Fecha de elaboración: 07.04.2023 [del RAI]			
Tipo de documento	TID: X	Obra Creación:	Proyecto Investigación:
Título	Diseño de un control de acceso peatonal para el ingreso a las instalaciones de la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección en Bogotá -sede Américas		
Autor(es)	**Jhon Freddy Quitian, José Gabriel Ramirez, Edgar Daniel Soto**		
Tutor(es)	**Juan Carlos Guzmán**		
Fecha de finalización	10.04.2023		
Temática	**Sistema de acceso**		
Tipo de investigación	**Cualitativa**		

Resumen

La presente investigación está enfocada en la manera como se controla el acceso de las personas a las instalaciones de la Subdirección Especializada de Seguridad y Protección (SEPS) adscrita a la Unidad Nacional de Protección (UNP).
Este proyecto, se lleva a cabo después de analizar el control de acceso a las instalaciones, donde se identifican que se presentan falencias y dificultades a la hora de llevar un control eficiente con la identificación de las personas que ingresan a las instalaciones, debido a que no tienen herramientas para verificar la información que presenta la persona que va ingresar, es por esto que se hace necesario realizar un diseño de control de acceso peatonal reforzando la seguridad en el ingreso con el fin de garantizar que las personas que ingresan a las instalaciones estén plenamente identificas, con el fin de proteger la información que se encuentra en el edificio.

Palabras clave

SEPS: Subdirección Especializada de Seguridad y Protección; UNP: Unidad Nacional de Protección; Control de acceso; Software de administración; Biométricos; Enrolamiento; Torniquetes; Seguridad; Controlador.

Planteamiento del problema

Se visualiza que el acceso a la Subdirección especializada de Seguridad y Protección (SESP), se realiza un control de ingreso de marera precaria ya que no cuenta con las tecnologías y procedimientos necesarios para cumplir de manera responsable con las actividades necesarias para salvaguardar la integridad de los funcionarios e instalaciones.

En el presente en la SESP el control de acceso peatonal es realizado de forma visual. En la puerta de ingreso a las instalaciones está asignado un guarda de seguridad que está

pendiente de todas las personas que ingresan a la institución. Como el flujo es constante y elevado en algunas horas, la labor de identificación es dispendiosa y se torna ineficiente ya que el control depende de las habilidades y antigüedad del funcionario, por esta razón para un vigilante que lleve tiempo en este mismo puesto es más fácil identificar el personal administrativo, sin embargo, se dificulta para las personas que van a realizar alguna solicitud y se debe solicitar un medio de identificación para permitirles el ingreso.

Por lo mencionado anterior, desde la creación de la Subdirección Especializada de Seguridad y Protección en el 2017, no se tiene un registro histórico del personal que ha ingresado a las instalaciones ya sean funcionarios o personal externo, por tal razón ante algún evento que se presentara en las instalaciones no se podría identificar oportunamente que personas estaban en las instalaciones, convirtiéndose en una situación muy delicada ya que en las instalaciones se maneja información delicada la cual debe ser salvaguardada con medidas se seguridad más rigurosas ya que actualmente el registro de personal e ingreso de los objetos electrónicos se realiza de forma manual (bitácora de registro), este proceso no es el más seguro para guardar información ya que la minutas pueden ser extraviadas o dañadas fácilmente.

Pregunta

¿Como realizar un control de acceso peatonal para el ingreso a las instalaciones de la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección en Bogotá -sede Américas?

Objetivos

Objetivo general

Elaborar un diseño de control de acceso peatonal para el ingreso a las instalaciones de la Subdirección Especializada de Seguridad y Protección adscrita a la Unidad Nacional de Protección en Bogotá sede Américas.

Objetivos específicos

- Identificar las falencias del control de acceso peatonal que se tiene en la actualidad por medio de unas encuestas realizadas al personal que ingresa a las instalaciones tanto visitantes como los trabajadores.
- Definir la mejor solución del control de acceso peatonal a las instalaciones de la Subdirección de Seguridad y Protección (SESP), adscrita a la Unidad Nacional de Protección (UNP), sede Américas.
- Realizar un instructivo de procedimientos de acuerdo con el control de acceso peatonal propuesto para el ingreso a las instalaciones.

Marco teórico

Resuma únicamente los principales referentes teóricos o artísticos que siguió su trabajo. Señale los números de las páginas de su documento en los que se encuentra la información completa.

control de acceso es un sistema que impide que una persona entre en un lugar sin identificación previa de algún tipo. Ya sea la huella dactilar o un dispositivo electrónico, es necesario identificarse antes de entrar. Pag 10

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Pag 10 – 21

Bases teóricas de la Unidad Nacional de Protección. Pag 23 - 26

Método

Resuma únicamente los principales elementos metodológicos que empleó en su investigación. Señale los números de las páginas de su documento en los que se encuentra la información completa.

El enfoque de la investigación a realizar en el presente proyecto es la cualitativa ya que se utilizarán instrumentos de recolección de información apropiados como entrevistas y visitas al entorno para el desarrollo de la investigación.

Enfoque Cualitativo: Los autores Blasco y Pérez (2007:25), señalan que la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas.

Una vez utiliza esta variedad de instrumentos, para recoger información como las entrevistas, imágenes, observaciones, historias de vida, en los que se describen las rutinas y las situaciones problemáticas, así como los significados en la vida de los participantes. (Eumed.net, 2022) Pag28-30

Para la investigación a realizar los métodos de recolección de información que se utilizarán serán principalmente la encuesta, la observación de las instalaciones y la información de las personas que utilizan los servicios. Pag31 -34

La encuesta se aplicó a 476 y se presentarán los resultados obtenidos en cada una de las actividades expuestas necesarias para el cumplimiento del proyecto. De esta forma se podrá evidenciar el paso a paso para el cumplimiento del objetivo general en cuanto a las características necesarias para el diseño de un acceso de control de autenticación en las Instalaciones de la Unidad Nacional de Protección Sede Américas. Pag 36 - 39

Resultados, hallazgos u obra realizada Presente el resumen de los principales resultados o hallazgos de su investigación o una sinopsis de la obra creada. Señale los números de las páginas de su documento en los que se encuentra la información completa.
En los resultados encontramos que la mayoría de las personas que realizan las visitas no se encuentran conformes con el procedimiento actual para ingresar a las instalaciones. Realizado el análisis de información recopilada de manera visual como herramienta de recolección de datos se logra evidenciar. Pag 40 – 42 Teniendo en cuenta los resultados se generó un diseño para un sistema de control de acceso con sus diferentes elementos que lo componen. Pag 42 - 55
Conclusiones Presente el resumen de las conclusiones a las que llegó. Señale los números de las páginas de su documento en los que se encuentra la información completa.
Se puede observar a simple vista que el método de ingreso que se está usando actualmente para realizar el ingreso a la Unidad Nacional de protección es antiguo, inseguro y tardío. En el proceso de caracterización de falencias de la presente investigación se logra evidenciar que en la Unidad Nacional de protección – Sede Américas, presenta diferentes falencias al momento del ingreso de las personas al interior de las instalaciones , para esta actividad se usaron herramientas de recolección de información como los son la entrevista y método de observación, donde se realizó la tabulación de los datos obtenidos para posteriormente realizar su análisis, de igual modo se realizó análisis de los datos obtenidos por medio visual, los cuales se obtuvieron observando el procedimiento que realiza los vigilantes en el ingreso. En el diseño de esta solución se tuvieron en cuenta muchos factores como nivel de integración, compatibilidad y ante todo la seguridad de la información es por esto que se decidió trabajar con el sistema Access Management System (AMS) BOSCH, considerándose la opción más apropiada para el diseño propuesto en la Unidad Nacional de protección. Por otro lado, el sistema es compatibles con muchos dispositivos electrónicos que permitirán aumentar la seguridad al momento de ingresar a las instalaciones.
Productos derivados Referencie los artículos, libros, capítulos de libro, ponencias, etc., que fueron resultado de su proceso investigativo.
(s.f.). Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30030379 1341, L. (30 de 07 de 2009). Función pública. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913. Pag 12 - 14 1581, L. e. (17 de 10 de 2012). Función pública. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981 (10 de 09 de 2022). Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30030379 356, D. l. (11 de 02 de 1994). Función pública. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1341

Diseño de un control de acceso peatonal para el ingreso a las instalaciones de la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección en Bogotá sede Américas.

José Gabriel Ramírez Zambrano
Cod. 10226082
Jhon Freddy Quitian
Cod. 10226003
Edgar Daniel Soto Castillo
Cod. 10226074

Corporación Universitaria Unitec
Especialización en Gerencia de Proyectos
Bogotá, Distrito Capital
2023.

Diseño de un control de acceso peatonal para el ingreso a las instalaciones de la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección en Bogotá sede Américas.

José Gabriel Ramírez Zambrano

Cod. 10226082

Jhon Freddy Quitian

Cod. 10226003

Edgar Daniel Soto Castillo

Cod. 10226074

Asesor:

Juan Carlos Guzmán Gómez

Corporación Universitaria Unitec

Especialización en Gerencia de Proyectos

Bogotá, Distrito Capital

2023.

Tabla de Contenido

Tabla de figuras

Resumen

La presente investigación está enfocada en la manera como se controla el acceso de las personas a las instalaciones de la Subdirección Especializada de Seguridad y Protección (SEPS) adscrita a la Unidad Nacional de Protección (UNP).

Este proyecto, se lleva a cabo después de analizar el control de acceso a las instalaciones, donde se identifican que se presentan falencias y dificultades a la hora de llevar un control eficiente con la identificación de las personas que ingresan a las instalaciones, debido a que no tienen herramientas para verificar la información que presenta la persona que va ingresar, es por esto que se hace necesario realizar un diseño de control de acceso peatonal reforzando la seguridad en el ingreso con el fin de garantizar que las personas que ingresan a las instalaciones estén plenamente identificas, con el fin de proteger la información que se encuentra en el edificio.

Palabras Claves

SEPS: Subdirección Especializada de Seguridad y Protección.
UNP: Unidad Nacional de Protección.
Control de acceso.
Software de administración.
Biométricos.
Enrolamiento.
Torniquetes.
Seguridad.
Controlador.

1. Planteamiento del problema

Se visualiza que el acceso a la Subdirección especializada de Seguridad y Protección (SESP), se realiza un control de ingreso de marera precaria ya que no cuenta con las tecnologías y procedimientos necesarios para cumplir de manera responsable con las actividades necesarias para salvaguardar la integridad de los funcionarios e instalaciones.

En el presente en la SESP el control de acceso peatonal es realizado de forma visual. En la puerta de ingreso a las instalaciones está asignado un guarda de seguridad que está pendiente de todas las personas que ingresan a la institución. Como el flujo es constante y elevado en algunas horas, la labor de identificación es dispendiosa y se torna ineficiente ya que el control depende de las habilidades y antigüedad del funcionario, por esta razón para un vigilante que lleve tiempo en este mismo puesto es más fácil identificar el personal administrativo, sin embargo, se dificulta para las personas que van a realizar alguna solicitud y se debe solicitar un medio de identificación para permitirles el ingreso.

Por lo mencionado anterior, desde la creación de la Subdirección Especializada de Seguridad y Protección en el 2017, no se tiene un registro histórico del personal que ha ingresado a las instalaciones ya sean funcionarios o personal externo, por tal razón ante algún evento que se presentara en las instalaciones no se podría identificar oportunamente que personas estaban en las instalaciones, convirtiéndose en una situación muy delicada ya que en las instalaciones se maneja información delicada la cual debe ser salvaguardada con medidas se seguridad más rigurosas ya que actualmente el registro de personal e ingreso de los objetos electrónicos se realiza de forma manual (bitácora de registro), este proceso no es el más seguro para guardar información ya que la minutas pueden ser extraviadas o dañadas fácilmente.

2. Justificación

Actualmente en la Subdirección especializada de Seguridad y Protección (SESP) la seguridad de las instalaciones y personal administrativo y operativo que labora allí está a cargo de una empresa de vigilancia privada, en el último año pese a las dificultades de seguridad de los beneficiarios la instalaciones se han visto concurridas diariamente por un gran flujo de personas administrativos, agentes escoltas de todo el territorio nacional ascienden a más de 1300 personas, y a diario en las instalaciones ingresan el personal de planta y contratistas ops a prestar sus servicios los cuales son más de 200 personas.

Se logra identificar una dificultad en el acceso del personal que labora en las instalaciones y visitantes, ya que el ingreso se realiza por medio de verificación visual de un carné que otorga la Subdirección Especializada de Seguridad y Protección (SESP) y que lo verifica la empresa de seguridad que presta los servicios de vigilancia, los cuales son los responsables del ingreso de toda persona a las instalaciones. Por tal motivo se trabaja en el proyecto de investigación orientado a crear un diseño de acceso peatonal eficiente y procedimientos con el fin de garantizar la seguridad y validar la identificación con plenitud de las personas que ingresan a las instalaciones.

3. Pregunta de Investigación

¿Como realizar un control de acceso peatonal para el ingreso a las instalaciones de la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección en Bogotá -sede Américas?

4. Objetivos

4.1 Objetivo general

Elaborar un diseño de control de acceso peatonal para el ingreso a las instalaciones de la Subdirección Especializada de Seguridad y Protección adscrita a la Unidad Nacional de Protección en Bogotá sede Américas.

4.2 Objetivos específicos

Identificar las falencias del control de acceso peatonal que se tiene en la actualidad por medio de unas encuestas realizadas al personal que ingresa a las instalaciones tanto visitantes como los trabajadores.

Definir la mejor solución del control de acceso peatonal a las instalaciones de la Subdirección de Seguridad y Protección (SESP), adscrita a la Unidad Nacional de Protección (UNP), sede Américas.

