Conector macho para tecno ducto	4	Unidad	\$1.15	\$4.60
9	Caja rectangular	2	Unidad	\$1.10	\$2.20
10	Caja de conexiones.	2	Unidad	\$5.55	\$11.10
11	Canaleta plástica	1	Unidad	\$6.95	\$6.95
12	Conector UTP	4	Unidad	\$1.05	\$4.20
13	Servicios de instalación puntos de red	1	C/U	\$125.00	\$125.00
Total, materiales					\$287.15
Total del proyecto					\$3,087.15

5.2. Instalación de Software de administración del sistema (SmartPSS-AC)

Para la administración de controladores de acceso nuestra solución se complementa con el software SmartPSS-AC para el cual se describe el procedimiento de instalación en los siguientes apartados.

5.2.1. Requerimientos de sistema para instalación de software

Las especificaciones mínimas necesarias que debe tener la PC para una exitosa instalación del software de administración son las siguientes:

- Sistema operativo: Windows 7 / Windows 10.
- Procesador: Intel Core I3.
- Memoria RAM²⁴: 2 GB²⁵.
- Resolución: 1024x768 píxeles.

5.2.2. Instalación de Software SmartPSS-AC.

En el CD de instalación encontramos la carpeta nombrada SmartPSS-AC que contiene los instaladores del software de administración.

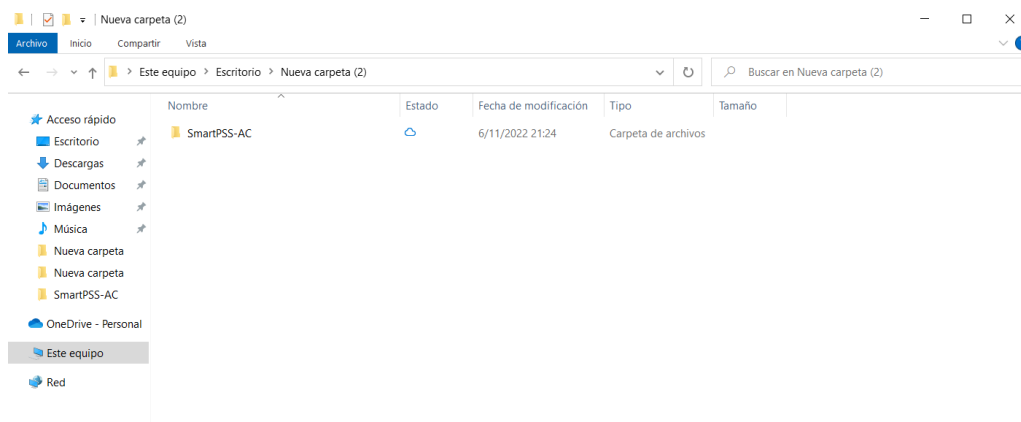


Figura 62: Carpeta de instalador del Software

Ingresamos a la Carpeta y ejecutamos el archivo en modo administrador **SmartPSSAC.exe**

²⁴ Random Access Memory ('memoria de acceso aleatorio')

²⁵ Gigabyte

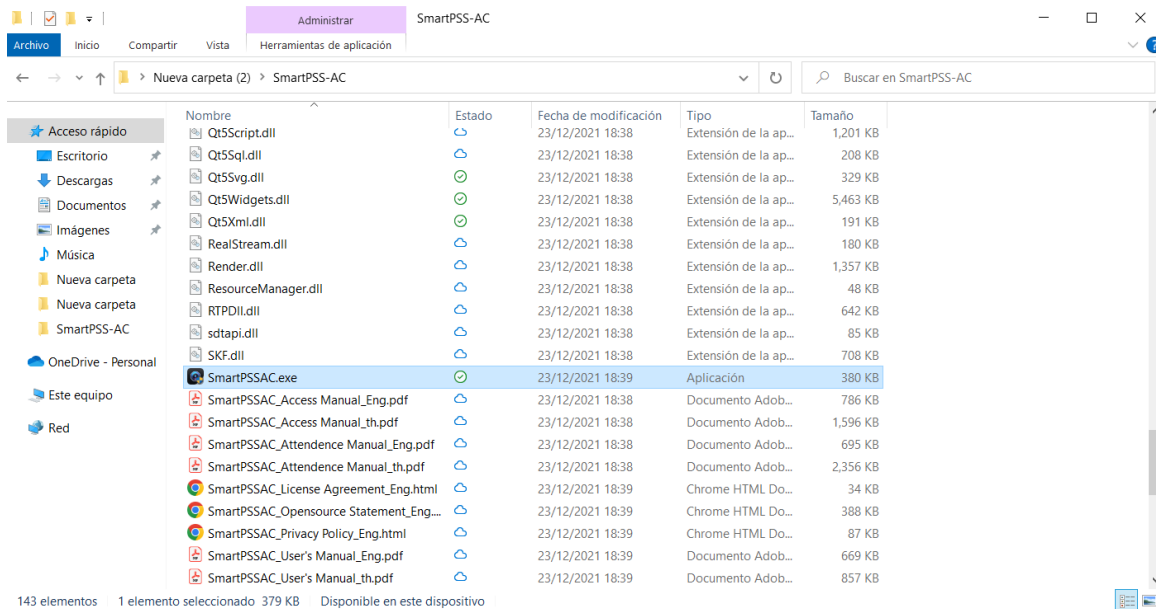


Figura 63: Ejecutable del Software SmartPSSAC.

Nos aparecerá el acuerdo de licencia y cliqueamos aceptar.



Figura 64: Acuerdo de Licencia

Establecemos la contraseña de administración con el que ingresamos al sistema

Inicialización

Configuración de contraseña Protección de contraseña

⚠ Por favor, establezca la contraseña de administrador en la primera instalación!

Contraseña

Seguridad de la c...

Confirmar

☒ Inicio de sesión auto. tras el registro

Siguiente Cancelar

Figura 65: Configuración de contraseña

Para la seguridad y la recuperación de la contraseña, el sistema nos sugiere ingresar tres preguntas claves como se muestra en la figura N° 66 y damos click en finalizar.

En la pantalla de inicio de sesión ingresamos las credenciales configuradas en los pasos anteriores con el usuario por defecto **“admin”**.

Inicialización

Configuración de contraseña Protección de contraseña

⚠ ¡Por favor, establezca preguntas de seguridad!

Pregunta 1

Responder

Pregunta 2

Responder

Pregunta 3

Responder

Finalizar

Figura 66: Preguntas de seguridad

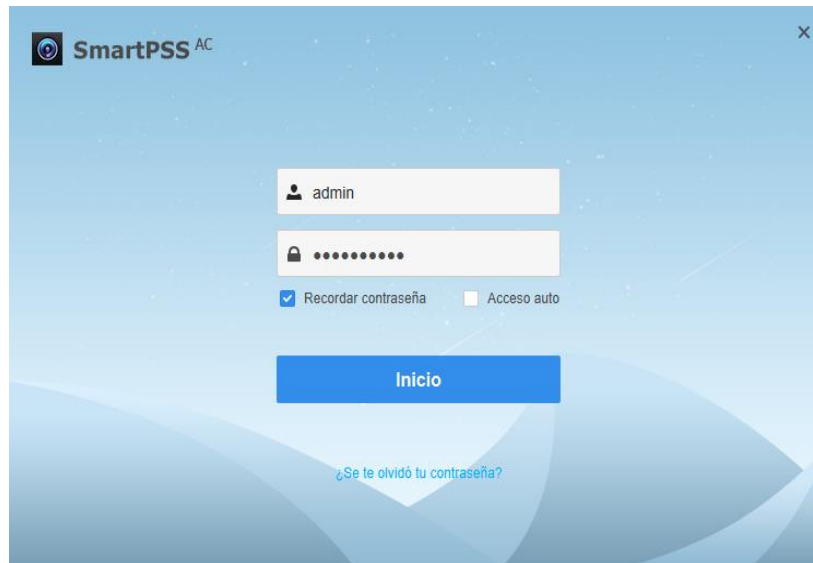


Figura 67: Pagina de acceso de credenciales Software SmartPSS

Nos aparecerá la pantalla de inicio siguiente:

