# UNIVERSIDAD PRIVADA DE TACNA
## FACULTAD DE INGENIERÍA
## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

**TESIS**

# "USO DE SISTEMA DE RECONOCIMIENTO DE IRIS BASADO EN DEEP LEARNING PARA LA IDENTIFICACIÓN HUMANA EN EL CONTROL DE ACCESO AL ÁREA DE TESORERÍA DEL GOBIERNO REGIONAL DE TACNA - TACNA 2020"

**PARA OPTAR:**

**TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS**

**PRESENTADO POR:**

**Bach. LUIS EDUARDO MAMANI BEDREGAL**

**TACNA – PERÚ**

**2022**

# UNIVERSIDAD PRIVADA DE TACNA
## FACULTAD DE INGENIERÍA
## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

## TESIS

# "USO DE SISTEMA DE RECONOCIMIENTO DE IRIS BASADO EN DEEP LEARNING PARA LA IDENTIFICACIÓN HUMANA EN EL CONTROL DE ACCESO AL ÁREA DE TESORERÍA DEL GOBIERNO REGIONAL DE TACNA - TACNA 2020"

**Tesis sustentada y aprobada el 06 de setiembre de 2022; estando el jurado calificador integrado por:**

| | | |
|---|---|---|
| **PRESIDENTE** | **:** | **Mtro. ENRIQUE FELIX LANCHIPA VALENCIA** |
| **SECRETARIO** | **:** | **Mag. PATRICK JOSÉ CUADROS QUIROGA** |
| **VOCAL** | **:** | **Mag. RICARDO EDUARDO VALCÁRCEL ALVARADO** |
| **ASESOR** | **:** | **M.Sc. HUGO MANUEL BARRAZA VIZCARRA** |

## DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Luis Eduardo Mamani Bedregal, en calidad de bachiller de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de la Universidad Privada de Tacna, identificado con DNI 72463957 declaro bajo juramento que:

1. Soy el autor de la tesis titulada: *Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna - Tacna 2020* la misma que presento para optar el *Título Profesional de Ingeniero de Sistemas*.
2. La tesis no ha sido plagiada ni total ni parcialmente, habiéndose respetado las normas internacionales de citas y referencias para las fuentes consultadas.
3. La tesis presentada no atenta contra derechos de terceros.
4. La tesis no ha sido publicada ni presentada anteriormente para obtener algún grado académico o título profesional.
5. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados, ni copiados.

Por lo expuesto, mediante la presente asumo frente a *La Universidad* cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido de la tesis, así como por los derechos sobre la obra.

En consecuencia, me hago responsable, frente a *La Universidad* y a terceros, de cualquier daño que pudiera ocasionar, por el incumplimiento de lo declarado o que pudiera encontrar como causa del trabajo presentado, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello en favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontrasen causa en el contenido de la tesis.

De identificarse fraude, piratería, plagio, falsificación o que la obra haya sido publicada anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Privada de Tacna.

Tacna, 21 de abril de 2022

Luis Eduardo Mamani Bedregal
DNI: 72463957

## DEDICATORIA

A Dios por la vida y salud que me ha brindado.

A mis padres Daniel y Marisol, y hermanos Luis Daniel y Cecilia, por todo su apoyo incondicional, del cual estaré eternamente muy agradecido.

A mis abuelos y demás familiares, en especial a mi abuelo Dionicio y mi abuela Luisa, que me cuidan desde el cielo.

Luis Eduardo Mamani Bedregal

## AGRADECIMIENTO

Agradecer a Dios por cuidarme ante cualquier adversidad, y brindarme la salud para poder concluir mi tesis. Así mismo, agradecer a mis padres Daniel y Marisol, hermanos Luis Daniel y Cecilia, y demás familiares, a quienes amo con todo mi ser, ya que, sin la ayuda de ellos, no hubiera sido capaz de concluir con el presente proyecto.

Agradecer al M.Sc. Hugo Manuel Barraza Vizcarra, por todo el apoyo brindado para el desarrollo de la presente tesis: asesoramiento, tiempo, dedicación, y espíritu de investigación.

Agradecer a los trabajadores del Gobierno Regional de Tacna que, de alguna manera, manifestaron el apoyo solicitado para el acceso y despliegue del proyecto en sus instalaciones.