Realizar un instructivo de procedimientos de acuerdo con el control de acceso peatonal propuesto para el ingreso a las instalaciones.

5. Marco Teórico

Para el desarrollo del diseño de control de acceso revisaremos referencias teóricas las cuales nos ayudara a entrar en contexto sobre las tecnologías que se utilizaran para controlar el acceso de personas.

5.1 Control de acceso

Un control de acceso es un sistema que impide que una persona entre en un lugar sin identificación previa de algún tipo. Ya sea la huella dactilar o un dispositivo electrónico, es necesario identificarse antes de entrar.

Todas las empresas, casas o edificios tienen cosas que proteger: dinero, bienes, personas, ideas… Cualquier cosa que apreciemos y queramos conservar y pongamos a salvo tras un sistema de seguridad y un sistema de control de acceso que permita controlar quién accede al interior de un edificio.

Las cerraduras y las llaves permiten el acceso a un edificio, pero si hay algún problema como la pérdida de llaves, se crea un alto riesgo para nuestra propiedad porque las llaves pueden ser copiadas fácilmente. Además, es muy costoso solucionar el problema ya que hay que cambiar la cerradura o hacer llaves nuevas. (Protelec, s.f.)

5.1.1 Sistemas biométricos.

En un sistema de Biometría típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 999,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (False Acceptance Rate o FAR), la tasa de falso negativo (False NonMatch Rate o FNMR, también False Rejection Rate o FRR), y el fallo de tasa de alistamiento (Failure-to-enroll Rate, FTR o FER).

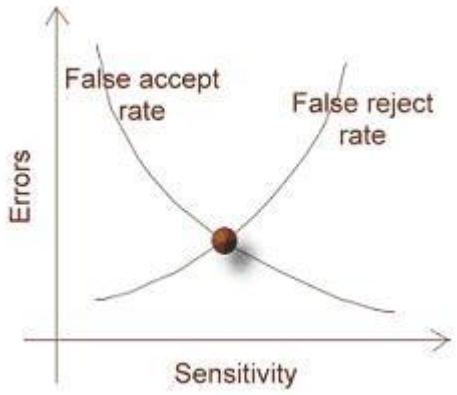


Figura 1 Funcionamiento y rendimiento. Maersa (2022).

En los sistemas biométricos reales el FAR y el FRR puede transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los relojes checadores biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (Equal Error Rate o EER), también conocida como la tasa de error de cruce (Cross-over Error Rate o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto. (Maersa, s.f.)

Un sistema biométrico en general consta de componentes tanto hardware como softwares necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

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

Tabla comparativa de sistemas biométricos.

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Geometría de la mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Baja	Alta	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

Figura 2 Funcionamiento y rendimiento. Maersa (2022).

5.1.2 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.

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 3. Identificando Patrones. César Tolosa Borja (2019).

Todo esto da lugar a un patrón complejo único para cada individuo, distinto incluso en gemelos idénticos. En concreto, se estima que la probabilidad de que dos personas tengan las mismas huellas dactilares es aproximadamente de 1 en 64.000 millones. Cuando se digitaliza una huella, los detalles relativos a las líneas (curvatura, separación, ...), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten obtener un índice numérico correspondiente a dicha huella. En el momento en que un usuario solicita ser identificado, coloca su dedo sobre un lector (óptico, de campo eléctrico, por presión, ...) y su huella dactilar es escaneada y analizada con el fin de extraer los elementos característicos y buscar su homóloga en la base de datos. El resultado es un diagnóstico certero en más del 99% de los casos. Las técnicas utilizadas para la comparación de la huella dactilar se pueden clasificar en dos categorías:

La técnica de puntos Minutia primero encuentran estas minucias y posteriormente procede a su colocación relativa en el dedo. Es difícil extraer los puntos de las minucias exactamente cuando la huella dactilar es de baja calidad. También este método no considera el patrón global de crestas y de surcos.

El método correlación puede superar algunas de las dificultades de la comparación por puntos Minutia; sin embargo, tiene algunos inconvenientes propios. La técnica de correlación requiere una localización precisa de un punto de registro y se ve afectada por el desplazamiento y rotación de la imagen. **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

y entonces, en un nivel más fino, se compara con el subconjunto de la base de datos que contiene solamente ese tipo de huella dactilar. Se utilizan algoritmos desarrollados para identificar a cuál de estos tipos de pertenecer una huella en concreto. Realce de la Huella Un paso crítico en la clasificación automática de la huella dactilar está en extraer mediante un algoritmo las minucias 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 del surco de las imágenes de las huellas dactilares de entrada. (Graciani, s.f.Biometria.pdf)

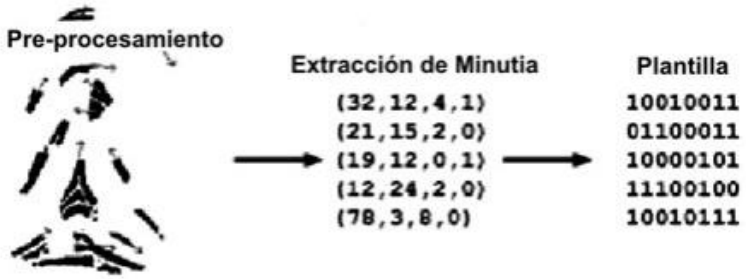


Figura 4. Realce de la Huella. César Tolosa Borja (2019).

5.1.3 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 calculara 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.

Funcionamiento

Figura 5. Funcionamiento. César Tolosa Borja (2019).

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. 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 eigenfaces 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 con normalidad 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". (César Tolosa Borja, Sistemas Biométricos, s.f.)

5.1.4 Reconocimiento de iris

El iris es la porción de color del ojo, en el centro del iris se encuentra la pupila. El patrón del iris de una persona es único y permanece inalterado a lo largo su vida. Además, cubierto por la córnea, el iris está bien protegido del daño, por lo que es una parte adecuada del cuerpo para la autenticación biométrica.

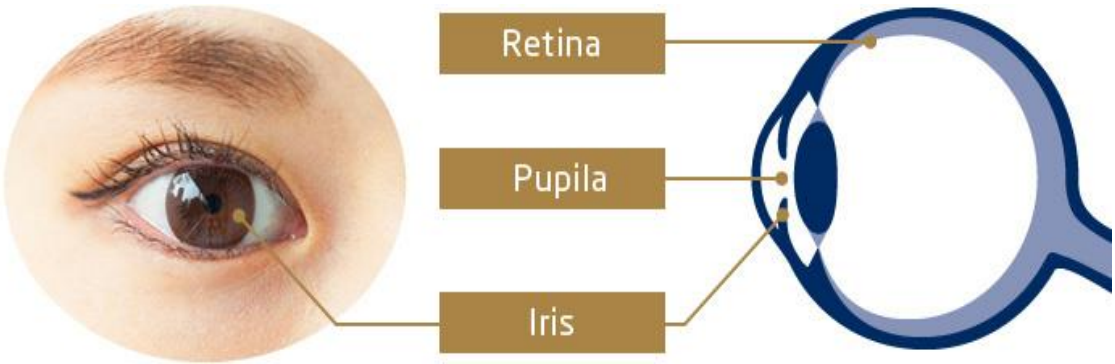


Figura 6. Reconocimiento de Iris. Nec (2022).

Características del reconocimiento de iris

El reconocimiento del iris es altamente preciso, rápido y presume de tener una exactitud de primera clase entre los diferentes tipos de tecnologías de autenticación biométrica.

- Permanece inalterable a lo largo de la vida. (Esto no constituye una garantía)
- Dado que el iris es diferente entre el ojo izquierdo y el derecho, el reconocimiento se puede realizar por separado en cada ojo.
- Posibilita el distinguir gemelos.
- Mientras los ojos estén expuestos, el reconocimiento del iris se puede utilizar incluso cuando el sujeto lleva un sombrero, máscara, anteojos o guantes.
- Debido al uso de una cámara infrarroja, el reconocimiento está disponible incluso de noche o en la oscuridad.
- No hay necesidad de tocar un dispositivo, la autenticación sin contacto es posible, por lo que es higiénico de usar.

Mecanismo del reconocimiento del iris

En primer lugar, se detecta la ubicación de la pupila, seguida de la detección del iris y los párpados.

Las partes innecesarias (ruido), como párpados y pestañas, se excluyen para recortar sólo la parte del iris, que luego se divide en bloques y se convierte en valores para cuantificar la imagen.

A continuación, la coincidencia se realiza con los datos de las características extraídas previamente en los mismos métodos. (Nec,ReconocimientodeIriss.f.)

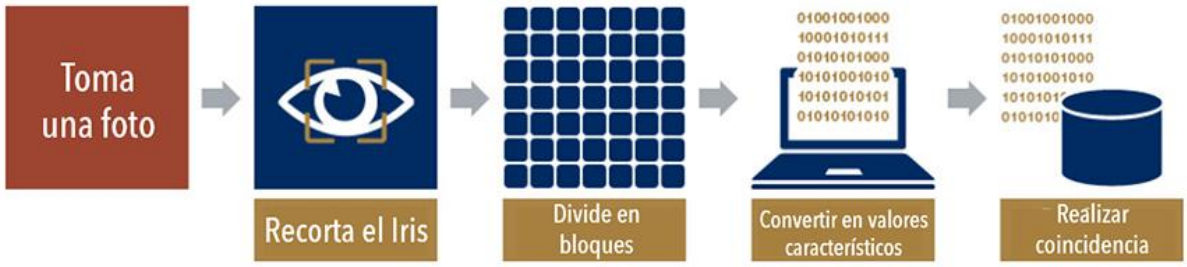


Figura 7. Mecanismo del reconocimiento del Iris. Nec (2022).

5.1.5 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 las 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.

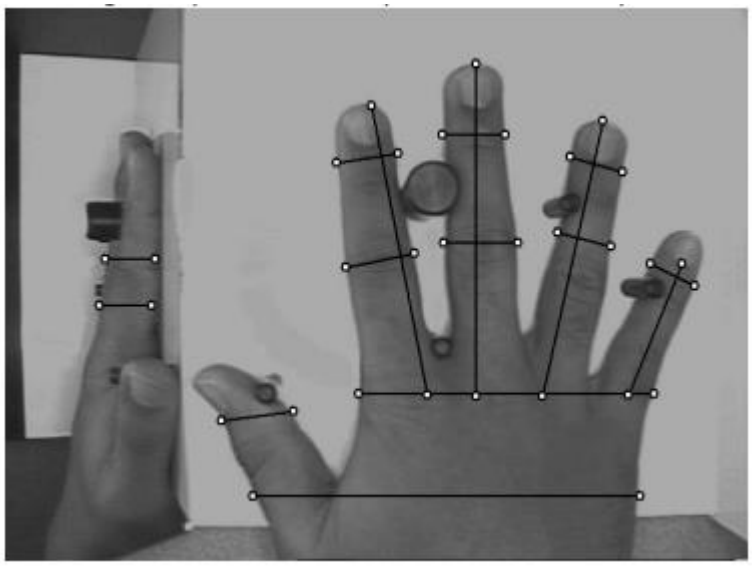


Figura 8. Geometría de la mano. César Tolosa Borja (2019).

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, actualizan 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. (César Tolosa Borja, Sistemas Biométricos, s.f.)

5.2 Antecedentes

Durante años se ha desarrollado proyectos referentes a los controles de acceso para diferentes entidades, a continuación, citaremos algunas.

Qusay H. Tawfeeq, **Ahmed H. Y. Al-Noori**, **Amjed N. Jabir** en su proyecto Design and Implementation of an Access Control System Using Open Source Personality Identification Software desarrollado en Department of Computer Engineering, Al_Nahrain University, Baghdad, Iraq, basaron su proyecto en mejorar las seguridad de control de acceso a casilleros con una biometría multimodal, en el cual identifican rasgos faciales y de habla de cada persona, con esto buscan minimizar el ingreso de intrusos, este sistema se implementa con éxito en una Raspberry pi 3 de bajo costo en tiempo real. Los resultados obtenidos por este trabajo logran una alta precisión en el sistema de verificación de rostro y voz. (H. Tawfeeq, HY Al-Noori, & N. Jabir, 2020)

Otra de la investigaciones a nivel internacional encontramos a los estudiantes Ahmed Raad Al-Sudania , Wanlei Zhoub , Bo Liuc , Ahmed Almansoorid and Mengmeng Yange en su publicación Detecting Unauthorized RFID Tag Carrier for Secure Access Control to a Smart Building en su investigación exponen la importancia de contar con un control de acceso

confiable para proteger el edificio inteligente de acceso no autorizados a él, para ello explican la forma de hacerlo a través de 3 algoritmos que se encargan de verificar diferentes puntos de seguridad y con ellos evitar ingreso de cualquier intruso a la zona protegida a través de una tarjeta RFID e imágenes de video.