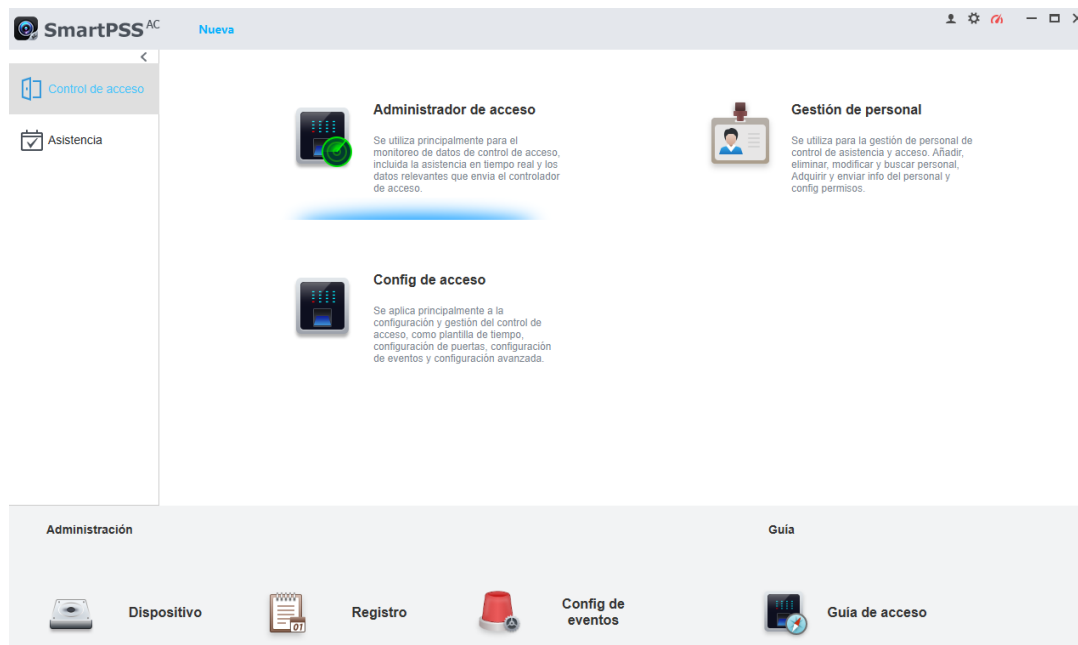


Figura 68: Página de Inicio del Software SmartPSS

5.3. Configuración de controles de acceso en el Software SmartPSS-AC.

Para la configuración y administración de los dos controles de accesos ya instalados se procede a la importación de los dos equipos al Software SmartPSS-AC

5.3.1 Agregar controles de acceso al software SmartPSS-AC

Para agregar el control de acceso ubicado en Universidad Técnica Latinoamericana, ingresamos al SmartPSS-AC y seleccionamos dispositivos

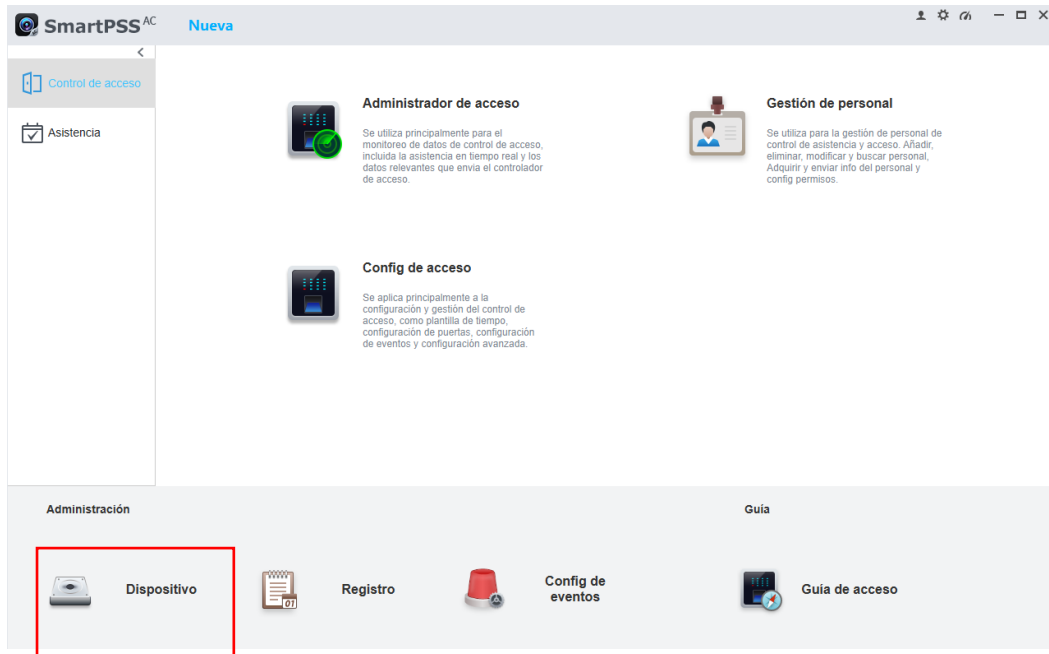


Figura 69: Acceso a configuración de dispositivos

Nos mostrará la lista de dispositivos disponibles

The screenshot shows the 'Dispositivo' configuration page in SmartPSS-AC. It includes a search bar, action buttons (Agregar, Borrar, Importar, Exportar), and a table of devices. The table has columns for Num., Nombre, IP, Tipo de dispositivo, Modelo dispos., Puerto, Número de cana, Estado en línea, SN, and Operación. There are 3 devices listed, with the first two being disconnected and the third being connected.

Num.	Nombre	IP	Tipo de dispositivo	Modelo dispos.	Puerto	Número de cana	Estado en línea	SN	Operación
1	192.168.1.108	192.168.1.108	N/A	N/A	37777	0/0/0/0	Desconecta...	N/A	[Edit] [Settings] [Refresh] [Delete]
2	192.168.2.27	192.168.1.27	N/A	N/A	37777	0/0/0/0	Desconecta...	N/A	[Edit] [Settings] [Refresh] [Delete]
3	UTLA	192.168.1.21	Acceso independie...	DHI-ASI7213X-T1	37777	2/0/2/2	Conectado	6E0A672RAJB369A	[Edit] [Settings] [Refresh] [Delete]

Figura 70: Lista de dispositivos

Seleccionamos Agregar y se nos mostrará una ventana al lado derecho donde podremos agregar cada uno de los dispositivos como se muestra en la siguiente imagen.

Agregar

Nombre Dispo:

* UTLA

Método para añadir:

IP

IP:

* 192.168.1.1.21

Puerto:

* 37777

Nombre Usuario:

* admin

Contraseña:

*

Figura 71: Configuración IP

En los campos usuario y contraseña se ingresarán las credenciales configuradas en la inicialización del equipo apartado 5.1.1.