Por último, agradecer a los docentes de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Privada de Tacna, por toda la formación profesional brindada durante mis 5 años de estudios, años donde aprendí el valor e impacto de ser un Ingeniero de Sistemas dentro de la sociedad.

Luis Eduardo Mamani Bedregal

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# ÍNDICE DE ANEXOS

## RESUMEN

Se realizó la investigación mediante el uso de un Sistema de Reconocimiento de Iris para controlar el acceso al área de Tesorería del Gobierno Regional de Tacna, específicamente a uno de sus ambientes ubicado en la sede Hipólito Unanue, donde se almacenan documentos vitales e importantes, cuyo proceso de control de acceso presenta deficiencias en aspectos de seguridad que ponen en riesgo la integridad de los activos del espacio físico en cuestión. Para ello, se estableció el objetivo general de determinar el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning. Así mismo, se establecieron objetivos específicos: a) Determinar el nivel de seguridad en la identificación del personal durante el proceso de control de acceso, b) Determinar el nivel de seguridad en la autenticación del personal identificado durante el proceso de control de acceso, c) Determinar el nivel de seguridad en la autorización del acceso del personal autenticado durante el proceso de control de acceso, d) Determinar el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el proceso de control de acceso. La investigación tomó como población y muestra a 15 personas pertenecientes al área de Tesorería. Se aplicó una investigación de tipo Aplicada y de nivel Experimental, y se utilizó el instrumento Prueba de Comprobación mediante la técnica Ficha de Evaluación para la obtención de la información correspondiente. Para el proceso estadístico, la información se analizó y consolidó mediante técnicas estadísticas, permitiendo la discusión de resultados según la contrastación de hipótesis mediante la prueba T de muestras relacionadas, aplicada a la variable dependiente. Esto permitió la obtención de resultados positivos, procediendo con la aceptación de la hipótesis general y específicas alternas, donde el Sistema de Reconocimiento de Iris mejoró significativamente los niveles de seguridad para el proceso de control de acceso, con un p-valor de 0,000 < 0,05 (nivel de significancia). Por ende, se concluyó que los niveles de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, mejoró en un 98,5% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning. Finalmente, se indicaron diversas recomendaciones y mejoras significativas a desarrollar en futuras investigaciones, para lograr el 100% de nivel de seguridad mediante el uso de la solución tecnológica propuesta.

**Palabras clave:** Aprendizaje profundo; biometría; control de acceso; reconocimiento de iris; redes neuronales convolucionales; sistemas cognitivos

## ABSTRACT

The investigation was carried out through the use of an Iris Recognition System to control access to the Tesorería area of the Gobierno Regional de Tacna, specifically to one of its environments located in the Hipólito Unanue headquarters, where vital and important documents are stored, whose access control process presents deficiencies in security aspects that put at risk the integrity of the assets of the physical space in question. To this end, the general objective of determining the level of security for the process of access control to the warehouse of the Tesorería area was established with the implementation of an Iris Recognition System based on Deep Learning. Likewise, specific objectives were established: a) Determine the level of security in the identification of personnel during the access control process, b) Determine the level of security in the authentication of personnel identified during the access control process, c) Determine the level of security in the authorization of access of authenticated personnel during the access control process, d) Determine the level of security in the access traceability record of personnel during the access control process. The research took as population and shows 15 people belonging to the Tesorería area. Applied and experimental level research was applied, and the Verification Test instrument was used using the Evaluation Sheet technique to obtain the corresponding information. For the statistical process, the information was analyzed and consolidated using statistical techniques, allowing the discussion of results according to the hypothesis testing by the T test of related samples, applied to the dependent variable. This allowed the obtaining of positive results, proceeding with the acceptance of the general hypothesis and specific alternatives, where the Iris Recognition System significantly improved the security levels for the access control process, with a p-value of 0,000 < 0,05 (significance level). Therefore, it was concluded that the security levels for the process of access control to the warehouse of the Tesorería area of the Gobierno Regional de Tacna, improved by 98,5% through the use of the Iris Recognition System based on Deep Learning. Finally, several recommendations and significant improvements were indicated to be developed in future research, to achieve 100% level of security through the use of the proposed technological solution.