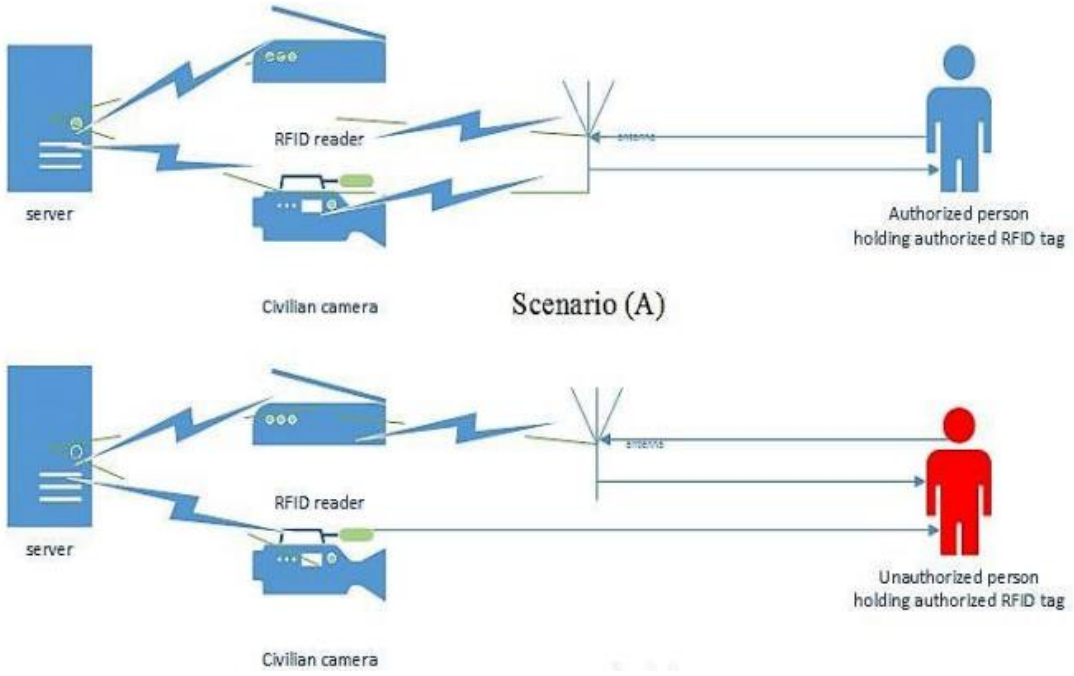


Figura 9. Detecting Unauthorized RFID Ahmed Raad Al-Sudania (2021)

Otra interensante investigacion es la del estudiante CASTRO MIRANDA PABLO CESAR (2018) en su proyecto de investigación "implementar un sistema de control de acceso biométrico ZK-X7 por medio de huella dactilar en el laboratorio de hardware de la Carrera de Ingeniería en Computación y Redes" en la universidad estatal del sur de Manabí-ecuador facultad de ciencias técnicas. Tuvo como objetivo optimizar el ingreso laboratorio debido a que carecía de un control de acceso y por ende un nivel de seguridad nulo, por lo cual el riesgo de pérdida de equipos informáticos es alto.

Se concluye que esta investigación refleja los beneficios de carácter personal e institucional, evidenciados en los resultados obtenidos en la encuesta y entrevista donde se demuestra que, mediante esta implementación fiable, se logrará obtener un nivel de seguridad óptimo y a la vanguardia de la tecnología.

También San Martín Guillén, (2019) en su tesis de grado "Diseño e implementación de un sistema de control de acceso por Biometría" para la empresa PERÚ OFFSET EDITORES tuvo como objetivo mejorar la seguridad y el control de acceso al área de mantenimiento, utilizando características inherentes de las personas afines al área, tales como huellas digitales; ya que es uno de los métodos más populares usados con mayor grado de éxito para la identificación de las personas y el reconocimiento facial; para lo cual se realizó el diseño de un prototipo basado en una tarjeta Raspberry Pi, la cual almacena la información de los usuarios en una base de datos y es capaz de analizar sus características mediante algoritmos como los desarrollados por Paul Viola y Michael Jones para decidir si la persona que desea ingresar está o no autorizada para hacerlo.

Por otra parte, FERNANDEZ ORTIZ, (2019) en su proyecto de grado "sistema de control de acceso basado en la tecnología de autenticación biométrica por huella dactilar para el instituto técnico comercial - la paz" para desarrollar el proyecto opto por mejorar los controles existentes en la institución, para esto utilizo diferentes metodologías como son:

- El método analítico será utilizado en el análisis teórico de los protocolos de comunicación que serán utilizados como interfaz para la etapa de comunicación.
- El método lógico deductivo se lo empleara en los circuitos de control y el software de visualización para la interfaz, puesto que los procesos se llevarán dentro de los mismos.
- El método experimental es primordial en el presente proyecto porque el sistema propuesto deberá ser compatible con tecnologías existentes, cuya eficiencia y estabilidad será puesta a prueba de forma exhaustiva experimentando el correcto funcionamiento de los diversos subsistemas que la conforman.

Todo el desarrollo lo hicieron a medida con Arduino en el cual programaron la tarjeta controladora para analizar huellas a través de lectores, permitiendo identificar cada persona para verificar si tenía acceso al área o no. El diseño de la interfaz gráfica de usuario, usando Windows Forms. Ofrece una interfaz de comunicación USB, entre la tarjeta de desarrollo y el equipo PC. Asegurando que los datos enviados lleguen a su destino sin ningún tipo de distorsión.

5.3 Bases teóricas

De conformidad con lo establecido en el artículo tercero (3°) del Decreto 4065 de 2011, "el objetivo de la Unidad Nacional de Protección (UNP) es articular, coordinar y ejecutar la prestación del servicio de protección a quienes determine el Gobierno Nacional que por virtud de sus actividades, condiciones o situaciones políticas, públicas, sociales, humanitarias, culturales, étnicas, de género, de su calidad de víctima de la violencia, desplazado, activista de derechos humanos, se encuentren en situación de riesgo extraordinario o extremo de sufrir daños contra su vida, integridad, libertad y seguridad personal o en razón al ejercicio de un cargo público u otras actividades que pueden generar riesgo extraordinario, como el liderazgo sindical, de ONG y de grupos de personas desplazadas, y garantizar la oportunidad, eficiencia e idoneidad de las medidas que se otorgan. Se exceptúan del campo de aplicación del objetivo de la Unidad los programas de competencia de la fiscalía general de la Nación, la Procuraduría General de la Nación y el Programa de Protección a Víctimas y Testigos de la Ley de Justicia y Paz". (PROTECCIÓN, UNIDAD NACIONAL DE PROTECCIÓN, 2022)

Misión

La Unidad Nacional de Protección es un organismo de seguridad del orden nacional, con orientación de Derechos Humanos, encargada de desarrollar estrategias para el análisis y evaluación de los riesgos, amenazas y vulnerabilidades, e implementar las medidas de protección individuales y/o colectivas de las poblaciones objeto, con enfoques diferenciales. (PROTECCIÓN, UNIDAD NACIONAL DE PROTECCIÓN, 2022)

Visión

Ser una Entidad idónea, confiable y comprometida, que contribuya en la garantía efectiva al derecho a la vida, integridad, libertad y seguridad de las poblaciones objeto de prevención y protección. (PROTECCIÓN, UNIDAD NACIONAL DE PROTECCIÓN, 2022)

Objetivos estratégicos

a. Propender por una cultura de respeto y garantía de los Derechos Humanos, que contribuya al proceso de construcción de paz.

b. Fortalecer la capacidad institucional para identificar oportunamente las amenazas, riesgos y vulnerabilidades a las cuales están expuestas las poblaciones objeto.

c. Gestionar soluciones estratégicas que contribuyan a la garantía efectiva al derecho a la vida, libertad y seguridad de las poblaciones objeto y optimizar los tiempos de respuesta en la ruta de protección.

d. Fortalecer las capacidades institucionales para la inclusión de los enfoques diferenciales en los procesos misionales.

e. Fortalecer la entidad a través de la implementación de las políticas de desempeño institucional de MIPG y las mejores prácticas que generen valor público a nuestra población objeto y grupos de interés. (PROTECCIÓN, UNIDAD NACIONAL DE PROTECCIÓN, 2022)

Organigrama

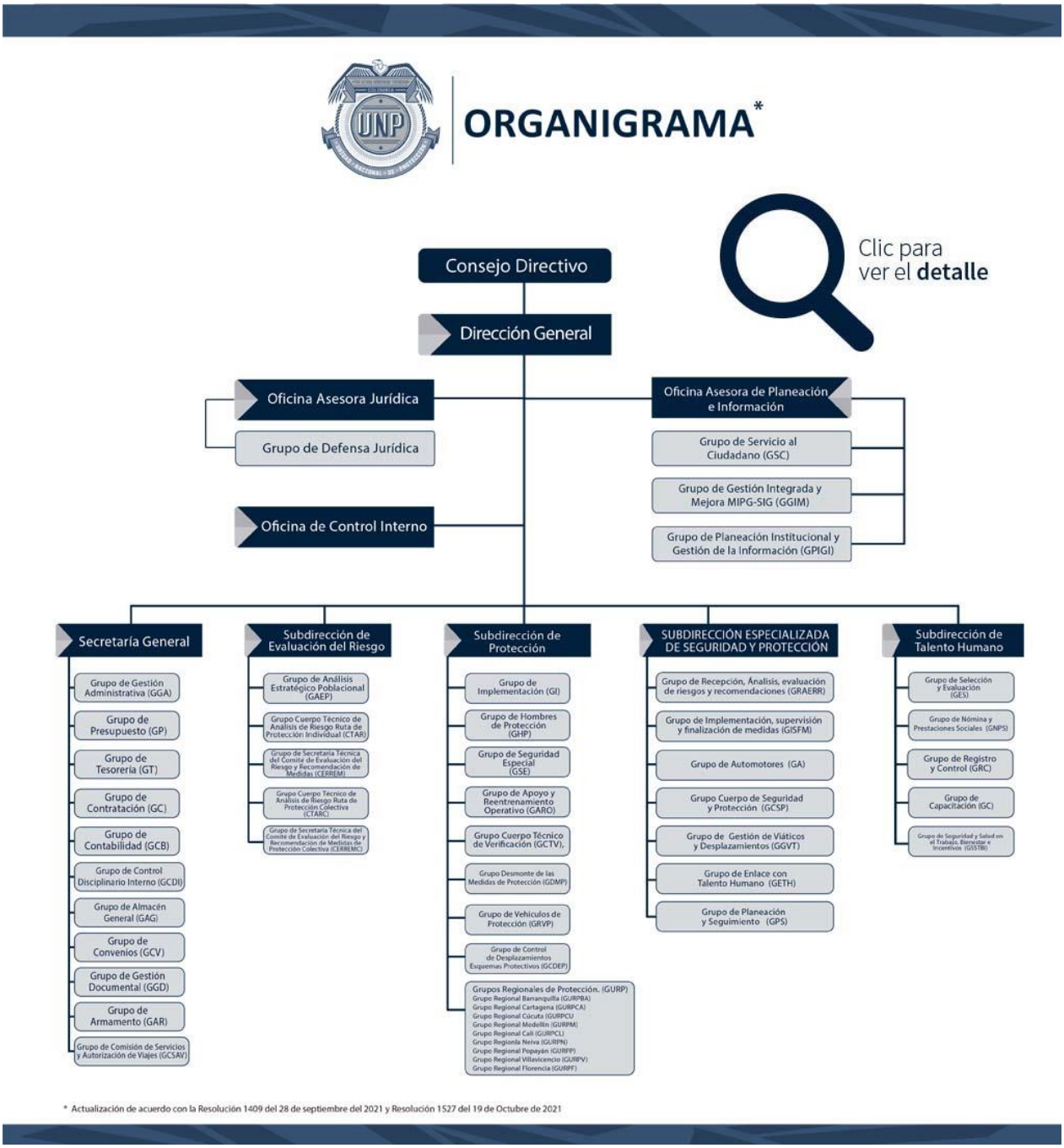


Figura 10. Organigrama Unidad nacional de protección – resolución 1527 de octubre (2021)

5.4 Marco legal

Decreto 356 del 11 febrero de 1994, por el cual se expide el Estatuto de Vigilancia y Seguridad Privada, entiéndese por servicios de vigilancia y seguridad privada, las actividades de que en forma remunerada o en beneficio de una organización pública o privada, desarrollan las personas naturales o jurídicas, tendientes a prevenir o detener perturbaciones

a la seguridad y tranquilidad individual en lo relacionado con la vida y los bienes propios o de terceros y la fabricación, instalación, comercialización y utilización de equipos para vigilancia y seguridad privada, blindajes y transporte con este mismo fin. (356, 1994)

Ley 675 de 2001 por medio de la cual se expide el régimen de propiedad horizontal, la cual regula la forma especial de dominio, denominado propiedad horizontal, en la que concurren derechos de propiedad exclusiva sobre bienes privados y derechos de copropiedad sobre el terreno y los demás bienes comunes, con el fin de garantizar la seguridad y la convivencia pacífica en los inmuebles sometidos a ella, así como la función social de la propiedad. (675, 2001)

Ley 1341 del 30 de julio de 2009, **Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones, determinando** el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información. (1341, 2009)

Ley estatutaria 1581 del 17 de octubre de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales, teniendo presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (1581, 2012)

5.5 Marco Conceptual

Seguridad electrónica:

El concepto de seguridad electrónica engloba a todos los productos y servicios que, basados en algún dispositivo electrónico, permiten implementar controles y avisos automáticos como complemento fundamental de cualquier plan general de seguridad. (ETICSA, s.f.)

Sistemas de Control de Acceso

Es aquel sistema que permite la autorización o la restricción de paso de una persona o vehículo a una zona restringida teniendo en cuenta determinados parámetros establecidos previamente.

Estos sistemas de control de acceso pueden darse en dos vertientes. En el sentido físico, para realizar un seguimiento del acceso a instalaciones físicas, ya sea a edificios de empresas, a comunidades de vecinos o a zonas concretas de estas instalaciones. Se podrá segmentar el acceso de los usuarios en función de horarios, días o según las concesiones de cada uno.

En el sentido virtual, refiriéndose a la seguridad informática, para determinar qué usuarios tienen los permisos correspondientes para acceder a determinados recursos o información en los sistemas informáticos**.** (VIATEK, s.f.)

Identificación

Existen distintos métodos para identificar a la persona que intenta acceder a la zona restringida. La identificación es esencial para determinar si el usuario cumple los requisitos de acceso. (VIATEK, s.f.)