SmartPSS ^{AC} Nueva Dispositivo									
Búsqueda a... + Agregar Borrar Importar Exportar Buscar Todos los disp.: 2 Disp. conectados: 1									
Todos los disp.									
☐ Num.	Nombre	IP	Tipo de dispositivo	Modelo dispos.	Puerto	Número de cana	Estado en línea	SN	Operación
☐ 1	Laboratorio	192.168.1.22	N/A	N/A	37777	N/A	Desconecta...	N/A	  
☐ 2	UTLA	192.168.1.21	Acceso independie...	DHI-ASI7213X-T1	37777	2/0/2/2	Conectado	6E0A672RAJB369A	  

Figura 72: Estado de dispositivos disponibles

5.3.2 Configuración de Hora

Para los controles de acceso la configuración de la hora se realiza de la siguiente forma:

Paso 1 Seleccione Administrador de dispositivos.

Paso 2 Haga clic en  desplegándose los controles de acceso disponibles, seleccionamos el equipo a configurar:

☐ Num.	Nombre	IP	Tipo de dispositivo	Modelo dispos.	Puerto	Número de cana	Estado en línea	SN	Operación
☒ 1	192.168.1.21	192.168.1.21	Acceso independie...	DHI-ASI7213X-T1	37777	2/0/2/2	Conectado	6E0A672RAJB369A	  

Figura 73: Configuración de equipo seleccionado

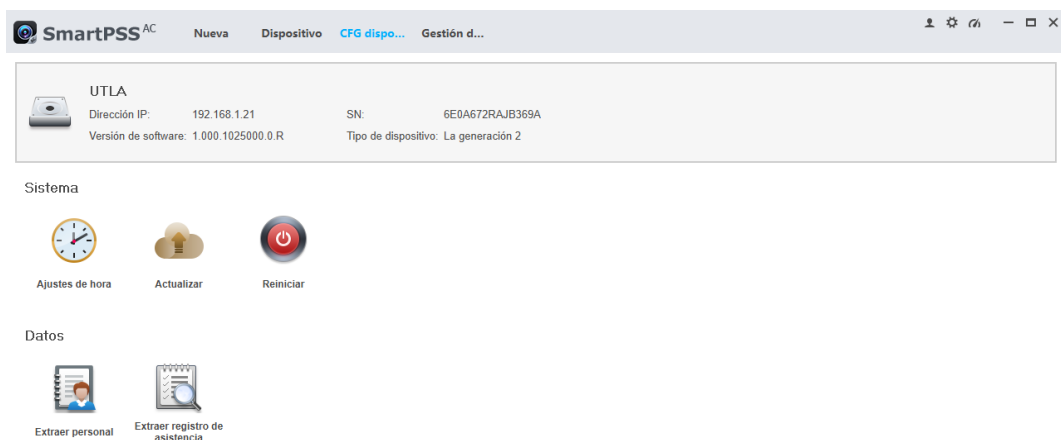


Figura 74: Ventana de configuración de dispositivo

Paso 3 Configure la hora del dispositivo.

The 'Ajustes de hora' dialog box contains the following settings:

- Formato de fecha: yyyy-MM-dd
- Formato de hora: 24-H
- Zona Horaria: GMT-06:00
- Hora del sistema: 2022-11-04, 07:59:16, with a 'PC Sync' button.
- ☐ Activar DST
 - Hora de inicio: Ene, La 1ª, Jueves, 00:00
 - Final: Ene, La 1ª, Viernes, 00:00
- ☐ NTP
 - Servidor NTP: clock.isc.org
 - Puerto: 123 (1-65535)
 - Período de actualización: 10 Minute(0-65535)

Buttons at the bottom: 'Guardar' (Save) and 'Cancelar' (Cancel).

Figura 75: Configuración de hora

Tabla 11: Descripción de parámetros hora

Parámetro	Descripción.
Formato de fecha.	Configure el formato de visualización de la fecha.
Formato de tiempo.	Configure el formato de visualización de la hora.
Zona horaria.	Establezca la zona horaria.
Hora del sistema	Configure la hora del sistema. También puede hacer click en sincronización PC para configurar la hora del sistema como la hora del PC.
DST	Habilite DST según sea necesario. Configure el tipo de horario de verano, la hora de inicio y la hora de finalización.
NT	Habilite el servidor NTP si necesita sincronizar la hora del sistema con la misma hora que la hora NTP. Ingrese la dirección del servidor, el puerto y el periodo de actualización.

5.3.3 Extraer usuarios

Para extraer los usuarios enrolados en el control de acceso hacia el software SmartPSS-AC se realizan los siguientes pasos:

Paso 1 seleccionamos Extraer personal

Datos

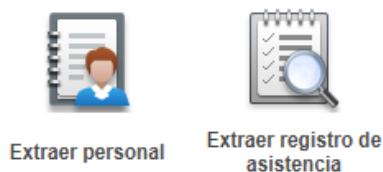


Figura 76: Iconos de extracción de reportes

Paso 2 Se nos mostrará la ventana donde estarán los usuarios disponibles, podremos hacer una extracción seleccionando el usuario y luego damos click en Extraer:

Extraer info. tarjeta

IP de dispositivo:UTLA

ID/Nombre/Tarjeta

☐	Num.	ID de usuario	Nombre	N° de tarjeta	Tipo persona	Departamento	Recuento de huellas
☐	1	1693	oscar mancia		General		0
☐	2	1234	Victor		General		0
☐	3	1232	nicolas		General		0

Extraer

Exportar

Cancelar

Figura 77: Ventana de extracción de Usuarios

5.3.4 Extraer Registros de asistencia.

Cuando un usuario se ha registrado en el sistema hace una marcación en el control de acceso, los registros son almacenados en él, para poderlos extraer y hacer el respectivo análisis, se realiza el siguiente procedimiento:

Paso 1 seleccionamos Extraer registro de asistencia

Paso 2 Configuramos el rango de fechas que deseamos extraer de las marcaciones y damos click en Extraer y Aplicar

Registro de extracción manual			
Tiempo de extracción... 2022/10/10 0:00:00 - 2022/11/10 23:59:59			
Hora	ID de trabajo	Nombre	Asistencia
2022-10-24 07:24:22	1693	oscar mancia	Desbloqueo por reconocimiento facial
2022-10-24 07:24:25	1693	oscar mancia	Desbloqueo por reconocimiento facial
2022-10-24 07:24:28	1693	oscar mancia	Desbloqueo por reconocimiento facial
2022-10-24 07:24:50	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:27:10	1232	nicolas	Desbloqueo por reconocimiento facial
2022-10-24 07:28:46	1232	nicolas	Desbloqueo por reconocimiento facial
2022-10-24 07:28:49	1232	nicolas	Desbloqueo por reconocimiento facial
2022-10-24 07:28:52	1232	nicolas	Desbloqueo por reconocimiento facial
2022-10-24 07:29:14	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:31:37	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:31:37	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:31:48	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:18	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:21	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:24	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:37	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:50	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:35:56	1234	Victor	Desbloqueo por reconocimiento facial
2022-10-24 07:36:17	1234	Victor	Desbloqueo por reconocimiento facial
Aplicar Extraer Cancelar			

Figura 78: Ventana de extracción de registros

5.3.5 Creación de Horarios.

El software SmartPSS-AC además de la administración de los controles de acceso también nos permite la creación y administración de horarios que la institución crea necesarios, los cuales pueden ser aplicados a cada uno de los usuarios existentes en el sistema.