**Keywords:** Deep learning; biometrics; access control; iris recognition; convolutional neural networks; cognitive systems

# INTRODUCCIÓN

La seguridad es uno de los temas más importantes dentro de múltiples enfoques. Alrededor del mundo, hablar de seguridad, sea digital o física, es tratar con conceptos y criterios que algunas personas o empresas tienen mayor conocimiento, ya que apuestan más por seguridad mediante herramientas tecnológicas para poder salvaguardar sus bienes tangibles e intangibles, evitando pérdidas importantes; como también existen personas o empresas que aún confían en procesos mecánicos debido a múltiples factores, como el bajo nivel de conocimiento sobre seguridad y tecnología, políticas inadecuadas, o el simple hecho de desinterés en transformación tecnológica.

La preocupación más importante para las personas o empresas, es mantener a salvo sus bienes más valiosos, ya que, cualquier pérdida, ocasiona gastos de restauración, pérdida de información documental o digital, manipulación de información, hasta incluso pérdidas irreparables. Por ende, tener un control de acceso eficiente y eficaz a estos bienes, debe ser altamente prioritario.

Como es visto en diversos estudios realizados a nivel mundial y nacional relacionado al control de acceso a determinados ambientes para la protección de bienes, existen diferentes autores que manifiestan un mismo problema, de los cuales, se encuentran las investigaciones de Montaña (2017) y Pérez (2018), donde ambos autores manifiestan que, la consecuencia de no contar con un control de acceso más eficiente, y al no realizar cuidadosamente la inspección de personas que ingresan o salen de algún lugar protegido, surgen problemas tales como el ingreso de personas no autorizadas y pérdida de bienes, generando gastos de restauración o robo de información.

Dentro del ámbito local, el Gobierno Regional de Tacna cuenta con protocolos de seguridad para acceder a sus instalaciones, pero no existe un control de acceso a instalaciones internas. El área de Tesorería perteneciente a la misma entidad pública, solo cuenta con llaves de acceso (llave de cerrojo) para el acceso correspondiente a sus ambientes. Esta área es muy importante para la entidad, ya que cuenta con un almacén ubicado en la sede Hipólito Unanue de la misma entidad, donde se encuentran documentos vitales, necesarios para procesos internos o de auditoría. Por ello, la implementación de un sistema inteligente de control de acceso debe permitir restringir el almacén de manera eficiente, donde solo personal autorizado cuente con permisos de acceso, que toda actividad sea registrada para procesos de informes o auditoría por parte de seguridad, y que, algo que la persona puede producir, sea la única llave de

acceso, evitando el uso de llaves, tarjetas, y el recordatorio de contraseñas, códigos, entre otros.

Es importante señalar que, para el desarrollo del objetivo de investigación, se ha desarrollado un sistema de reconocimiento que usa el iris humano como llave de paso, aplicando aprendizaje profundo (Deep Learning) para diferenciar y reconocer a cada persona. Se incluyen múltiples servicios, donde cada uno realiza una acción específica para el correcto funcionamiento del proyecto. Así mismo, se ha desarrollado un lector biométrico de iris que sirve como base para la estructura del sistema biométrico, controlando la puerta de acceso.

La presente investigación cuenta con diferentes capítulos, de los cuales se describen a continuación:

a. Capítulo I, se describe la problemática que da inicio a la investigación, definiendo la formulación general del problema, y problemas específicos. Además, se da a conocer la justificación e importancia de la investigación, como también los objetivos e hipótesis, generales y específicos.
b. Capítulo II, se presentan los antecedentes de la investigación, estudiados a nivel internacional, nacional y local. Se presentan las bases teóricas de las variables de investigación, y la definición de términos.
c. Capítulo III, se describe el tipo y diseño de investigación, la población y muestra a ser estudiada, las variables de investigación (dependiente, independiente, interviniente), las técnicas e instrumentos de recolección de información, y el procesamiento y análisis de los datos obtenidos.
d. Capítulo IV, se presentan los resultados obtenidos a partir del uso de un sistema de reconocimiento de iris para el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, validando y determinando el nivel de seguridad alcanzado.
e. Capítulo V, se discuten los resultados obtenidos en base al nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
f. Finalmente, se presentan las conclusiones de la investigación, y recomendaciones. Del mismo modo, se presentan las referencias bibliográficas y anexos, utilizados para el desarrollo de la presente investigación.

# CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

## 1.1. Descripción del problema

El problema de seguridad en el control de acceso a áreas o zonas de una empresa no es un problema reciente. Este problema se ha manifestado desde hace varios años en organizaciones empresariales, donde la información y bienes, tales como documentos, registros, archivos, equipos costosos, entre otros, son de gran importancia para las empresas. Los métodos de seguridad, en ese entonces, eran los más comunes, como el de asignar a un personal de seguridad que resguarde los activos de la empresa. Cuando una empresa mantiene información vital y/o bienes que son muy importantes, estos deben ser salvaguardados por diferentes políticas de seguridad. Pero, estas políticas no eran las más eficientes para mantener los bienes de la empresa en su total seguridad.

El proceso de identificación de una persona debe ser considerado paso esencial para la correcta otorgación de los respectivos accesos a las diversas áreas cruciales de una empresa. Según la identificación proporcionada, el personal de seguridad puede, o no, otorgar el acceso correspondiente según los permisos que la persona posee en sus credenciales. Pero, el personal de seguridad, al no contar con un registro automatizado del personal autorizado, se basa en el reconocimiento visual, obviando si la persona aún posee los permisos de acceder a ciertas áreas, o en el peor de los casos, al no contar con alguna herramienta que valide las credenciales de la persona, estas credenciales pueden ser falsificadas por el mismo personal de la empresa. Esto es una preocupación por parte de las empresas, debido a que los controles deben ser fuertes y rigurosos para proteger la totalidad de los bienes tangibles e intangibles de cualquier caso de robo o ataque.

En el mundo existen diversos casos donde el problema de seguridad, en controles de accesos a una entidad o a zonas internas de la misma entidad, no son las más óptimas, caso observado por Montaña (2017), en la Universidad Libre Sede Bosque Popular, en Colombia, donde el no contar con un control de acceso más eficiente, y no seguir correctamente el protocolo de seguridad impuesto por la universidad, donde se debe inspeccionar rigurosamente a las personas que ingresan o salen de la casa de estudio, surgen inconvenientes tales como el ingreso de personas pertenecientes o no a la universidad, cuellos de botella debido a horas de mayor concurrencia, dando como resultado la pérdida de bienes de los mismos estudiantes y de la propia universidad.

El problema observado por Pérez (2018), en una empresa de electro servicios, en Ecuador, donde el control de acceso a las instalaciones de la empresa lo realizan guardias de seguridad, sin implementar políticas esenciales de seguridad en el proceso de identificación, solo de forma visual, trabajando con cámaras de seguridad en diferentes zonas de la empresa. Así mismo, al no tener un control de seguridad, los mismos guardias son los que otorgan los accesos, provocando que personas puedan ingresar sin autorización. Este problema ha provocado que la empresa sea víctima de robos en varias oportunidades, generando gastos de restauración de los materiales sustraídos por personas ajenas o por los mismos empleados de la empresa.

Los problemas de seguridad en controles de accesos en el Perú no son ajenos a la realidad problemática de los demás países. San Martín (2019), observa el problema de seguridad en una empresa de mantenimiento de maquinarias, donde la preocupación por resguardar los materiales y herramientas de trabajo de la empresa no es del todo considerada. En la empresa transitan varias personas, entre empleadores y terceros, donde no existen cámaras de seguridad en zonas internas de la misma empresa, solo en la entrada principal de acceso. No existe la presencia de personal de seguridad que realice el control de los accesos a las áreas donde se encuentran materiales costosos, considerando solo el uso de candados como medida de seguridad.

El problema observado por Bravo (2019), en la Universidad Tecnológica del Perú, donde el ingreso de los estudiantes a la universidad se realiza mediante métodos tradicionales, presentando identificación física al personal de seguridad, dando como resultado la demora en el ingreso por la aglomeración del personal y estudiantes, y el disgusto por parte de la comunidad universitaria. El ingreso de personas ajenas a la universidad por la falta de un control robusto de accesos, mejores políticas y herramientas de seguridad que ayuden al personal de seguridad cumplir con una excelente labor, resulta en hechos que infringen las normas de la casa de estudio, y atentan contra la integridad del personal y estudiantes de la universidad.