6. Método

El enfoque de la investigación a realizar en el presente proyecto es la cualitativa ya que se utilizarán instrumentos de recolección de información apropiados como entrevistas y visitas al entorno para el desarrollo de la investigación.

Enfoque Cualitativo: Los autores Blasco y Pérez (2007:25), señalan que la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas.

Una vez utiliza esta variedad de instrumentos, para recoger información como las entrevistas, imágenes, observaciones, historias de vida, en los que se describen las rutinas y las situaciones problemáticas, así como los significados en la vida de los participantes. (Eumed.net, 2022)

6.1 Tipos de diseño

Si hay un problema por resolver o un tema específico por investigar científicamente, es muy útil tener un conocimiento detallado de los posibles tipos de investigación que se pueden realizar. pueden continuar. El tipo de investigación utilizado en este estudio se enumera a continuación.

Investigación Experimental: Recibe este nombre la investigación que se realiza con el propósito de destacar los aspectos fundamentales de una problemática determinada y encontrar los procedimientos adecuados para elaborar una investigación posterior. (Tomala, 2022)

Bitácora de las actividades a ejecutar

Las siguientes actividades son las que se van a ejecutar en el proyecto.

DISEÑO DE UN CONTROL DE ACCESO PEATONAL PARA EL INGRESO A LAS INSTALACIONES DE LA SUBDIRECCION ESPECIALIZADA DE SEGURIDAD Y PROTECCION ADSCRITA A LA UNIDAD NACIONAL DE PROTECCIÓN EN BOGOTÁ -SEDE AMERICAS
ACTIVIDADES POR EJECUTAR
INICIO
• Evaluación del acceso actual a la sede
• Identificación de falencias
ANÁLISIS DE LA SOLUCIÓN
• Definir el dispositivo para la identificación de personas
• Definir el sistema de control de acceso
• Definir el torniquete para control de acceso
DISEÑO Y MODELAMIENTO
• Diseño de diagrama de conexiones de los dispositivos
• Diseño del diagrama de comunicación con el software de control de acceso
DISEÑO DEL CONTROL DE ACCESO PEATONAL A LAS INSTALACIONES
• Crear procedimiento del control de acceso
• Crear manual de uso
• Definición de requerimientos para una posible implementación
• Características necesarias a nivel de hardware
• Características necesarias a nivel de software

Figura 11. Fuente Propia (2022)

6.2 Participantes o fuentes de datos

Población: personal a ingresar a las instalaciones de la subdirección especializada de seguridad y protección en Bogotá sede Américas.

Muestra: funcionarios de la unidad nacional de protección a ingresar a la subdirección especializada de seguridad y protección en Bogotá sede Américas.

Se mejorará el acceso y la seguridad a las instalaciones en la subdirección especializada de seguridad y protección adscrita a la unidad nacional de protección (UNP) en Bogotá sede américas, a través de un sistema de control de acceso.

6.3 Recolección de datos

Para la investigación a realizar los métodos de recolección de información que se utilizarán serán principalmente la encuesta, la observación de las instalaciones y la información de las personas que utilizan los servicios.

INSTRUMENTOS DE RECOPILACIÓN DE INFORMACIÓN:

Los instrumentos utilizados para la recopilación de datos e información necesaria para el desarrollo del proyecto fueron los siguientes:

INSTRUMENTO OBSERVACION

Una de las herramientas para recopilar la información es la observación, que implica observar a las personas en su entorno natural o en situaciones que suceden naturalmente.
APLICACIÓN DE INSTRUMENTO OBSERVACION

Para realizar el ingreso a las instalaciones de la Unidad Nacional de Protección – sede Américas, del personal administrativo, operativo, visitantes o cualquier otra persona externa se debe realizar un paso a paso que lo realiza la empresa de vigilancia que tiene a cargo las instalaciones, en el cual se realiza a observar la metodología utilizada con el fin de realizar un análisis de este.

Descripción del ingreso de las personas a las instalaciones de la Unidad Nacional de protección Sede Américas.

- Se inicia en la entrada de las instalaciones con la presencia de un vigilante mostrando el debido carné de identificación de la UNP o documento personal, seguido de la verificación por parte de este con una paleta de scanner de metales de manera manual.

Figura 12. Primer Ingreso

- Seguidamente se realiza anotación manual por parte de otro vigilante de los equipos tecnológicos que se ingresen a las instalaciones, del mismo modo se pasa las pertenencias por la banda scanner.

Figura 13. Segundo ingreso

- Sin ninguna novedad se realiza el ingreso a las instalaciones de la Unidad nacional de protección de la UNP. (el scanner de arco se encuentra deshabilitado)

Figura 14. Tercer Ingreso

- Para el ingreso a las instalaciones del personal externo y beneficiarios del programa es un poco más demorado el ingreso y el paso a paso es el siguiente.
    - Se inicia con la identificación de la persona y para que dependencia se va a dirigir, seguido de seguido de la verificación por parte de este con una paleta de scanner de metales de manera manual
    - Pasa a la sala de espera, donde el vigilante se desplaza hasta la coordinación correspondiente para generar el correo que se debe enviar al correo de la empresa de vigilancia para poder realizar el ingreso.

Figura 15. Sala de espera

    - De la misma manera la persona externa pasa a la ventanilla de ingreso de visitantes, donde se le toman alguno daos personales y entrega de un documento para poder asignarle una identificación temporal para que pueda recorrer las instalaciones de la UNP.

Figura 16. Cuarto Ingreso

- Terminando para el paso a paso se realizan los puntos 2 y 3 anteriormente descritos en el ítem anterior e ingresa a las instalaciones

INSTRUMENTO ENCUESTA

según (Manuel García Ferrando, 2023) define la encuesta una "técnica que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge y analiza una serie de datos de una muestra de casos representativa de una población o universo más amplio, del que se pretende explorar, describir, predecir y/o explicar una serie de características"

APLICACIÓN DE INSTRUMENTO ENCUESTA

Dentro de los resultados arrojados para la encuesta realizada al personal que hace presencia a las instalaciones de la Unidad Nacional de Protección como insumo para el diseño de un acceso de control de autenticación se realizó con el instrumento de encuesta de manera digital por la aplicación de Google (formularios). Mediante el enlace https://forms.gle/syXgKn2ZBHgMZfQY6 . La encuesta realizada se aplicó a 437 personas que respondieron satisfactoriamente las preguntas que se realizaron.

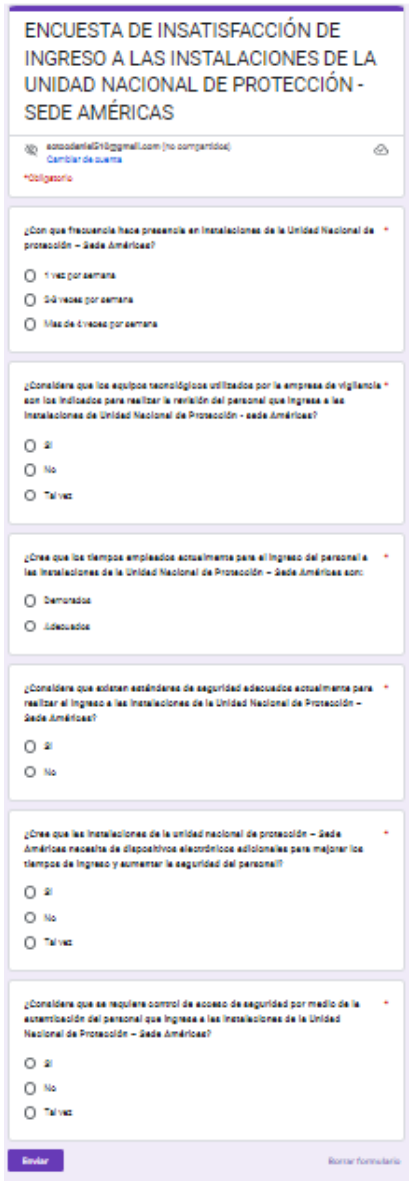


Figura 17. Encuesta

6.4 Análisis

A continuación, se presentarán los resultados obtenidos en cada una de las actividades expuestas necesarias para el cumplimiento del proyecto. De esta forma se podrá evidenciar el paso a paso para el cumplimiento del objetivo general en cuanto a las características necesarias para el diseño de un acceso de control de autenticación en las Instalaciones de la Unidad Nacional de Protección Sede Américas.

RESULTADO DE LAS ENCUESTAS

Como resultado de este análisis a la pregunta ¿Con que frecuencia hace presencia en instalaciones de la Unidad Nacional de protección – Sede Américas?, el 77,8% con 340 respuestas ingresan más de 4 veces por semana, el 18,8% con 82 respuestas ingresan de 2- 3 veces por semana y el 3,4% con 15 respuestas ingresan 1 vez por semana.

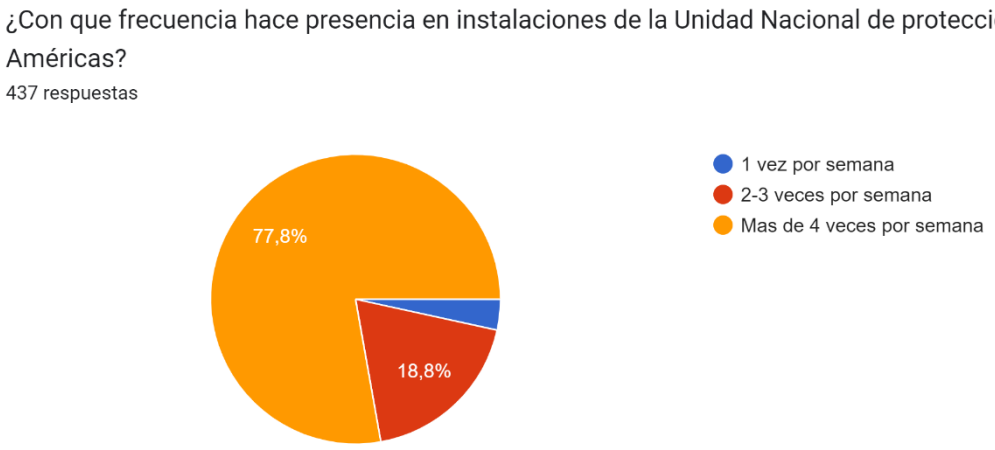


Figura 18. Resultado primera pregunta

Así mismo en la pregunta ¿Considera que los equipos tecnológicos utilizados por la empresa de vigilancia son los indicados para realizar la revisión del personal que ingresa a las instalaciones de Unidad Nacional de Protección - sede Américas?, El 80,5% con 352 respuesta indican que no son los indicados, el 11% con 48 respuesta opinan que tal vez lo sean, 8,5% con 37 respuestas indican que si son los indicados.

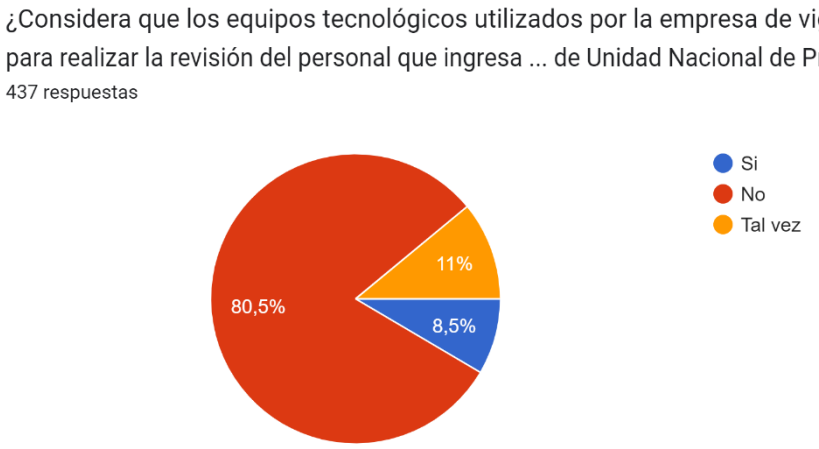


Figura 19. Resultado segunda pregunta

De igual modo en respuesta a ¿Cree que los tiempos empleados actualmente para el ingreso del personal a las instalaciones de la Unidad Nacional de Protección – Sede Américas son: El 95% con 415 respuestas indican que los tiempos de ingreso son demorados y el 5% con 22 respuestas indican que los tiempos de ingreso son los adecuados.

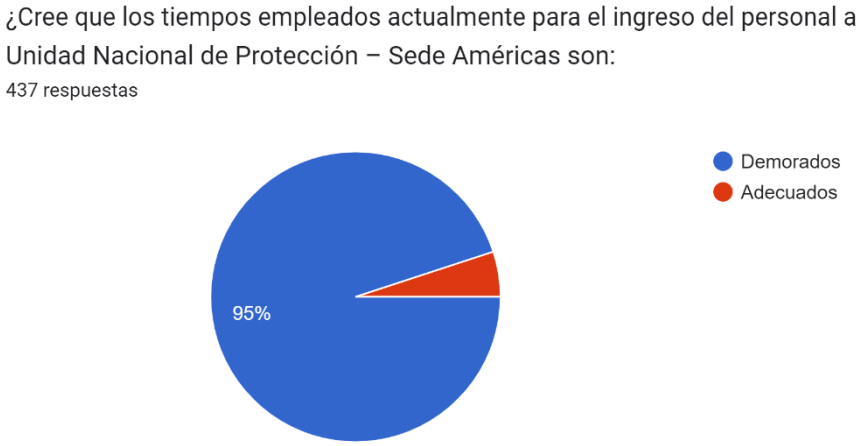


Figura 20. Resultado tercer pregunta

En respuesta a la pregunta ¿Considera que existen estándares de seguridad adecuados actualmente para realizar el ingreso a las instalaciones de la Unidad Nacional de Protección – Sede Américas?, para lo cual el 87% con 380 respuestas indicaron que no existen

estándares de seguridad y el 13% con 57 respuestas indicaron que si existen.