5.3.5.1 Periodo de asistencia.

Seleccionamos en la ventana principal **“asistencia”**



Figura 79: Ventana de selección de asistencia

Seleccionamos periodo de asistencia en la primera sección el cual nos muestra la lista de periodos existentes, los cuales podemos seleccionar para editar o eliminar. En la sección dos, vemos todos los parámetros por los cuales podemos configurar un periodo de asistencia.

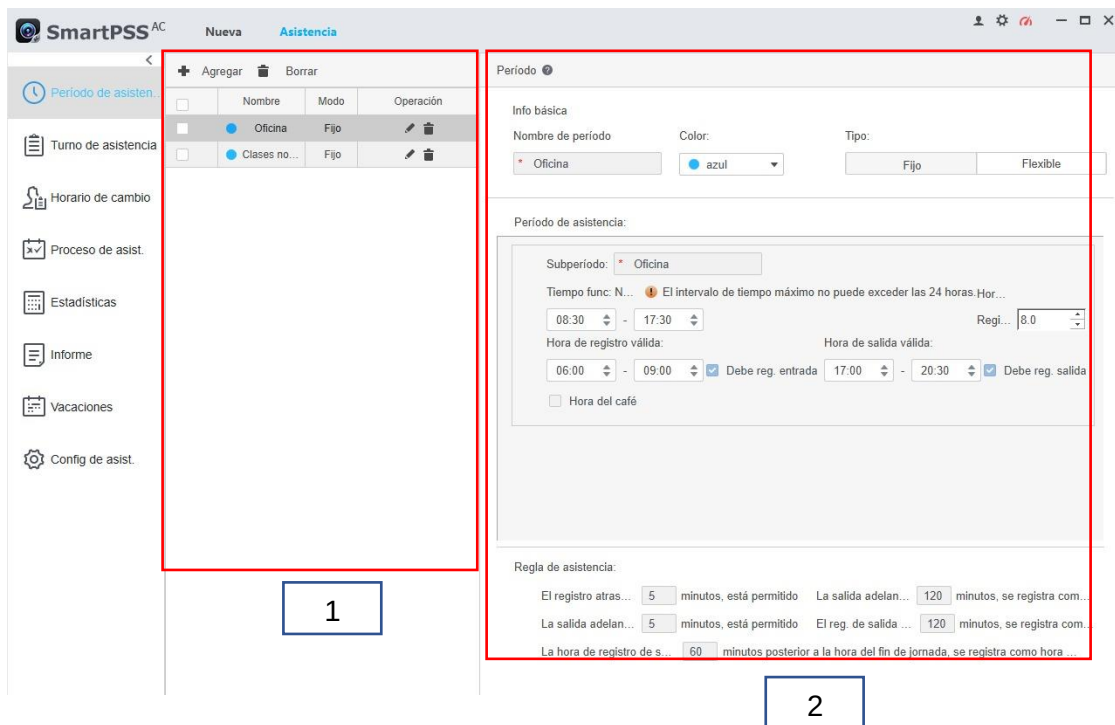


Figura 80: Periodos de asistencia.

5.3.5.2 Turno de asistencia.

Seleccionamos turno de asistencia en la primera sección, este nos muestra la lista de turnos existentes, los cuales podemos seleccionar para editar o eliminar. En la sección dos todos los parámetros por los cuales podemos configurar un turno de asistencia.

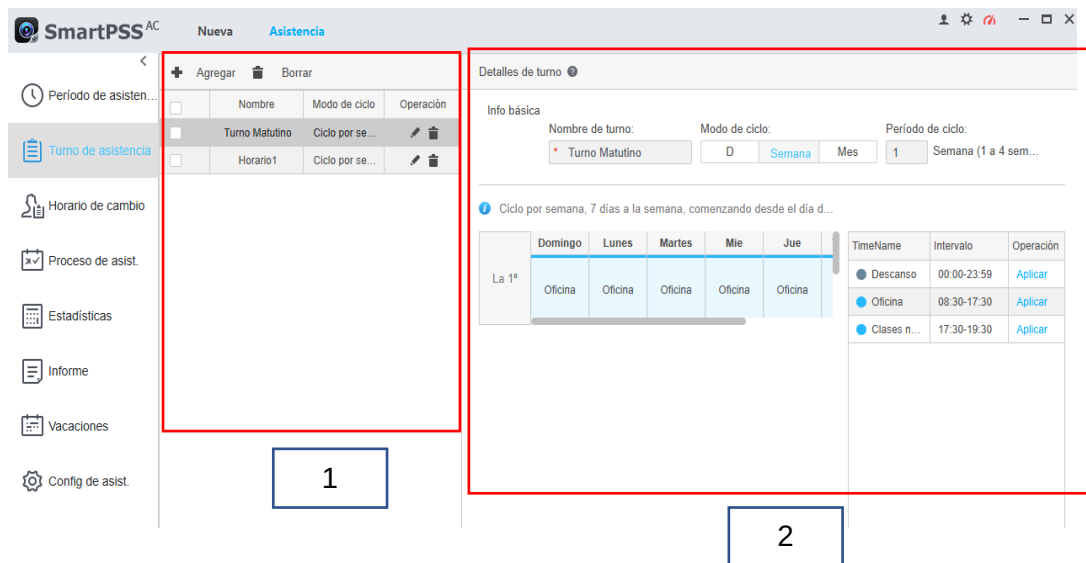
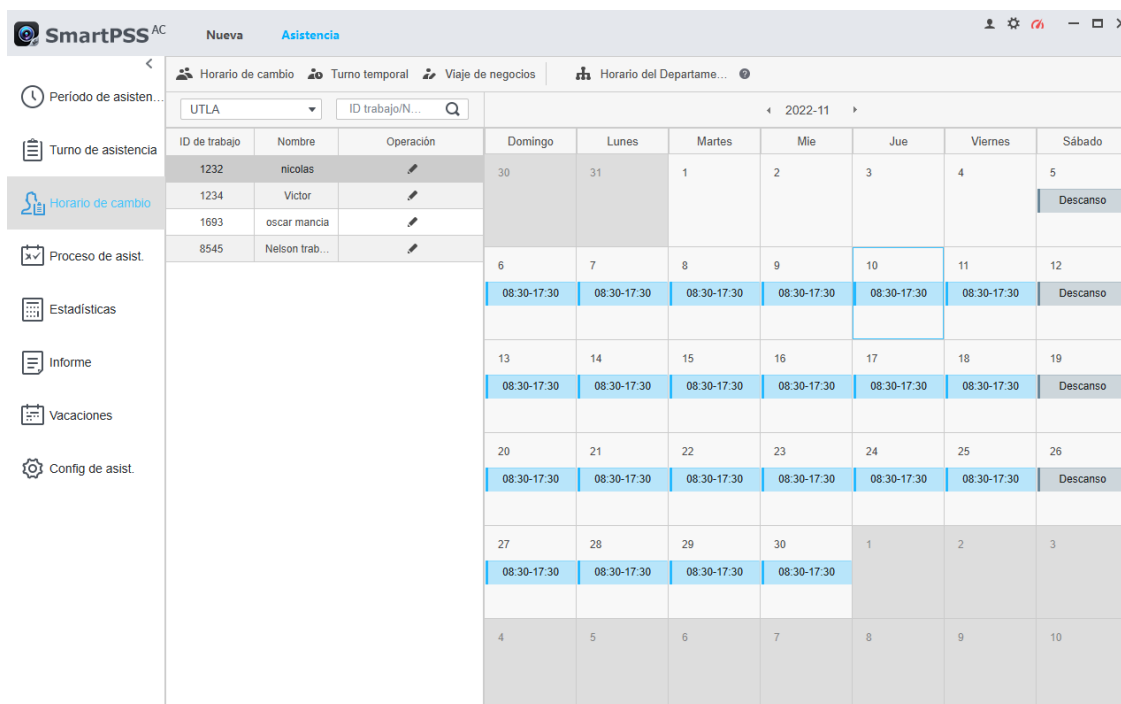


Figura 81: Turnos de asistencia

5.3.5.3 Horario de turno

Seleccionamos Horario de cambio, asignaremos a cada uno de los usuarios los turnos creados en el apartado anterior.