La constante evolución y avance de la tecnología, permite implementar mejores técnicas y protocolos de seguridad, procesos automatizados donde la persona solo se encargue de la supervisión y del monitoreo. Estas mejoras proporcionan alivio a las empresas, ya que los ayudan a tener un mayor control en su seguridad: sistemas inteligentes que proporcionan mayor confiabilidad, políticas basadas en marcos de trabajo, procesos que no necesitan demasiada acción humana. Todas estas novedades, lamentablemente, no son, en su totalidad, asequibles por empresas o entidades pequeñas, donde no existe el presupuesto dirigido a la seguridad, o por el simple hecho de que los dueños o gerentes desconocen de las tecnologías actuales.

Las empresas más experimentadas se enfocan en proteger sus bienes con recelo, en cambio, empresas que recién salen al mercado, se enfocan en la meta de vender y ganar más, dejando a un lado el tema de seguridad, punto importante para cualquier empresa. Estas empresas, al no dar mucha importancia al tema de seguridad, solo cuentan con procedimientos de seguridad tradicionales, sin uso de alguna tecnología, es decir, utilizan como control de seguridad al personal de seguridad para el acceso a áreas internas, donde este personal puede ser de la misma empresa o contratación por terceros. Este método de control de seguridad, que tiene como actor principal a un personal de seguridad, no es un método del todo seguro.

Hoy en día, existen sistemas biométricos de reconocimiento que permiten a las empresas tener un mejor control de seguridad, ya que la llave de paso es alguna parte del propio cuerpo humano. Métodos tradicionales de seguridad utilizan llaves de paso tales como tarjetas, carnés, fotochecks, llaves, entre otros. Los métodos biométricos utilizan partes del cuerpo humano, como lo es la huella, palma de la mano, retina, rostro, iris, entre otros. Sistemas modernos de biometría para el reconocimiento humano son desarrollados basados en inteligencia artificial, donde la visión computacional y arquitecturas de redes neuronales juegan un rol importante para la detección y clasificación de características de alto y bajo nivel de las personas.

El Gobierno Regional de Tacna cuenta con políticas de seguridad, en la cual, para ingresar a sus sedes, es necesario registrarse (mediante DNI, nombre y apellido) o identificarse ante el personal que custodia la entrada, indicando el objetivo de su visita. Para el caso de los trabajadores, cada trabajador presenta su fotocheck al personal de seguridad para poder tener acceso a las respectivas sedes según su lugar de trabajo. El acceso a las instalaciones internas de la institución, por parte del personal que labora en el lugar, se realiza mediante la solicitud de la llave de acceso al personal de seguridad (llave de cerrojo). Por otro lado, los visitantes tienen libre circulación solo hasta los lugares de atención al público (cada área cuenta con un lugar de atención al público).

Las áreas o ambientes del Gobierno Regional de Tacna solo están resguardadas por una llave física, sin implementar alguna tecnología eficaz de seguridad, como lo son los sistemas biométricos, y en vez de este método de seguridad, la entidad solo cuenta con personal de seguridad, que habitualmente resguardan solo la entrada a la institución, no a cada área o ambiente. Los trabajadores que laboran en las diferentes áreas o ambientes, son responsables del ingreso de personas externas al lugar. Así mismo, los mismos trabajadores son los encargados de cerrar las puertas cuando salen a almorzar o es horario de salida. Esto es un gran problema debido al hecho de que la

persona puede no cerrar correctamente la puerta de acceso, o en el peor de los casos, se extravíe la llave de acceso, siendo tomada por otra persona que no tiene alguna relación con el lugar. Una vez que el personal cierra las puertas, la llave es retornada al personal de seguridad. El personal de seguridad, con poca frecuencia, se cerciora de que las puertas se encuentren cerradas del todo, pero este proceso no es muy confiable debido a que el personal de seguridad solo realiza una revisión no exhaustiva o visual del lugar.

El área de Tesorería es el área encargada de manejar el movimiento de dinero que realiza la entidad. Esta área es muy susceptible de que ocurran hechos delictivos, como pérdida de dinero, pérdida de documentación, manipulación de información, u otro relacionado. El área de Tesorería cuenta con 15 personas, cada una de ellas con diferentes responsabilidades de trabajo. El acceso a esta área, u otra subárea de la misma, solo es de personal autorizado, pero permiten el acceso a otros trabajadores mediante autorización del jefe de área o de algún encargado.