Figura 21. Resultado cuarta pregunta

En respuesta a la pregunta ¿Cree que las instalaciones de la unidad nacional de protección – Sede Américas necesita de dispositivos electrónicos adicionales para mejorar los tiempos de ingreso y aumentar la seguridad del personal?, para lo cual el 93,1% con 407 respuestas indicaron que si son necesarios nuevos dispositivos electrónicos y el 4,8% con 21 respuestas indicaron que no son necesarios y el 2,01% indicas que tal vez sean necesarios.

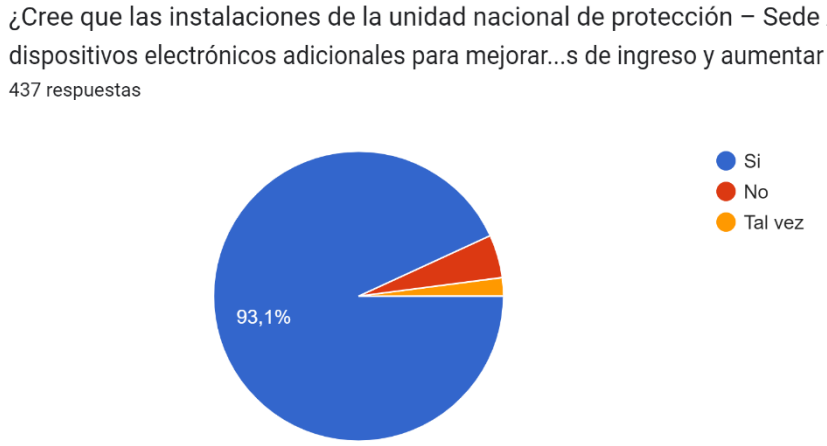


Figura 22. Resultado quinta pregunta

En respuesta a la pregunta ¿Considera que se requiere control de acceso de seguridad por medio de la autenticación del personal que ingresa a las instalaciones de la Unidad Nacional de Protección – Sede Américas?, para lo cual el 94,7% con 414 respuestas indicaron que, si se requiere un control de acceso, 2,99% con 13 respuestas indicaron que

no se requiere y el 2,4% con 10 respuestas indican que tal vez se requiera.

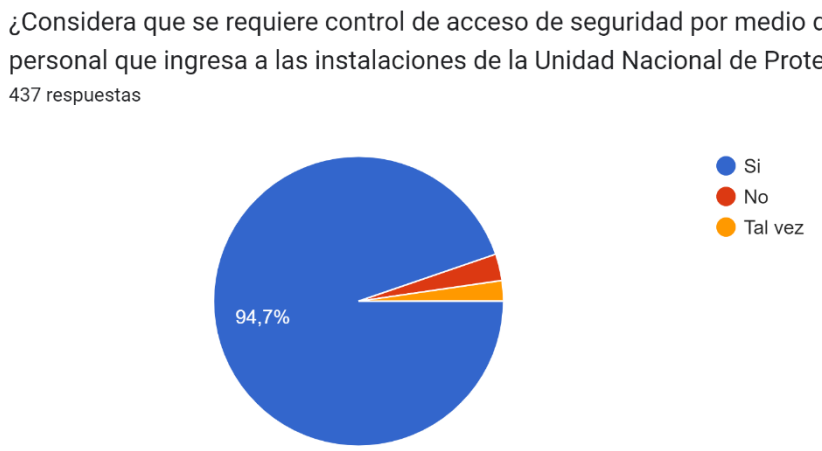


Figura 23. Resultado sexta pregunta

7. Cronograma y presupuesto

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1		PLAN DE CONTROL DE ACCESO PEATONAL PARA EL INGRESO A LAS INSTALACIONES DE LA SUBDIRECCION ESPECIALIZADA DE SEGURIDAD Y PROTECCION ADSCRITA A LA UNIDAD NACIONAL DE PROTECCIÓN EN BOGOTÁ -SEDE AMERICAS	204 días	mar 16/08/22	vie 26/05/23		
2		**INICIO**	0 días	mar 16/08/22	mar 16/08/22		Jose Gabriel Ramirez
3		evaluacion del acceso actual a la sede	20 días	mar 16/08/22	lun 12/09/22	2	
4		Identificacion de falencias	30 días	mar 16/08/22	lun 26/09/22		
5		**Analisis de la solucion**	0 días	lun 26/09/22	lun 26/09/22	4	
6		Definir el dipositivos para la identificación de personas	25 días	mar 27/09/22	lun 31/10/22	5	
7		Definir el torniquete para control de acceso	25 días	mar 27/09/22	lun 31/10/22		
8		Definir el sistema de control de acceso	25 días	mar 27/09/22	lun 31/10/22		
9		**Diseño y modelamiento**	0 días	lun 31/10/22	lun 31/10/22	8	
10		Diseño de diagrama de conexiones de los dispositivos	20 días	mar 01/11/22	lun 28/11/22	9	
11		Diseño del diagrama de comunicación con el software de control de acceso	20 días	mar 29/11/22	lun 26/12/22	10	
12		**Plan de acceso peatonal a las instalaciones**	0 días	lun 26/12/22	lun 26/12/22	11	
13		Crear procedimiento del control de acceso	20 días	mar 27/12/22	lun 23/01/23	12	
14		Crear manual de uso	18 días	mar 14/02/23	jue 09/03/23		
15		**Definicion de requerimientos para una posible implementacion**	0 días	jue 09/03/23	jue 09/03/23	14	

Figura 24. Elaboración Propia (2022)

PLAN DE CONTROL DE ACCESO PEATONAL PARA EL INGRESO A LAS INSTALACIONES DE LA SUBDIRECCION ESPECIALIZADA DE SEGURIDAD Y PROTECCION ADSCRITA A LA UNIDAD NACIONAL DE PROTECCIÓN EN BOGOTÁ -SEDE AMERICAS	Unidad	Valor unitario
Evaluacion del acceso actual a la sede	3 personas	$ 7.200.000
Identificacion de falencias	1 persona	$ 3.300.000
Definir el dipositivos para la identificación de personas	2 personas	$ 7.500.000
Definir el torniquete para control de acceso	1 persona	$ 2.000.000
Definir el sistema de control de acceso	1 persona	$ 2.000.000
Diseño de diagrama de conexiones de los dispositivos	1 persona	$ 1.800.000
Diseño del diagrama de comunicación con el software de control de acceso	1 persona	$ 1.800.000
Crear procedimiento del control de acceso	1 persona	$ 1.200.000
Crear manual de uso	1 persona	$ 1.080.000
Caracteristicas necesarias a nivel de hardware	1 persona	$ 400.000
Caracteristicas necesarias a nivel de software	1 persona	$ 400.000
Lectores de tarjetas	4 und	$ 4.100.000
Tornos	2 und	$ 8.500.000
Fuentes de alimentacion	4 und	$ 2.200.000
Paneles de acceso	2 und	$ 3.600.000
Tarjetas de acceso	200 und	$ 300.000
Cableado electrico	200 mtrs	$ 280.000
Cableado de instrumentacion 6 *14	200 mtrs	$ 320.000
Equipo para gestion del control de acceso	1 und	$ 3.200.000
Software de control de acceso	1 und	$ 6.000.000
Ajustes de infraestrutura para instalacion de equipos	1 und	$ 3.500.000
Instalacion del control de acceso	1 und	$ 5.000.000
Configuracion y puesta en marcha de sistema	1 und	$ 2.500.000
Capacitacion del personal en el uso adecuado del sistema de control de acceso	1 und	$ 1.200.000
	Total	**$ 69.380.000**

Figura 25. Elaboración Propia (2022)

8. Resultados o hallazgos

Realizando el análisis de los instrumentos aplicados (método de observación y encuesta) con base a los resultados obtenidos, se logra evidenciar los siguientes hallazgos en relación con el ingreso a las instalaciones de la Unidad Nacional de protección - Sede Américas. Realizado el análisis de información recopilada de manera visual como herramienta de recolección de datos se logra evidenciar:

- Las personas que ingresan a las instalaciones de la Unidad Nacional de protección-Sede Américas no son plenamente identificados, se afirma ya que los vigilantes no conocen a todo el personal operativo y/o administrativo y solo con observar el carné que se presenta no se puede identificar al funcionario.
- Los tiempos de demora en el ingreso de los funcionarios presenta retrasos de más de 5 min en algunos casos.

- Se presenta cuellos de botellas en el ingreso y salida de los funcionarios ya que los elementos de deben pasar por un mismo scanner y la anotación de entrada y salida de los elementos electrónicos los realiza la misma persona.
- El personal externo presenta demoras de más de 20 min para realizar el ingreso a las instalaciones.
- No se tiene control de que cantidad de personas se encuentran al interior de las instalaciones de la Unidad Nacional de Protección- Sede Américas.
- No se tiene control de la hora de ingreso y salida de las personas que hacen presencia en las instalaciones

Cotejando y relacionando cada una de las preguntas que se realizaron en la encuesta como recolección de información y análisis acerca de las falencias que se presentan a la entrada de las instalaciones de la Unidad Nacional de protección se logra evidenciar:

- Aproximadamente el 97% de la población encuestada hace presencia por lo menos más de dos veces por semana a las instalaciones, lo que indica que hay frecuencia de personal que realiza en el ingreso.
- Mas del 90% de los encuestados afirman que los equipos utilizados actualmente por la empresa de vigilancia no son los indicados para la revisión que se realiza en la entrada de las instalaciones
- El 95% de las personas encuestadas afirman que los tiempos empleados para el ingreso a las instalaciones de la Unidad Nacional de Protección – Sede Américas, son demorados, afectando las labores que realizan en la entidad.
- El 87% de los encuestados consideran que no existen estándares mínimos actualmente en cuestión de seguridad para ingresar a las instalaciones de la Unidad Nacional de Protección – Sede Américas.
- Los encuestados no están de acuerdo con la forma en que se lleva actualmente el proceso de ingreso a las instalaciones.
- El personal considera que la Unidad Nacional de Protección necesita dispositivos electrónicos adicionales para realizar un control de acceso acorde a las instalaciones y seguridad de sus empleados.

- Del personal encuestado más del 95% indican que es necesario tener un control de acceso de seguridad por medio de autenticación del personal que ingresa a las instalaciones de la Unidad nacional de Protección.

Por las observaciones mencionadas anteriormente la entidad no cuenta con la identificación pertinente del personal que ingresa a las instalaciones de la Unidad Nacional de Protección- Sede Américas, por lo cual se ve la necesidad de diseñar un control de acceso peatonal que permita solucionar cada una de las inconformidades descritas.

Con el fin de poder definir la mejor solución para el diseño del sistema de control de acceso peatonal para la subdirección de seguridad y protección, realizamos un comparativo de los distintos dispositivos de identificación con el fin de evaluar sus características a nivel de fiabilidad, seguridad, costos entre otros (Ver tabla figura 26)

Dispositivos de identificación de personas

Características	Tipo de dispositivo de identificación			
	Huella	**Facial**	**Iris**	**Geometría mano**
Facilidad de uso	Alta	Alta	Media	Alta
Fiabilidad	Muy alta	Alta	Muy alta	Alta
Aceptación	Alta	Muy alta	Media	Alta
Prevención de ataque	Alta	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Alta
Costo	Bajo	Medio	Alto	Alto

Figura 26. Comparativo de dispositivos Elaboración Propia (2023)

Luego de evaluar los diferentes sistemas de identificación de personas se tomó la determinación de utilizar los dispositivos de identificación facial, ya que ofrecen un grado de seguridad alto, otros de los factores claves para la decisión fue que no es necesario tener contacto físico con el dispositivo lo cual minimiza los riesgos de infecciones.

Con el fin de utilizar el dispositivo de reconocimiento facial de mayores beneficios para la Subdirección de Seguridad y Protección vamos a evaluar algunos modelos como son los siguientes:

Figura 27. Lector Facial FACESTATION F2, Bioentrada. (2023)

Pricipales caracteristicas de **Suprema FaceStation F2** MultiModal (Bioentrada, 2023)

Es un terminal multimodal de fusión con un rendimiento de reconocimiento facial inigualable. con la precisión de autenticación excepcional y el rendimiento antispoofing logrado por la tecnología fusión única de Suprema.

El mejor multimodal de su clase con varias credenciales al ofrecer opciones de credenciales de cara, huellas dactilares, tarjetas y acceso móvil, FaceStation F2 es el mejor dispositivo multimodal de su clase en la industria. También admite tarjetas de acceso de doble frecuencia, tarjetas de acceso móvil basadas en NFC y BLE, así como Template on Card que permite la autenticación a través de datos biométricos almacenados en tarjetas.

Algoritmo de inteligencia artificial basado en aprendizaje profundo aplicado para la detección de rostros / huellas dactilares en vivo.

- Rendimiento facial inigualable
- El mejor dispositivo multimodal de su clase
- Solución sin contacto para la nueva normalidad
- Seguridad robusta del dispositivo y cifrado de datos

Fusión Matching

La tecnología fusión Matching de Suprema combina el reconocimiento facial e infrarrojos con un algoritmo de aprendizaje profundo único para lograr una precisión de autenticación excepcional y el mejor rendimiento anti-spoofing de la industria.

Tasa de aceptación falsa (FAR) de 1 en 10 mil millones.

Solución sin contacto para nuevos estándares de seguridad e higiene FaceStation F2 satisface las necesidades del mundo pospandémico con funciones como la inscripción remota de usuarios, la detección de usuarios sin máscaras y el reconocimiento facial de los usuarios que

usan máscaras. Cuando se combina con Suprema Thermal Camera, FaceStation F2 puede identificar personas con temperatura de piel elevada.