ID de trabajo	Nombre	Operación	Domingo	Lunes	Martes	Mie	Jue	Viernes	Sábado
1232	nicolas		30	31	1	2	3	4	5
1234	Victor								Descanso
1693	oscar mancia								
8545	Nelson trab...								

	Domingo	Lunes	Martes	Mie	Jue	Viernes	Sábado
6	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	Descanso
13	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	Descanso
20	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30	Descanso
27	08:30-17:30	08:30-17:30	08:30-17:30	08:30-17:30			
4							

Figura 82: Lista de horarios

5.3.6 Generación de reportes de asistencia.

Luego de tener los registros descargados y con horarios configurados, el software SmartPSS-AC nos permite la generación de reportes, como se muestra en la figura 83, en los formatos PDF, UVG, XLS.

Para ingresar los reportes damos click en informe. En los cuales encontramos las siguientes opciones.

- Registrar.
- Tabla de resumen diaria.
- Resumen por horas.
- Asistencia diaria.
- Asistencia flexible.
- Resumen mensual.

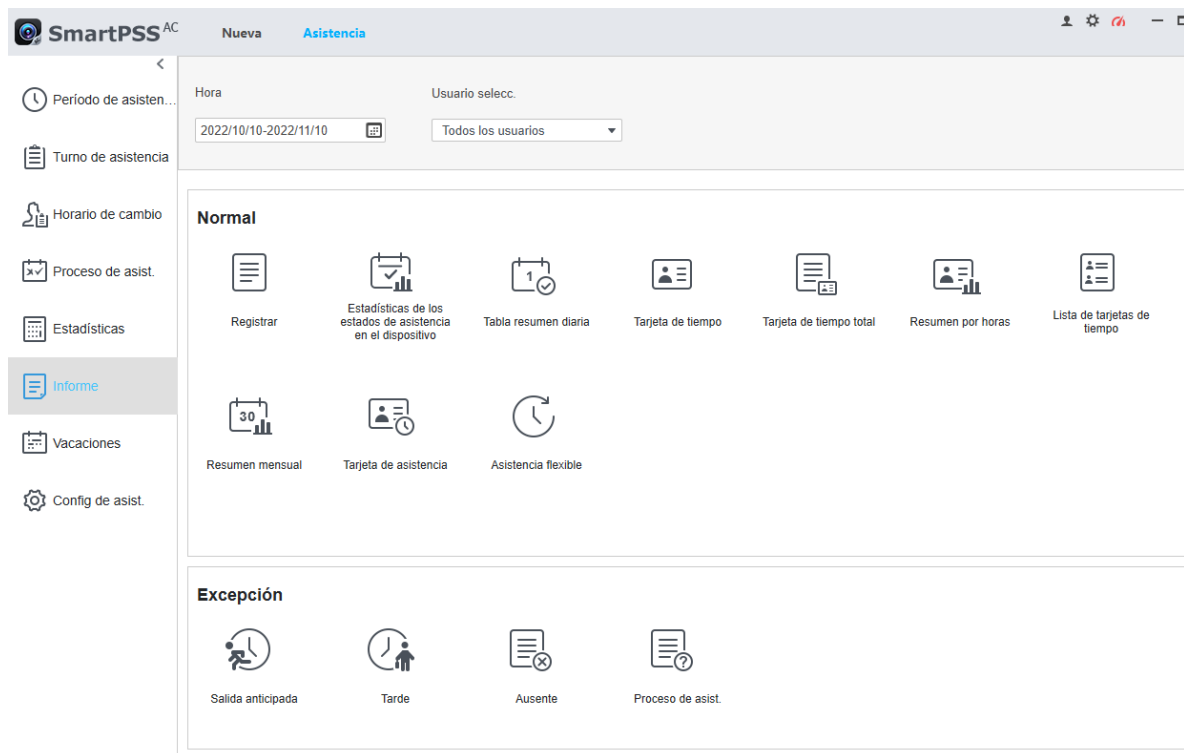


Figura 83: Ventana de informes

Conclusiones

- La solución implementada es operativa en las ubicaciones definidas en el campus de la UTLA tal cual se diseñó
- Con la configuración instalada, se alcanza una eficiencia de 93% de acuerdo a las pruebas de funcionamiento en el ingreso del campus universitario, por ser un espacio de luz no controlada y con una optimización de esta podríamos alcanzar hasta el 96%.
- La implementación de la solución, robustece la infraestructura del campus de la UTLA, de cara a una era digital.

Recomendaciones

- Una de las mejoras que se podrían lograr en el sistema implementado es unificar la administración de los controles de acceso mediante el software, por lo que se recomienda adquirir servicios de conectividad de un proveedor de conveniencia para alcanzar la conectividad entre las dos localidades.
- Explotar las bondades ofrecidas por el sistema instalado expandiendo su uso al personal administrativo generando la reportaría asociada.
- Definir y dar continuidad a un programa de mantenimiento preventivo semestral de los equipos, con énfasis en los lentes de las cámaras operativas.

Bibliografía

- Atico34, G. (2010). <https://protecciondatos.com/empresas/control-de-acceso/>. Obtenido de <https://protecciondatos.com/empresas/control-de-acceso/>
- <https://www.ecured.cu/>. (28 de Abril de 2014). Obtenido de https://www.ecured.cu/Ley_de_Wien
- Kaspersky, E. (1997). *Karpesky*. Obtenido de <https://latam.kaspersky.com/resource-center/definitions/what-is-facial-recognition>
- Lacort, J. (15 de Agosto de 2017). <https://www.xataka.com/>. Obtenido de <https://www.xataka.com/seguridad/las-claves-de-los-sistemas-de-reconocimiento-facial-cual-es-su-verdadero-nivel-de-seguridad>
- Regulatorias), R. (. (20 de Agosto de 2022). *Electronic Identification*. Obtenido de <https://www.electronicid.eu/es/blog/post/como-funciona-reconocimiento-facial/es>
- S.L., B. S. (Diciembre de 2020). <https://www.bizneo.com/>. Obtenido de <https://www.bizneo.com/blog/control-de-acceso-biometrico/#:~:text=El%20control%20de%20acceso%20biom%C3%A9trico%20es%20un%20sistema%20de%20identificaci%C3%B3n,jornada%20laboral%20de%20los%20trabajadores>
- Salud, O. M. (2019). <https://www.who.int/es>. Obtenido de [https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it](https://www.who.int/es/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it)
- Social, I. S. (2021). *Guía cuadro clinico del COVID 19 en adultos, embarazadas y niños*.
- Superior, C. d. (2020). *Protocolo de seguridad sanitaria y contención de COVID-19 de las Instituciones de Educación Superior para una apertura gradual de actividades*.
- Techlogy, d. (s.f.). <https://www.dahuasecurity.com/>. Obtenido de [https://www.dahuasecurity.com/products/All-Products/Dedicated-Products/Project-Exclusive/Access-Control/ASI7213X-T1\(only-for-project\)](https://www.dahuasecurity.com/products/All-Products/Dedicated-Products/Project-Exclusive/Access-Control/ASI7213X-T1(only-for-project))
- Technologies, E. (s.f.). <https://excemtech.com/>. Obtenido de <https://excemtech.com/control-de-accesos-en-la-era-post-covid-19/>
- Vázquez., E. R. (s.f.). Obtenido de <https://kime25.tripod.com/avance.htm>
- Vázquez., E. R. (2006). *El Protocolo de investigacion* . Obtenido de <https://kime25.tripod.com/avance.htm>
- www.tecnoseguro.com. (2021). <https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso>. Obtenido de <https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso>