El área de Tesorería cuenta con un ambiente en la sede Hipólito Unanue de la misma entidad, donde almacenan documentos u otros activos importantes, ya que sirven ante cualquier proceso interno o auditoría interna/externa. El ambiente es resguardado solo por llave, método mecánico no seguro para salvaguardar documentos tan importantes y esenciales, sin supervisión del mismo personal de seguridad, o alguna herramienta que custodie la puerta de acceso. Este método de control de acceso tradicional no permite la identificación individual del propio trabajador, ni verificación de la persona que ingresa al espacio físico, siendo este uno de los tantos problemas que aqueja al área de Tesorería, ya que, no saben con certeza si la persona a quien se le entregó la llave de acceso es quien ingresa al almacén.

El personal, al usar la llave de acceso para acceder al almacén, siente una gran preocupación debido a que necesitan mantener la llave a salvo, y transportarlo hasta el espacio físico para poder ingresar dentro de él. Durante este proceso, han acontecido situaciones donde la llave física se extravió, y el área responsable ha tenido que solicitar la copia de la llave a Seguridad, sin realizar cambio de cerradura. Cabe señalar que, la llave, actualmente, es resguardada por el mismo jefe o encargado del área de Tesorería (y no por el personal de Seguridad), el cual, es un inadecuado lineamiento de seguridad adoptado por los mismos trabajadores.

El proceso de acceso al almacén del área de Tesorería, es realizado de forma manual y hablada, sin tener algún registro de los accesos que se otorgan a las personas, ni registros que se deberían contemplar cuando una persona ingresa al espacio físico.

Del mismo modo, la propia entidad no manifiesta interés de implementar controles de acceso de seguridad a los diversos espacios físicos donde se almacenan activos importantes para la misma entidad, controles de accesos tales como: controles biométricos u otra forma alterna de control (tarjetas, PINs, entre otros).

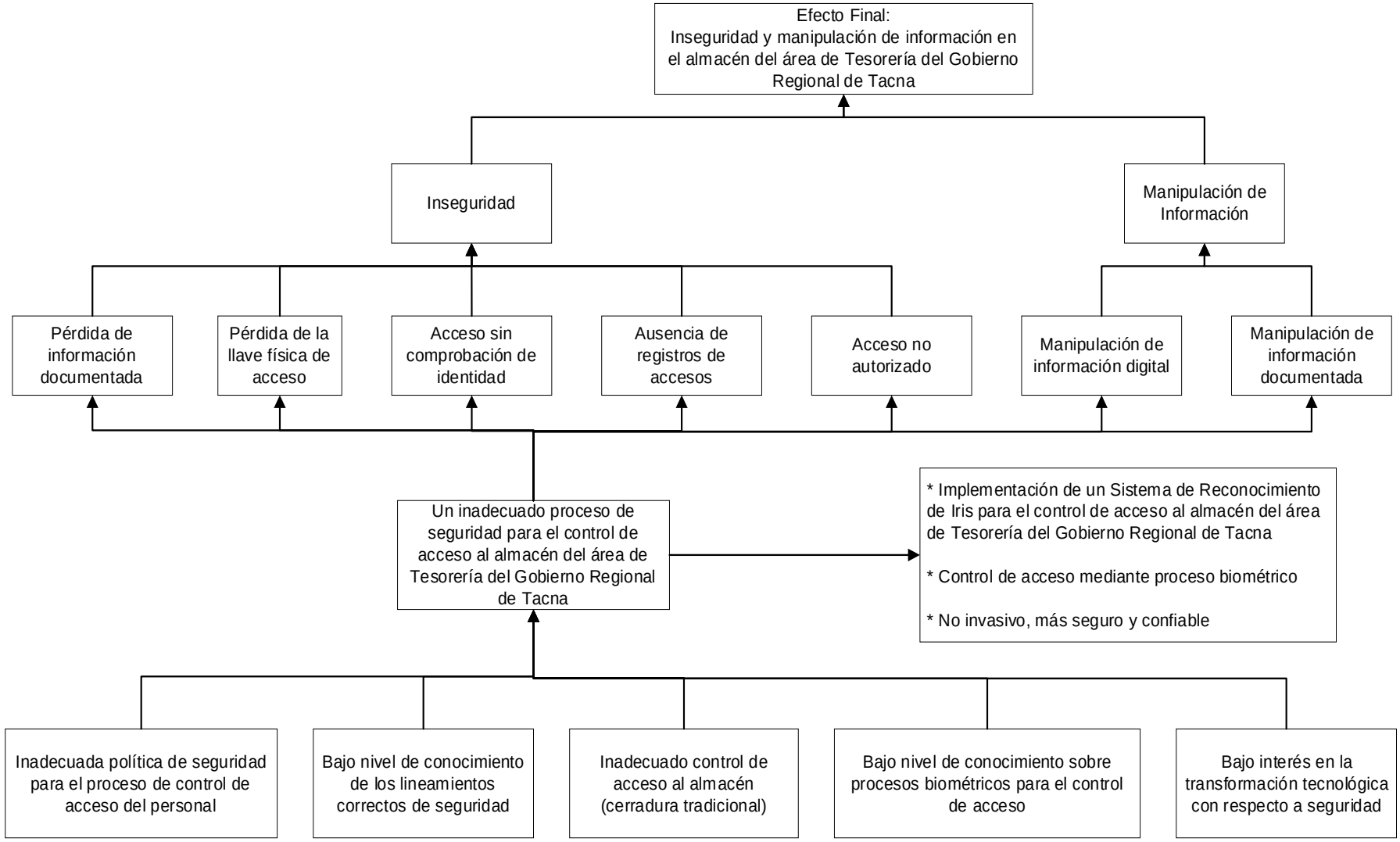
Debido a las características bajas de seguridad implementadas por la entidad, el almacén del área de Tesorería tiene un alto riesgo de inseguridad, riesgo que preocupa a los mismos trabajadores del área, y al mismo personal de seguridad. Riesgos tales como la manipulación de información y pérdida de documentación, son hechos ocurridos (no muy frecuentes) en el ambiente problemático. Así mismo, la pérdida de la llave de acceso, la no comprobación de la identidad de la persona que accede al almacén, y la falta de responsabilidad de registrar los accesos otorgados al personal, son hechos que atentan contra la seguridad e integridad del espacio físico en cuestión.