Figura 28. ProFAC, Zkteco. (2023)

ProFAC es una terminal de control de acceso con tecnología de reconocimiento facial y lector RFID. Con el más reciente algoritmo ZKFACE v7.0 de alta velocidad, equipada con un veloz procesador de 1.2 GHz, la verificación de usuarios es extremadamente rápida. El ProFAC puede almacenar hasta 4.000 plantillas faciales (1:1) o 2.000 (1: N) y 10.000 tarjetas RFID. Es compatible con paneles de acceso de terceros mediante la salida Wiegand y soporta la conexión de cerradura eléctrica, alarma, timbre y sensor de puerta. (ZKTeco-Colombia-Control-de-Acceso-ProFAC-Ficha-Tecnica, 2023)

Figura 29. Lector facial DS-K1T341AMF, Hikvision (2023)

La terminal de reconocimiento facial Hikvision DS-K1T341AMF es un tipo de dispositivo de control de acceso para el reconocimiento facial que es principalmente aplicado en sistemas de control de acceso de seguridad, como centros logísticos, aeropuertos, campus universitarios, centrales de alarma, viviendas.

El terminal cuenta con el algoritmo de reconocimiento de rostros más avanzado del mundo, más rápido que cualquier otro y más seguro debido a su algoritmo patentando imposible de falsificar. (Hikvision, 2023)

Comparación de las principales características. (Ver Tabla)

Característica	Zkteco ProFAC	Suprema FaceStation F2	HIKVISION DS-K1T341AMF
Protección	N/A	IP65	IP65
Capacidad de rostros	4,000	100,000	1,500
Velocidad de autenticación	< 0,5 sec	< 0,5 sec	< 0,2 sec
Credenciales	Facial, tarjeta, contraseña	Facial, NFC, BLE, tarjetas	Facial, tarjeta
CPU	1,2 GHz Dual Core	1,8 GHz Dual Core	N/A
Memoria	128MB	16GB Flash + 2GB	N/A
Certificaciones	CE, FCC, RoHS	CE, FCC, KC, RoHS, REACH, WEEE	CE, FCC, RoHS
Comunicación	Wiegand, Ethernet	Wiegand, RS-485, Ethernet	Wiegand, RS-485, Ethernet

Figura 30. Comparación de características Fuente Propia (2022)

Una vez evaluados algunos de los modelos disponibles en el mercado de los cuales nos centramos en 3 de ellos, decidimos elegir el lector F2 de la marca suprema ya que este lector no solo permite, tener identificación facial si no otros tipos lo cual permite adaptarse mejor a cualquier requerimiento futuro. Permitiendo incluso combinar dos tipos de identificación, esto permite que el nivel de seguridad sea más fiable.

El algoritmo que utiliza este fabricante permite identificar personas por su rostro en condiciones adversas como por ejemplo zona con baja iluminación.

Otras características importantes para destacar es que cuenta con encriptación de datos y con inteligencia artificial que no permite engañar el reconocimiento con fotos o videos de un rostro.

Evaluación de sistemas de control de acceso

BioStar 2 es una plataforma de seguridad abierta e integrada basada en la web que proporciona una funcionalidad completa para el control de acceso, las programaciones y el soporte. Debido a su estructura modular y flexible, la plataforma soporta el SDK de dispositivos BioStar 2, que se utiliza para integrar terminales Suprema en sistemas de terceros, y la API web, que se utiliza para integrar la funcionalidad de la plataforma BioStar 2 en sistemas de terceros. Además, en relación con la era del móvil, la aplicación móvil BioStar 2 está diseñada para permitirle controlar remotamente la plataforma BioStar 2 y también una plataforma para obtener una tarjeta móvil que puede utilizarse para el acceso.

Las principales características son:

- **Ingeniería de sistemas personalizados**: Es compatible con sistemas centralizados y distribuidos y, por lo tanto, puede proporcionar un excelente sistema
- **Compatibilidad de la integración del sistema**: Admite plataformas de integración basadas en web api e integración de hardware basada en SDK (dispositivo BioStar API 2 y BioStar 2 SDK)
- **Control remoto y tarjetas móviles:** Proporciona registro de usuario, alarma en tiempo real y control de puertos en la aplicación móvil BioStar 2 y también es compatible con la autenticación de tarjetas móviles

- **Solución flexible para la programación y gestión de llegadas:** Puede definir varias reglas de trabajo y crear informes de programación y asistencia personalizados, así como ver la programación de tareas y establecer turnos
- **Solución óptima de control de acceso**: Brinda soporte para todas las características de control de acceso: puertas, ascensores, control de zonas, mapa gráfico, autenticación en servidores, registros de video, registros de imágenes y registro de auditoría.
- **Ciberseguridad:** Encripta todos los datos de una persona que pueden ser rastreados. Certificación ISO 27001 e ISO 27701 para la información del sistema de administración seguridad
- **Gestión de visitantes + Soporte de registro de video:** Gestiona las aplicaciones de visitantes y emite/revoca los derechos de acceso de visitantes. Monitorea los eventos grabados con el NVR y cámaras IP en los puntos de entrada. (SUPREMA-ASB-BS2-ES-REV05, 2023)

Access Management System (AMS) BOSCH

Es un sistema de control de acceso que se puede utilizar como aplicación independiente o integrado con otros sistemas, como Bosch Video Management System (BVMS). • Como sistema independiente cuenta con un visor de mapas y de alarmas fácil de usar para realizar una evaluación rápida de todos los dispositivos y las entradas en las instalaciones.

Como sistema integrado, permite al operador de un sistema de gestión de vídeo realizar tareas relacionadas con las puertas, como verificar ID mediante vídeo, conceder y denegar el acceso o desactivar puertas. AMS combina la resistencia, el rendimiento y las características de los productos de control de acceso de gama alta con una interfaz de usuario moderna que facilita la instalación y configuración. La gama de dispositivos de control de acceso de Bosch disponibles se puede analizar e integrar fácilmente. La privacidad de los datos y la seguridad de TI es vanguardista para cumplir con las normas de protección de datos más recientes.

Las principales características del AMS son las siguientes:

- Software fácil de usar, escalable y resistente con interfaz gráfica de usuario (GUI) intuitiva y moderna.

- Integración de funciones de terceros, como horario y asistencia, y otros sistemas de RRHH mediante API
- Integración con BVMS y otros sistemas de gestión de vídeo
- Integración con los paneles de control de intrusión de la serie B y G
- Compatibilidad con el protocolo abierto de dispositivos supervisados (canal seguro OSDPv2) para la comunicación cifrada bidireccional entre la lectora y el controlador
- Base de datos y comunicaciones cifradas en todas las etapas
- Adecuado para oficinas y edificios gubernamentales, instituciones educativas, hospitales, etc.
- Administra hasta: − 400 divisiones − 10.000 puertas − 200.000 titulares de tarjetas − 40 estaciones cliente concurrentes. (BOSCH, Access Management System V3.0, 2021)

Comparación de sistemas

Características	BioStar 2 SUPREMA	Access profesional BOSCH
Capacitas de lectores	1,000	20,000
Capacidad de registros	2048	200,000
Cifrado de información	SI	SI
Integración con otros sistemas	CCTV	CCTV, Intrusión
API	SI	SI
Control asistencia de tiempo	SI	SI

Compatibilidad Mobile Card	SI	SI
Control Visitantes	SI	SI
Combinación de autenticación	SI	SI

Figura 31. Comparación de sistemas de control de acceso Fuente Propia (2023)

Luego del análisis de estos dos sistemas de control de acceso que tomamos de muestra, nos decidimos para este diseño por el AMS del fabricante BOSCH, ya que este sistema tiene unas mayores capacidades pensando en el crecimiento que pueda llegar a tener la subdirección de seguridad y protección. Este sistema nos permitirá utilizarlo para futuros requerimientos debido a su integración con los distintos sistemas de seguridad.

Descripción del diseño de acceso peatonal

Para este diseño nos decidimos por el lector facial F2 acompañado de un sistema de control de acceso AMS del fabricante Bosch, para completar el diseño se deberán agregar paneles de acceso AMC que son los compatibles con el software de control de acceso AMS y 2 tornos medio cuerpo y 1 torno para discapacitados. (PRO, 2023)

A continuación, se describen el panel y los tornos

Torniquete: Se utilizarán para el diseño 2 torniquetes medio cuerpo de la marca accesspro Modelo XT-500 los cuales tienen un diseño para alto tráfico permitiendo el paso de 25 personas por minutos, las medidas de los torniquetes se muestran en la figura 20:

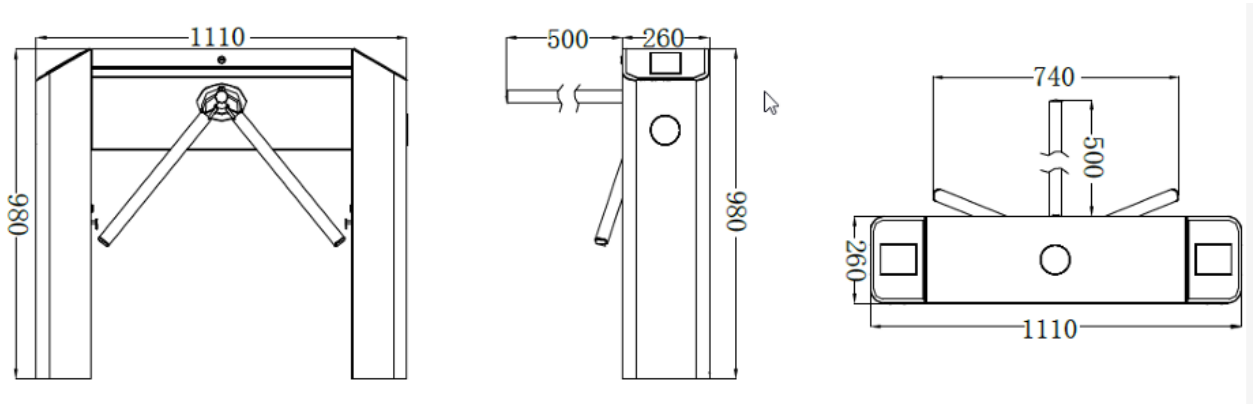


Figura 32. Dimensiones torniquete. Torniquete XT5000 (2023)

Para el torniquete de discapacitados se utilizará el del fabricante CAME con referencia 705EN1, este tiene las siguientes dimensiones ver figura 21: (TD-1302-0041_2_705_E_N1_TECHNICAL_SPECIFICATIONS, 2023)

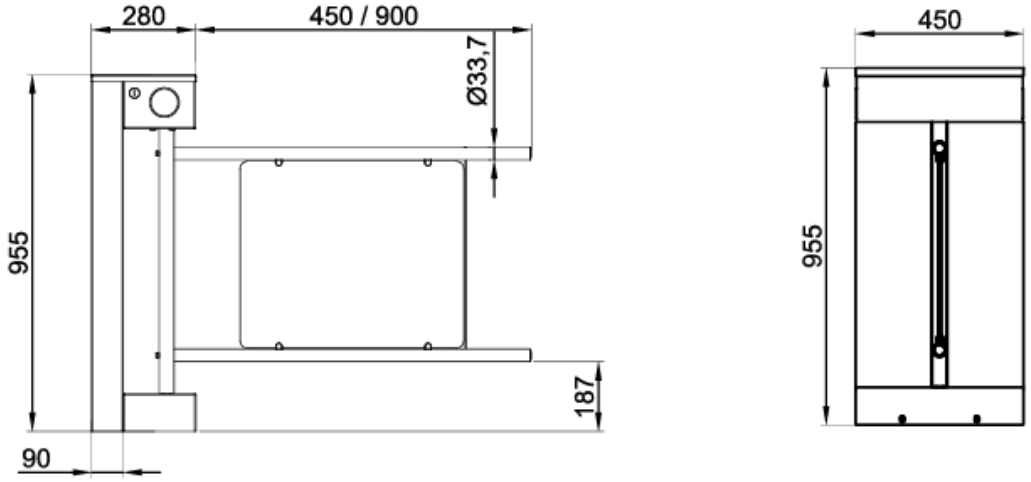


Figura 33. Medidas torno discapacitados.705 SPECIFICATIONS (2023)

Panel de control de acceso

Para este diseño vamos a utilizar los AMC de Bosch para los cuales vamos a describir las características de funcionamiento

Características de funcionamiento

– Administrador de acceso inteligente para 1 ... 4 entradas (por ejemplo, puertas, dobles puertas de seguridad, barreras)
– La dirección del host puede establecerse mediante un conmutador deslizante DIL
– Cuatro posibles interfaces de host configurables:
    – Ethernet
    – RS-485 2 cables
    – RS-485 4 cables
    – RS-232
– Interfaces de la lectora
    – cuatro interfaces Wiegand
– Ocho salidas de relé
    – sin tensión, fuente de alimentación externa (modo en seco)
    – alimentación mediante fuente de alimentación interna (modo húmedo)
– Ocho entradas análogas con fuente de alimentación interna
– Batería independiente SRAM y reloj en tiempo real (RTC)
– Compact Flash enchufable de 64 MB a (1024 MB
– Velocidad de transferencia de la interfaz de host de RS485: 38,4 kBit/s
– Velocidad de transferencia de la interfaz de host de RS232: 38,4 kBit/s
– Velocidad de transferencia de la interfaz de host de Ethernet: 10/100 Mbit/s
– Velocidad de transferencia a la interfaz de ampliación: 9,6 kBit/s
– Autorregulación de la conmutación transmisión/recepción
– Fuente de alimentación: 10 V a 30 Vdc, máx. 5 A
– Contacto antisabotaje para cubiertas internas y externas. (BOSCH, AMC2-4W.book, 2023)

Los lectores faciales deben ser conectados en los puertos señalados en la figura 22

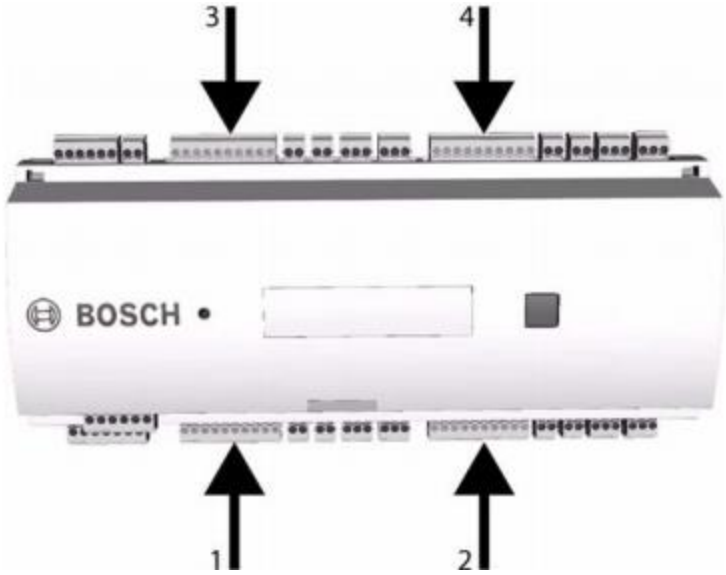


Figura 34. Conexión puertos wiegand. BOSCH, AMC2.book, (2023)

Instructivos de control de acceso a las instalaciones de la Unidad Nacional de Proteccion – Sede Américas

Propósito

Describir las forma, normas y mecanismos detallados para que los funcionarios, visitantes y todo el personal que ingrese a las instalaciones de la Unidad Nacional de Proteccion – Sede Américas, cuenten con la debida autorización, como medida para salvaguardar la integridad de las personas y la seguridad de las instalaciones.