Anexos

Anexo 1 Sensor infrarrojo y cable UTP

Sensor infrarrojo

Para introducirnos en el tema de sensores infrarrojos debemos iniciar por conocer conceptos importantes tales como:

La radiación electromagnética es la combinación de ondas eléctricas y magnéticas oscilantes, que se propagan a través del espacio transportando energía. Es importante definir cada uno de los elementos que la componen uno de ellos su longitud denominada λ (lambda) y que a su vez esta determina su frecuencia, otro componente importante es su amplitud que corresponderá a la energía.

λ (lambda): se define como la distancia entre dos crestas consecutivas.

La frecuencia es la cantidad de ciclos que completa una onda en un segundo, se mide en Hertz [Hz] y se calcula con la siguiente fórmula: $f = 1 / T$ donde T es el periodo, esto es el tiempo que le toma a la onda en completar un ciclo.

Amplitud: Es la distancia entre el punto más alejado de una onda y el punto de equilibrio o medio.

Teniendo en cuenta las definiciones anteriores y sobre todo la fórmula de la frecuencia que a mayor frecuencia, menor es su longitud de onda correspondiente. Esto nos ayuda a comprender el espectro electromagnético iniciando desde las ondas de radio, como las que emiten las estaciones de radio y cuya longitud de onda es muy grande, por ejemplo, el rango de frecuencia portadora la radio AM que inicia de 535-1605 kHz

$$\text{Longitud de onda } (\lambda) = \frac{\text{Velocidad de propagación}}{\text{Frecuencia de la Onda}} = \frac{3 \times 10^8 \text{ m/s}}{\text{Hz}} = m$$

Para comprender mejor podemos hacer el siguiente ejemplo calcular la longitud de onda para la frecuencia de 535 KHz que es el rango de frecuencia menor en AM

$$\lambda = \frac{3 \times 10^8 \text{ m/s}}{535 \times 10^3 \text{ Hz}} = 560.7476 \text{ m}$$

Continuando con el espectro electromagnético encontramos las señales microondas donde se involucran las señales de telecomunicaciones celular y en los hornos microondas cuya longitud de onda inicia desde un 1m hasta 1mm y frecuencia de 3-30 GHz.

En seguida de las microondas se encuentra la radiación infrarroja que utilizamos en los controles remotos para aparatos electrónicos y en nuestro caso para la medición de temperatura que tienen una longitud que abarca desde los 700nm hasta 1mm, si aplicamos la fórmula de longitud de onda para obtener la frecuencia se calcularía de la siguiente manera:

$$\text{Frecuencia de la Onda} = \frac{\text{Velocidad de propagación}}{\text{Longitud de onda } (\lambda)}$$

$$F = \frac{3 \times 10^8 \text{ m/s}}{700 \times 10^{-9} \text{ m}} = 4.2857 \times 10^{14} \text{ Hz}$$

A continuación, en el espectro se aprecia el intervalo que corresponde a la luz visible, ya que es la única que perciben nuestros ojos, en la que se observan los colores de los arcoíris ordenados de mayor a menor longitud de onda: rojo (cuya longitud de onda es aproximadamente 700 nm), naranja (650 nm), amarillo (600 nm), verde (570 nm), azul (450 nm) y violeta (400 nm). La luz blanca es la combinación de todos estos colores superpuestos y se les puede observar al hacer pasar esta radiación por un prisma.

Un detalle importante es que toda la radiación electromagnética, independientemente de la frecuencia, longitud de onda o energía que contiene, viaja a la misma velocidad. Esto es, a la velocidad de la luz, que en el vacío es equivalente a $3 \times 10^8 \text{ m/s}$.

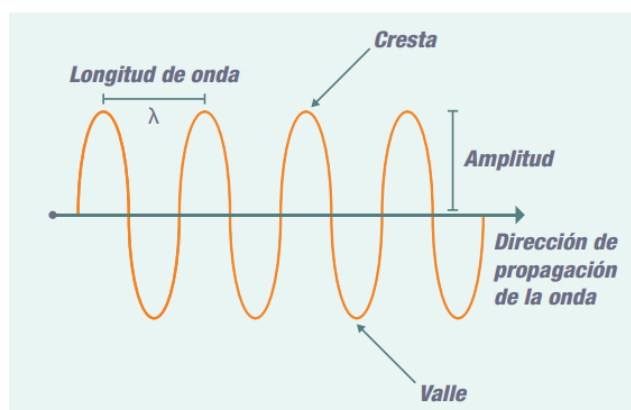


Figura 84 Onda senoidal

Aplicando la teoría en la electrónica utilizando para ello los diodos infrarrojos emisor y receptor, comprenderemos mejor el funcionamiento de una cámara termográfica.

Diodo Emisor:

Este led emite en el espectro electromagnético de la luz infrarroja que en nuestra aplicación es utilizado como la fuente de calor hacia el cuerpo a medir



Figura 85 Sensor infrarrojo emisor

Fototransistor:

Este dispositivo se diferencia de un transistor común porque su base ha sido sustituida por un cristal fotosensible que regula el flujo de corriente colector – emisor de acuerdo a la luz incidente sobre él (en nuestro caso luz infrarroja). Que sería el sensor responsable recibir la información de la emisividad del cuerpo y lo que lo convertirá a un valor digital.



Figura 86 Sensor infrarrojo emisor

Un esquema básico y que nos ayudara a comprender electrónicamente su funcionamiento entre el sensor emisor y receptor se detalla en la figura siguiente:

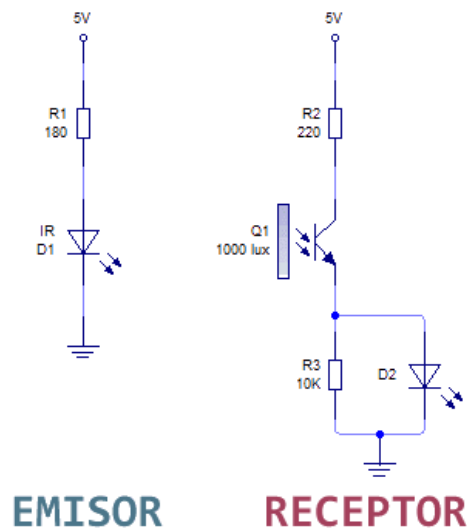


Figura 87 Circuito electrónico

Tomando en cuenta este ejemplo Una cámara infrarroja contiene un sistema óptico que enfoca la energía infrarroja en un detector especial (conjunto del sensor) que contiene miles de píxeles organizados en una cuadrícula.

Cada píxel del conjunto del sensor reacciona a la energía infrarroja concentrada en él y produce una señal electrónica. El procesador de la cámara toma la señal de cada píxel y utiliza un cálculo matemático para crear un mapa de color de la temperatura aparente del objeto. Cumpliendo así la toma de temperatura para ser procesada y mostrada en pantalla.