Las empresas más grandes suelen tener, y usar, dispositivos biométricos para el control de acceso. El más común es el dispositivo de reconocimiento mediante la huella digital. Este dispositivo, junto con el reconocimiento de iris, son los dos más mejores métodos (no muy costosos) de seguridad para el cuidado de los bienes de la empresa. Pero el método de reconocimiento de iris está un paso más adelante que el método de huella digital, y esto se debe a los fallos y “huecos” de seguridad que existen en el método de huella digital, como, por ejemplo, el contacto directo con el lector biométrico puede provocar la suplantación de identidad. Por ende, el método de reconocimiento de iris es el más seguro, fiable, no invasivo, y no muy costoso, logrando proteger los bienes lógicos y físicos de una organización.

La Figura 1 muestra el Árbol de Problemas, que resume la problemática en la entidad investigada, donde se indican las causas por la acción de un deficiente proceso de control de acceso, las posibles o respectivas consecuencias ocasionadas por un incorrecto proceso de acceso de seguridad, y la solución que podría mejorar el nivel de seguridad en el acceso al almacén del área de Tesorería.

**Figura 1**

*Árbol de problemas*



## 1.2. Formulación del problema

### 1.2.1. Problema general

¿Cómo es el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020?

### 1.2.2. Problemas específicos

a. ¿Cómo es el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?
b. ¿Cómo es el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?
c. ¿Cómo es el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?
d. ¿Cómo es el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?

## 1.3. Justificación e importancia

La presente investigación se enfocará en la elaboración y uso de un sistema de reconocimiento biométrico, donde la llave de paso será el iris humano. El sistema de reconocimiento biométrico será elaborado en base a un sistema web, donde la tecnología para el frontend estará basada en React & Redux, la tecnología para el backend estará basada en C# .Net Core, y la tecnología para los microservicios estará basada en Python, utilizando contenedores para el despliegue de los respectivos proyectos. Para el almacenamiento de la información que manejará el sistema, estará bajo el motor de base de datos MySQL. Toda la información que es transferida entre el frontend, backend y microservicios, y durante el proceso de reconocimiento, será cifrada

y encriptada (encriptado punto a punto) para aumentar y mejorar el nivel de seguridad de todo el sistema de reconocimiento biométrico.