Aplicación

Documento aplicable para el control de acceso al personal administrativo, operativo, personal externo.

Definiciones

Seguridad: Funcionamiento del sistema integrado de previsión de riesgos y capacidad de mantenimiento de apoyo.

Control de acceso: El control de acceso está diseñado para controlar quién tiene acceso a Zonas, o Determinadas Aéreas.

Personal externo: Visitante, pasante, contratista o funcionario ajeno a la unidad nacional de Protección – Sede Américas.

Se procede a describen los procesos que se realizaran cada vez que un usuario requiera ingresar a la Unidad Nacional de Protección -sede Américas

Instrucción

Registro de usuario administrativo o funcionario de la Unidad Nacional de Protección.

Procedimiento y descripción de la actividad

1- Presentar el documento de identificación: se inicia con la presentación de documento e identificación de la persona. de la cual se valida el numero de cedula, si ya es funcionario registrado o es primer registro
2- Se valida el rol (visitante o directivo SESP): Se valida si el número de cedula es de un registro nuevo
3- Se ingresan los datos: Se decepcionan datos, como nombres y apellidos, numero de cedula, correo electrónico, numero de contacto, área o dependencia en la cual labora, nombre del coordinador, si es de planta (indicar número de resolución de nombramiento) o contratista (indicar numero de contrato, fecha de inicio y finalización del mismo)
4- Toma del registro facial: Toma de capture facial de todos los ángulos.
5- Almacenamiento en la base de datos del software AMS: Los datos anteriores son almacenados en la base de datos del todo el personal registrado, el registro debe ser único por persona.

A continuación, se describe el procedimiento en el flujograma correspondiente al registro del funcionario de la Unidad Nacional de Protección.

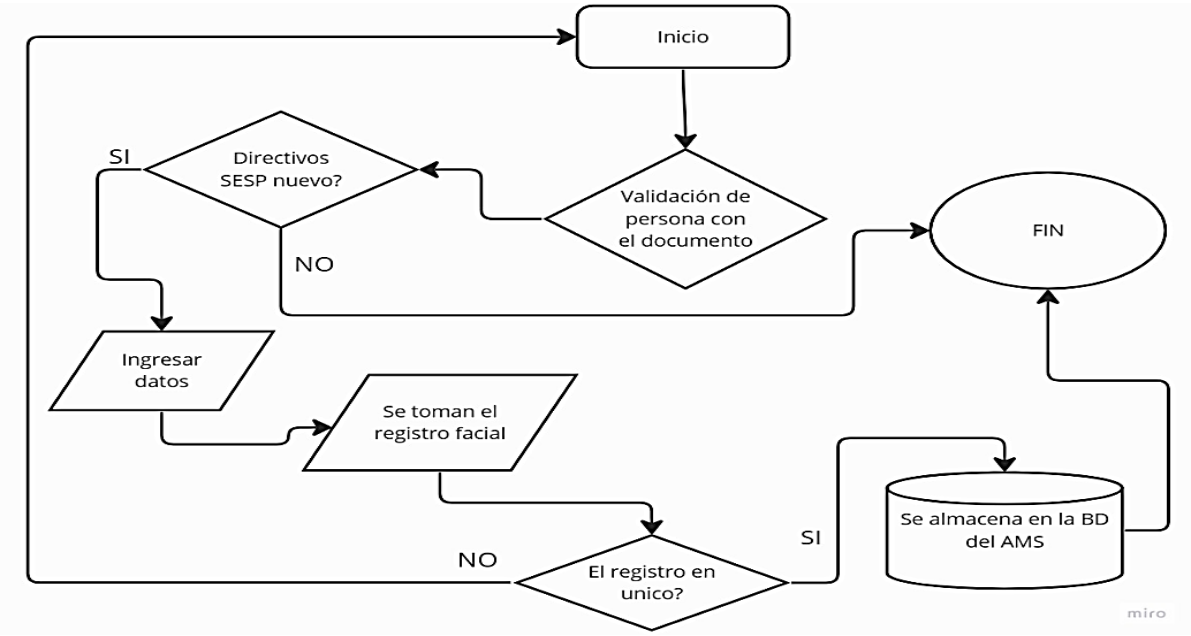


Figura 35. Flujo para directivos

Registro de usuario personal visitante que realiza ingreso a la Unidad Nacional de Protección.
Procedimiento y descripción de la actividad

1- Presentar Documento de identificación: se inicia con la presentación de documento e identificación de la persona.

2- Se validad si tiene autorización de ingreso: Si tiene cita o autorización se valida el número de cedula.

3- Verificar si ya está creado en la base de datos: Se valida si ya está registrado o es primer registro.

4- Crear o asignar el permiso de ingreso: Se decepcionan datos, como nombres y apellidos, numero de cedula, correo electrónico, numero de contacto, área o dependencia el cual visita, nombre del coordinador que da el ingreso, asunto al cual ingresa.

5- Toma del registro facial: Toma de capture facial de todos los ángulos.

6- Almacenamiento en la base de datos del software AMS: Los datos anteriores son almacenados en la base de datos del todo el personal registrado, el registro debe ser único por persona.

Descripción el procedimiento en el flujograma correspondiente al registro del personal visitante en las instalaciones de la Unidad Nacional de Protección – Sede Américas.

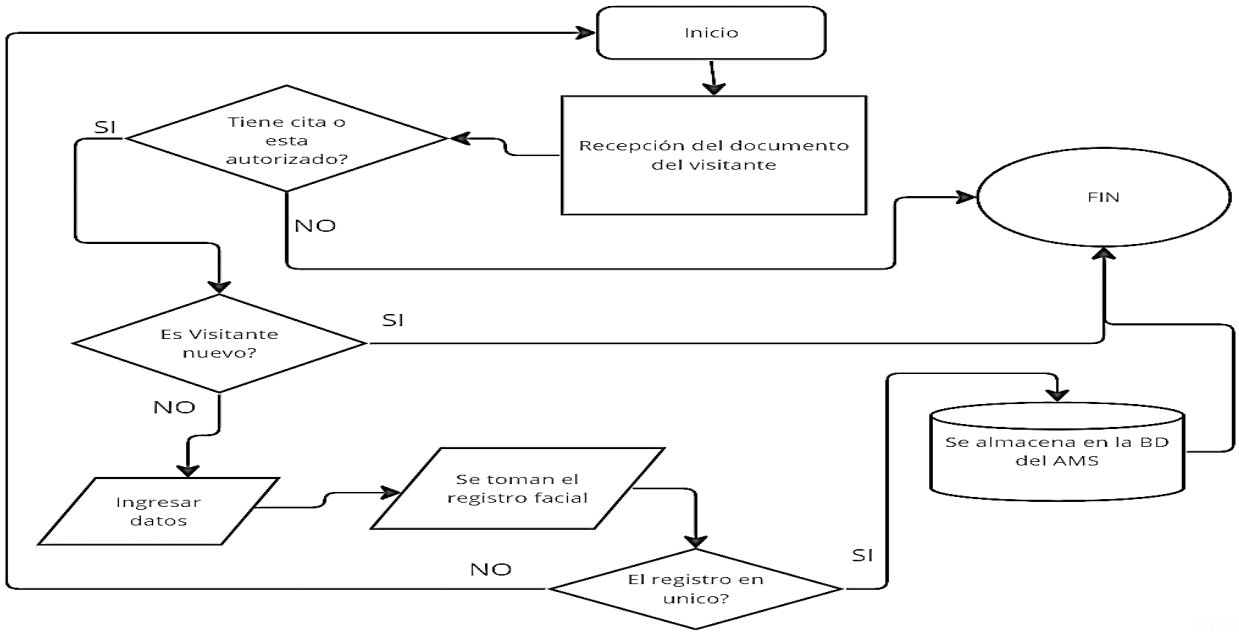


Figura 36. Flujo para visitantes

Diseño del sistema de control de acceso de las instalaciones de la Unidad Nacional de Protección – Sede Américas.
Una vez establecido el diseño y la referencia de los equipos necesarios, procedemos a ilustrar la opción del sistema de control de acceso, visualizando las conexiones y su funcionalidad con la finalidad de interpretar el diseño propuesto.

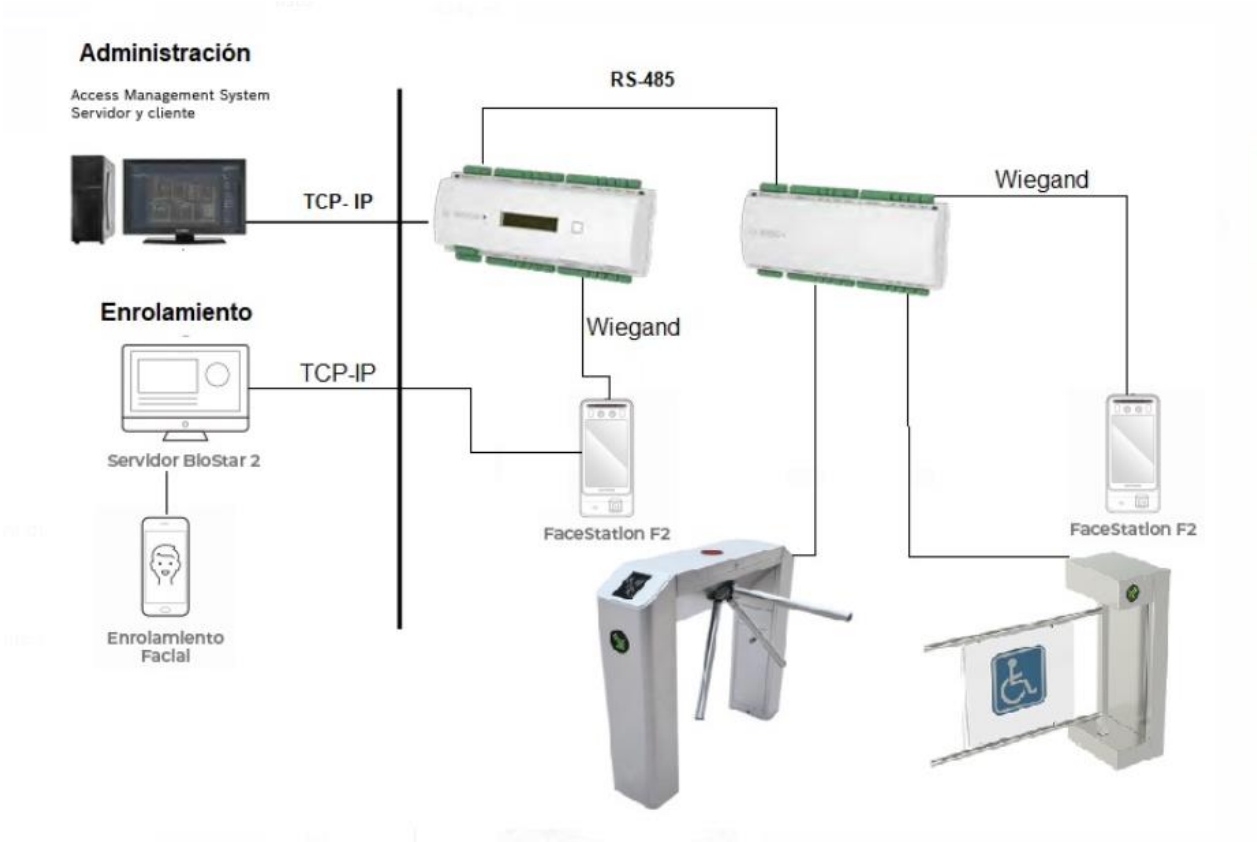


Figura 37. Esquema de la conexión

9. Conclusiones

Se puede observar que el método de ingreso que se está usando actualmente en la Unidad Nacional de Protección no es el apropiado debido a que realiza de forma manual lo cual causa tardanzas en el ingreso e inseguridad.