Cable utilizado para la comunicación de dispositivos con PC

El cable que se instaló para la implementación de nuestro proyecto es el UTP, que en sus siglas en ingles significa Unshielded Twisted Pair (lo que puede traducirse como “Par trenzado no blindado”). El cable UTP, por lo tanto, es una clase de cable que no se encuentra blindado y que suele emplearse en las telecomunicaciones.

Cuya categoría de UTP utilizado es la 5e, que es un tipo de cable que puede transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 MHz Que es la velocidad utilizada por el equipo Dahua ASI7213X-T1 del puerto IPv4 utilizado.

Anexo 2: Plano de instalación

Campus Universitario

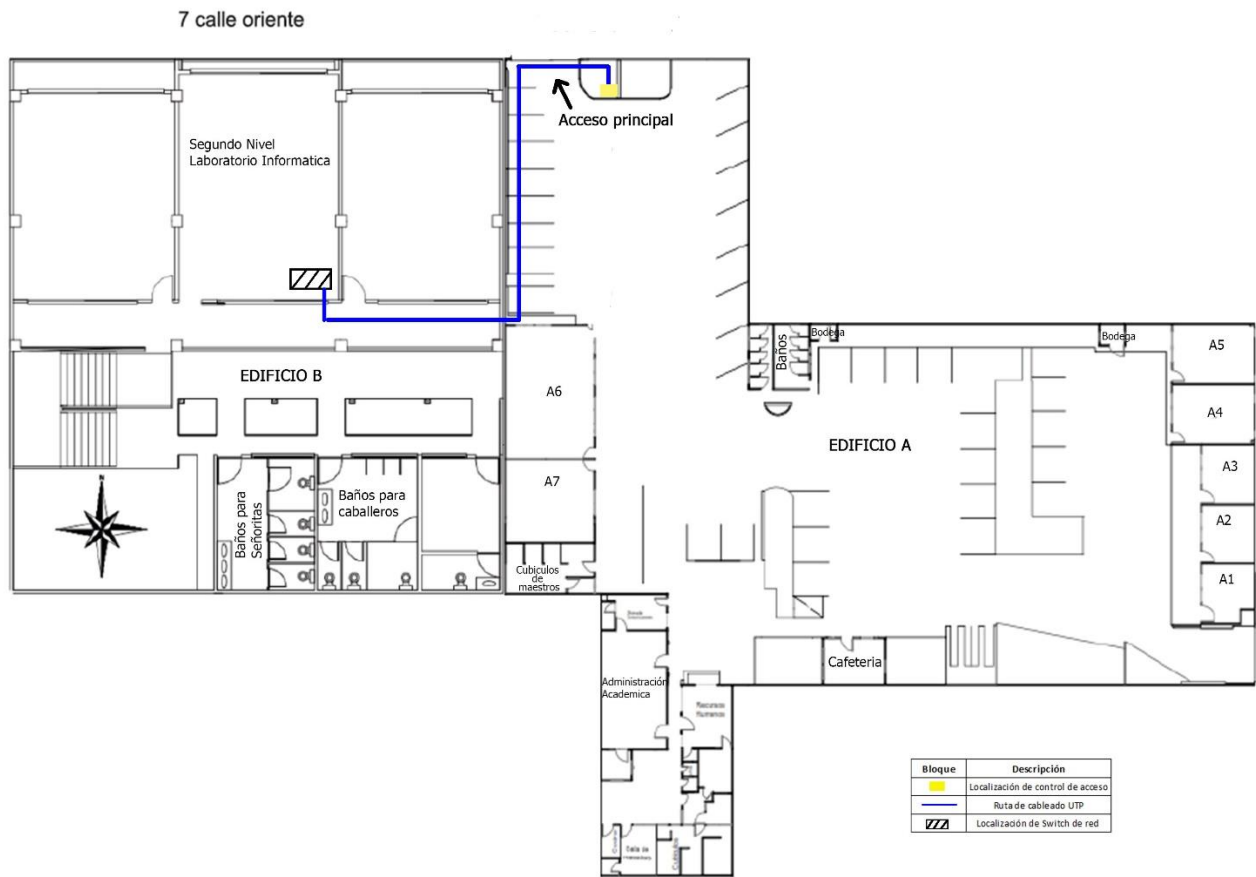


Figura 88 Plano de instalación de red Campus Universitario

Laboratorio Especializado

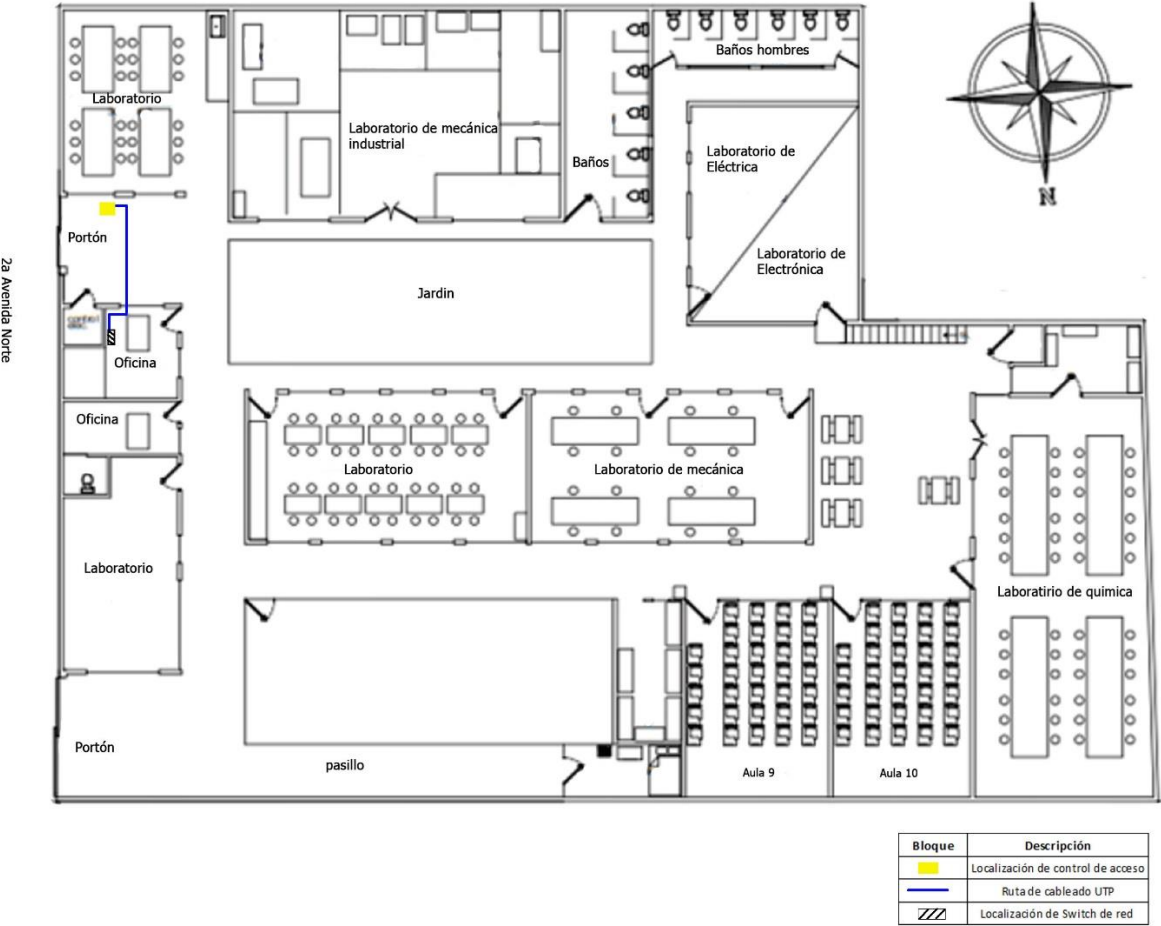


Figura 89 Plano de instalación de red Laboratorio Especializado

Anexo 3: Pruebas efectuadas en los ingresos de las instalaciones

Ingreso principal del campus Universitario:



Figura 90 Pruebas iniciales de ubicación del control de acceso



Figura 91 Imagen Izquierda Instalación y conexión de control de acceso, imagen derecha ubicación sugerida para la toma de temperatura.