En el proceso de caracterización de falencias de la presente investigación se logra evidenciar que en la Unidad Nacional de protección – Sede Américas, presenta diferentes falencias al momento del ingreso de las personas al interior de las instalaciones , para esta actividad se usaron herramientas de recolección de información como los son la entrevista y método de observación, donde se realizó la tabulación de los datos obtenidos para posteriormente realizar su análisis, de igual modo se realizó análisis de los datos obtenidos

por medio visual, los cuales se obtuvieron observando el procedimiento que realiza los vigilantes en el ingreso.

En el diseño de esta solución se tuvieron en cuenta muchas factores como nivel de integración, compatibilidad y ante todo la seguridad de la información es por esto que se decidió trabajar con el sistema Access Management System (AMS) BOSCH, considerándose la opción más apropiada para el diseño propuesto en la Unidad Nacional de Proteccion. Por otro lado, el sistema es compatibles con muchos dispositivos electrónicos que permitirán aumentar la seguridad al momento de ingresar a las instalaciones.

Durante la investigación que realizamos para determinar la mejor opción para dar solución a la problemática que se tiene para el ingreso a las instalaciones de la Unidad Nacional de Protección – Sede Americas, nos dimos cuenta que diariamente el flujo de personas que visita dicha sede es muy elevada, es por esta razón que se tomó la decisión de proponer el sistema AMS de Bosch ya que este sistema permite crecer de manera fácil lo cual permitirá satisfacer futuras necesidades, también combinamos el sistema AMS de Bosch con los biométricos faciales de la marca Suprema F2 ya que con estos tenemos la opción de identificar personas sin contacto físico con el dispositivo, lo cual permite tener mejores medidas de salubridad ya que luego de la pandemia COVID19, nos enseño tanto a las organizaciones como las personas que debemos esta muy atentos de la higiene.

10. Recomendaciones

1- En caso de realizar la ejecución del diseño propuesto se recomienda realizar con personal calificado o una compañía que tenga experiencia comprobada en este tipo de proyecto.

2- Es necesario que, para tomar una decisión de la implementación del sistema de control de acceso, se realice un buen análisis de los beneficios que traerá y no tomar las decisiones solo por el costo.

3- Si se implementa el sistema de control de acceso se recomienda realizar análisis constante del proceso de ingreso con el fin de identificar nuevas necesidades y adaptar el sistema para cubrirlas y así no comprometer su seguridad.

4- El sistema de control de acceso no pretende reemplazar el personal que se encuentra apoyando actividades de ingreso, por el contrario, lo que busca es mejorar el proceso a nivel de eficiencia y seguridad.

11. Bibliografía

(s.f.). Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30030379

1341, L. (30 de 07 de 2009). *Función publica.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913

1581, L. e. (17 de 10 de 2012). *Funcion publica.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

(10 de 09 de 2022). Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30030379

356, D. l. (11 de 02 de 1994). *Funcion publica.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=1341

675, L. (03 de 08 de 2001). Obtenido de https://www.sic.gov.co/sites/default/files/normatividad/Ley_675_2001.pdf

Ahmed Raad Al-Sudania , Wanlei Zhoub , Bo Liuc . (2021). *Detecting Unauthorized RFID.* Obtenido de [Imagen]: https://link.springer.com/article/10.1007/s12008-021-00760-6#Sec28

Ahmed Raad Al-Sudania, W. Z. (28 de 07 de 2021). *Biometric applications in education.* Obtenido de https://link.springer.com/article/10.1007/s12008-021-00760-6#Sec28

Bioentrada. (06 de 04 de 2023). *Bioentrada.com.* Obtenido de Bioentrada.com: https://www.bioentrada.com/product-page/FSF2-ODB

BOSCH. (22 de 01 de 2021). *Access Management System V3.0*. Obtenido de Access Management System V3.0: https://resources-boschsecurity-cdn.azureedge.net/public/documents/Access_Management_Sy_Data_sheet_esES_78880158347.pdf

BOSCH. (06 de 04 de 2023). *AMC2-4W.book.* Obtenido de AMC2-4W.book: http://resource.boschsecurity.com/documents/AMC2_Installation_Guide_esES_1354092299.pdf

CASTRO , P. C. (Diciembre de 2018). *IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO BIOMÉTRICO ZK - X7 POR MEDIO DE HUELLA DACTILAR EN EL LABORATORIO DE HARDWARE DE LA CARRERA DE*

INGENIERÍA EN COMPUTACIÓN Y REDES. Recuperado el 13 de 10 de 2022, de Repositorio Digital Unesum: http://repositorio.unesum.edu.ec/handle/53000/1487

César Tolosa Borja, Á. G. (2019). *Funcionamiento.* Obtenido de [Imagen]: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

César Tolosa Borja, Á. G. (2019). *Geometría de la mano.* Obtenido de [Imagen]: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

César Tolosa Borja, Á. G. (2019). *Identificando patrones.* Obtenido de [Imagen]: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

César Tolosa Borja, Á. G. (2019). *Realce de la Huella.* Obtenido de [Imagen]: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

César Tolosa Borja, Á. G. (s.f.). *Sistemas Biométricos*. Recuperado el 13 de 10 de 2022, de Documentación Biometria: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

César Tolosa Borja, Á. G. (s.f.). *Sistemas Biométricos*. Recuperado el 14 de 10 de 2022, de Sistemas Biométricos: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf

DECRETO299, M. D. (23 de 02 de 2017). *Sistema Único de Información Normativa,*. Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?id=30030379

ETICSA. (s.f.). Obtenido de https://www.eticsa.cl/seguridad-electronica/#:~:text=El%20concepto%20de%20seguridad%20electr%C3%B3nica,cualquier%20plan%20general%20de%20seguridad.

Eumed.net. (05 de Noviembre de 2022). *Enciclopedia Virtual*. Obtenido de Enciclopedia Virtual: https://www.eumed.net/tesis-doctorales/2012/mirm/enfoque_cualitativo.html#:~:text=4.3.2%20Enfoque%20cualitativo,acuerdo%20con%20las%20personas%20implicadas.

FERNANDEZ ORTIZ, G. W. (2019). *Sistema de control de acceso basado en la tecnología de autenticación biométrica por huella dactilar para el instituto técnico comercial la paz*. Recuperado el 15 de 10 de 2022, de Repositorio Institucional de la UTP: https://repositorio.utp.edu.pe/handle/20.500.12867/2648

Graciani, M. (s.f.). *Bioinformatica*. Recuperado el 14 de 10 de 2022, de Trabajos biometria: https://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Bio metria/Trabajo%20Biometria.pdf

H. Tawfeeq, Q., HY Al-Noori, A., & N. Jabir, A. (25 de 09 de 2020). *Scientific & Academic Publishing.* Obtenido de Scientific & Academic Publishing: http://article.sapub.org/10.5923.j.bioinformatics.20201001.01.html#Sec1

Hikvision. (06 de 04 de 2023). *Biometrico Hikvision DS-K1T341AMF facial*. Obtenido de Biometrico Hikvision DS-K1T341AMF facial: https://hikvision.lat/productos/lector-biometrico-facial-hikvision-ds-k1t341amf.html

Maersa. (2022). *Funcionamiento y rendimiento.* Obtenido de [Imagen]: https://www.maersa.com.mx/historia.html

Maersa. (2022). *Funcionamiento y rendimiento.* Obtenido de [Imagen]: https://www.maersa.com.mx/historia.html

Maersa. (s.f.). *Historia de la Biometría y la Huella Digital*. Recuperado el 13 de 10 de 2022, de Maersa: https://www.maersa.com.mx/historia.html

Marcela Hernandez-de-Menendez, Ruben Morales-Menendez, Carlos A. Escobar & Jorge Arinez. (28 de 07 de 2021). *SpringerLink*. Recuperado el 17 de 10 de 2022, de SpringerLink: https://link.springer.com/article/10.1007/s12008-021-00760-6#Sec28

Nec. (2022). *Mecanismo del reconocimiento del iris.* Obtenido de [Imagen]: https://co.nec.com/es_CO/global/solutions/biometrics/iris/index.html

Nec. (2022). *Reconocimiento de Iris.* Obtenido de [Imagen]: https://co.nec.com/es_CO/global/solutions/biometrics/iris/index.html

Nec. (s.f.). *Reconocimiento de Iris*. Recuperado el 14 de 10 de 2022, de Biometrics: https://co.nec.com/es_CO/global/solutions/biometrics/iris/index.html

PRO, A. (06 de 04 de 2023). *Torniquete XT5000*. Obtenido de Torniquete XT5000: https://ftp3.syscom.mx/usuarios/ftp/2015/07/23/9887c/xt5000.pdf

PROTECCIÓN, U. N. (2022). *UNIDAD NACIONAL DE PROTECCIÓN*. Obtenido de https://www.unp.gov.co/la-unp/que-hacemos/

PROTECCIÓN, U. N. (2022). *UNIDAD NACIONAL DE PROTECCIÓN*. Obtenido de https://www.unp.gov.co/la-unp/quienes-somos/

Protelec. (s.f.). *Qué es un control de acceso y para que sirve*. Recuperado el 13 de 10 de 2022, de Protelec: https://www.protelec.eu/que-es-un-control-de-acceso-y-para-que-sirve

Qusay H. Tawfeeq, Ahmed H. Y. Al-Noori, Amjed N. Jabir. (2020). *Scientific & Academic Publishing*. Recuperado el 17 de 10 de 2022, de Scientific & Academic Publishing: http://article.sapub.org/10.5923.j.bioinformatics.20201001.01.html#Sec1

San Martín Guillén, E. M. (2019). *Diseño e implementación de un sistema de control de acceso por Biometría*. Recuperado el 14 de 10 de 2022, de Repositorio Institucional de la UTP: https://repositorio.utp.edu.pe/handle/20.500.12867/2648

SUPREMA-ASB-BS2-ES-REV05. (06 de 04 de 2023). *SUPREMA-ASB-BS2-ES-REV05*. Obtenido de SUPREMA-ASB-BS2-ES-REV05: https://www.siasa.com/productos/documentos/Software%20BioStar%202%20Suprema%20Esp.pdf

TD-1302-0041_2_705_E_N1_TECHNICAL_SPECIFICATIONS. (06 de 04 de 2023). *TD-1302-0041_2_705_E_N1_TECHNICAL_SPECIFICATIONS*. Obtenido de TD-1302-0041_2_705_E_N1_TECHNICAL_SPECIFICATIONS: https://ftp3.syscom.mx/usuarios/scorrea/CA/CAME/705EN1/TD-1302-0041_2_705_E_N1_TECHNICAL_SPECIFICATIONS.pdf

Tomala, O. (05 de 11 de 2022). *Tipos de investigación*. Obtenido de Tipos de investigación: https://sites.google.com/site/misitioweboswaldotomala2016/tipos-de-investigacion

VIATEK, G. (s.f.). Obtenido de https://grupoviatek.com/sistemas-de-control-de-acceso/

ZKTeco-Colombia-Control-de-Acceso-ProFAC-Ficha-Tecnica. (06 de 04 de 2023). *ZKTeco-Colombia-Control-de-Acceso-ProFAC-Ficha-Tecnica*. Obtenido de ZKTeco-Colombia-Control-de-Acceso-ProFAC-Ficha-Tecnica: https://zktecocolombia.com/wp-content/uploads/2021/05/ZKTeco-Colombia-Control-de-Acceso-ProFAC-Ficha-Tecnica.pdf

CORPORACIÓN UNIVERSITARIA
UNITEC

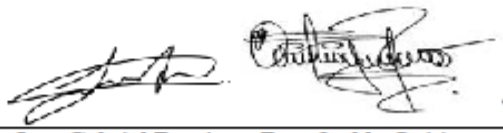
Por intermedio del presente documento en mi calidad de autor o titular de los derechos de propiedad intelectual de la obra que adjunto, titulada DISEÑO DE UN CONTROL DE ACCESO PEATONAL PARA EL INGRESO A LAS INSTALACIONES DE LA SUBDIRECCION ESPECIALIZADA DE SEGURIDAD Y PROTECCION ADSCRITA A LA UNIDAD NACIONAL DE PROTECCIÓN EN BOGOTÁ -SEDE AMERICAS, autorizo a la Corporación universitaria Unitec para que utilice en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador o titular de la obra objeto del presente documento.

La presente autorización se da sin restricción de tiempo, ni territorio y de manera gratuita. Entiendo que puedo solicitar a la Corporación universitaria Unitec retirar mi obra en cualquier momento tanto de los repositorios como del catálogo si así lo decido.

La presente autorización se otorga de manera no exclusiva, y la misma no implica transferencia de mis derechos patrimoniales en favor de la Corporación universitaria Unitec, por lo que podré utilizar y explotar la obra de la manera que mejor considere. La presente autorización no implica la cesión de los derechos morales y la Corporación universitaria Unitec los reconocerá y velará por el respeto a los mismos.

La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato electrónico, y en general para cualquier formato conocido o por conocer. Manifiesto que la obra objeto de la presente autorización es original y la realicé sin violar o usurpar derechos de autor de terceros, por lo tanto, la obra es de mi exclusiva autoría o tengo la titularidad sobre la misma. En caso de presentarse cualquier reclamación o por acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión asumiré toda la responsabilidad, y saldré en defensa de los derechos aquí autorizados para todos los efectos la Corporación universitaria Unitec actúa como un tercero de buena fe. La sesión otorgada se ajusta a lo que establece la ley 23 de 1982.

Para constancia de lo expresado anteriormente firmo, como aparece a continuación.

Firma 

Nombre Jose Gabriel Ramirez, Jhon freddy Quitian, Edgar Daniel Soto
CC. 1.111.768.066, 80.826.515, 1.094.280.616

LINK DEL VIDEO DE SUSTENTACIÓN PUBLICADO EN YOUTUBE

https://youtu.be/KqapLRbii4M