Figura 92 Pruebas de enrolamiento con personal de la Universidad

Ingreso principal del Laboratorio Especializado:



Figura 93 Ubicación de instalación en el ingreso de Laboratorio Especializado



Ilustración 2: Pruebas de funcionamiento del control de acceso.

Anexo 2: Ficha técnica

Serie ASI7 | DHI-ASI7213X-T1



DHI-ASI7213X-T1

Control de acceso por reconocimiento facial y medición de temperatura corporal



Especificaciones técnicas

Sistema

Procesador principal	Procesador incorporado
Protocolo de internet	IPv4, RTSP, RTP, TCP, UDP, P2P
Protocolo de OSDP	Sí
Interoperabilidad	ONVIF, CGI
SDK y API	Compatibilidad con SDK

Concepción Básica

Pantalla	Pantalla de 7 pulgadas
Tipo de pantalla	Pantalla capacitiva
Resolución	600(H)×1024(V)
Cámara	Cámara dual WDR de alta definición CMOS de 1/2.8" y 2 MP
WDR	120 dB
Compensación de luz	Luz blanca automática Luz IR automática
Indicador de estado	1 luz indicadora. Rojo: Error; Verde: Normal; Azul: En funcionamiento
Mensaje de voz	Sí
Material de la carcasa	Aleación de aluminio / vidrio templado / PC

- Pantalla curva 2,5 D.
- Pantalla LCD de 7 pulgadas con resolución de 1024 × 600.
- Sensor CMOS de 2 MP, WDR.
- La luz de llenado automático reduce la contaminación lumínica.
- Puede contener 100,000 usuarios, 100,000 imágenes faciales, 100,000 tarjetas, 100,000 contraseñas, 50 administradores y 300.000 registros.
- Compatible con rostros, tarjeta IC, desbloqueo de contraseña y desbloqueo por medio de sus combinaciones.
- Con tecnología de detección facial; el target con el rostro más grande que aparecen al mismo tiempo se reconoce primero; el tamaño máximo del rostro se puede configurar en la interfaz web.
- Distancia entre la cámara y el rostro: 0,3 m – 2,0 m; altura de las personas: 0,9 m – 2,4 m (distancia entre el lente y el suelo: 1,4 m).
- Con el algoritmo de reconocimiento facial, el controlador de accesos puede reconocer más de 360 posiciones en el rostro humano.
- Velocidad de reconocimiento facial: 0,2 s por rostro.
- Permite detección de vida en rostros humanos.
- Reconocimiento preciso en luz de fondo y luz frontal
- Varios modos de visualización del estado de desbloqueo protegen la privacidad del usuario.
- Admite activar/desactivar el modo de monitoreo de temperatura; el rango de monitoreo de temperatura es de 30 °C a 50 °C; el rango de distancia de monitoreo de temperatura es 0,3 m – 1,8 m; el error de monitoreo de temperatura es $\pm 0,5$ °C; informa alarma de anomalía de temperatura.
- Presenta detección de máscaras, informa alarma de eventos anormales sin usar una máscara.
- Presenta alarma de coacción, alarma de tamper, alarma de intrusión, alarma de tiempo de espera de contacto de puerta y alarma de tarjeta ilegal.
- Admite usuarios generales, usuarios de patrullaje, usuarios VIP, usuarios invitados y usuarios especiales.

Función

Modo de desbloqueo	Desbloqueo de tarjeta / remoto / de contraseña / facial y desbloqueo por medio de sus combinaciones; Desbloqueo facial en modo de monitoreo de temperatura
Tipo de lector de tarjetas	Tarjeta IC
Lista de periodos	128
Periodo de días festivos	128
Desbloqueo de primera tarjeta	Sí
Verificación remota	Sí

Lector de tarjetas periféricas	1 RS-485, 1 Wiegand
Múltiples autenticaciones	Sí
Vigilancia en tiempo real	Sí
Configuración por internet	Sí

Monitoreo de temperatura

Resolución IR	120°*90
Ángulo visual de monitoreo de temperatura	50°
Rango de monitoreo de temperatura	30° C a 50° C
Tiempo de monitoreo de temperatura	0,2 s
Precisión de monitoreo de temperatura	0,1°C
Error de monitoreo de temperatura	± 0,5 °C, sin calibración de blackbody
Distancia de monitoreo de temperatura	30 cm ~ 180 cm
Altura de monitoreo de temperatura	140 cm ~ 185 cm (cuando la distancia de monitoreo de temperatura es de 50 cm) 135 cm ~ 200 cm (cuando la distancia de monitoreo de temperatura es de 120 cm)

Capacidad

Capacidad de usuario	100, 000
Capacidad de imágenes faciales	100, 000
Capacidad de la tarjeta	100, 000
Capacidad de contraseña	100, 000
Capacidad de grabación	300.000 grabaciones

Entrada

RS-485	1
RS-232	1
Wiegand	1 (entrada o salida)
USB	2 entradas USB 2.0
Ethernet	1 entrada Ethernet 1000 M 1 entrada Ethernet 10 M / 100 M
Entrada de alarma	2 (cantidad de interruptores)
Salida de alarma	2 (Relé)
Vinculación de alarma	Sí
Botón de salida	1
Detección de estado de entrada	1
Control de bloqueo	1

Alarma

Anti-passback	Sí
Sabotaje	Sí
Coacción	Sí
Tiempo de espera del sensor de puerta	Sí

Intrusión	Sí
Tarjeta ilegal que excede el umbral	Sí

General

Fuente de alimentación	Proporcionada
Modo de fuente de alimentación	CC 12V 2A
Consumo de energía	≤24W
Dimensiones del producto	312,5 mm × 129,0 mm × 36,7 mm
Dimensiones del paquete	Embalaje del controlador: 380 mm × 235 mm × 124 mm Estuche protector: 494 mm × 402 mm × 275 mm
Temperatura de funcionamiento	Modo de monitoreo de temperatura inhabilitado: -10°C a +55 °C Modo de monitoreo de temperatura habilitado: +15°C a +32°C
Humedad de funcionamiento	0% HR ~ 90% HR (sin condensación)
Ambiente de funcionamiento	Interiores
Peso bruto	2,2 kg
Instalación	Montaje en pared
Certificaciones	CE/FCC

Información para hacer pedidos

Tipo	Modelo	Descripción
Controlador de accesos por reconocimiento facial (ambientes internos; monitoreo de temperatura)	DHI-ASI7213X-T1	Controlador de accesos por reconocimiento facial de 7 pulgadas (ambientes internos; monitoreo de temperatura)

Dimensiones (mm [pulgadas])