Como parte de los componentes electrónicos, se usará la plataforma electrónica Raspberry Pi, sirviendo como base para la estructura del sistema biométrico y para el control de la puerta de acceso al almacén del área de Tesorería. Esta plataforma comprenderá de conectores electrónicos y sensores, conectándose a electroimanes que controlan el abrir y cerrar de la puerta de acceso para permitir o no el ingreso de personas al ambiente protegido.

El proceso de detección, segmentación y reconocimiento del iris de las personas, se basará en el subcampo de Machine Learning: Deep Learning. Para la anotación manual del ojo, se usará LabelImg, desarrollado por Tzutalin (2015), y para la anotación manual del iris humano se usará Coco-Annotator, desarrollado por Brooks (2019). El resultado obtenido por la herramienta de anotación manual del ojo, será entrenado por YOLOv4, desarrollado por Bochkovskiy et al. (2020), y el resultado obtenido por la herramienta de anotación manual del iris humano, será entrenado por Detectron2, desarrollado por Wu et al. (2019), generando modelos de Deep Learning que detectarán y segmentarán las imágenes de iris de las personas. Las imágenes detectadas y segmentadas, pasarán por una red neuronal siamesa, construido sobre una arquitectura de red neuronal convolucional mediante el modelo entrenado por Boyd et al. (2020), modelo que servirá como extractor de características para la aplicación del enfoque de aprendizaje único (aprendizaje de una sola captura), para evitar el reentrenamiento de una red neuronal convolucional, y el uso de un mayor costo computacional (se considerará solo un iris de la persona, debido a que el iris es único para cada individuo).

Como ya expuesto en la descripción del problema, debido a las situaciones comunes que se presentan en una empresa o entidad en todo lo referido al tema de seguridad para otorgar accesos a áreas o zonas internas, las cuales no aplican o usan la tecnología como herramienta de ayuda en el control de seguridad, la presente investigación permitirá desarrollar un sistema de reconocimiento de iris para poder mejorar, con el uso de la tecnología, el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, otorgando un mayor nivel de seguridad y una mejor protección de los bienes tangibles e intangibles importantes de la entidad.

a. Desde el punto de vista científico; es importante conocer los beneficios y el alto nivel de seguridad que ofrece la biometría en diferentes enfoques, esto

debido a que, en el Perú, los estudios e investigaciones sobre el desarrollo de aplicaciones de biometría, aplicando inteligencia artificial, y más que todo, investigaciones enfocadas al reconocimiento biométrico mediante el iris humano, es casi nulo.

b. Desde el punto de vista económico; los sistemas de reconocimiento biométrico, al presentar un mayor control y manejo de la seguridad, ayudan a las empresas a proteger sus bienes importantes (tangibles e intangibles) con métodos referidos a la biometría, evitando pérdidas materiales, y, por ende, reduciendo costos de reposición y restauración.

La característica considerada importante en el mundo biométrico es el grado de diferencia que existe entre una persona y otra. Se estima que el patrón de similitud del iris entre dos personas es de 1 en $10^{78}$, es decir, el 0% de probabilidad. (Buitrago & Romero, 2018)

La Tabla 1 muestra la comparativa entre los tres procesos biométricos más utilizados para diferentes procesos o problemáticas, donde se indican ciertos aspectos que permiten diferenciar y evaluar cada método biométrico, según su unicidad, universalidad, persistencia en el tiempo, aceptabilidad, entre otros indicadores.

**Tabla 1**

*Comparativa de procesos biométricos más utilizados*

| Indicadores | Reconocimiento por Iris | Reconocimiento por Huella Dactilar | Reconocimiento Facial |
|---|---|---|---|
| Universalidad | Alto | Medio | Alto |
| Unicidad | Alto | Alto | Bajo |
| Permanencia | Alto | Alto | Medio |
| Coleccionismo | Medio | Medio | Alto |
| Desempeño | Alto | Alto | Bajo |
| Aceptabilidad | Alto | Medio | Alto |
| Resistencia al Fraude | Alto | Alto | Bajo |

*Nota*. Adaptado de Whitman & Mattord (2018).

## 1.4. Objetivos

### 1.4.1. Objetivo general

Determinar el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020.

### 1.4.2. Objetivos específicos

Para lograr el objetivo general de esta investigación, se describen los siguientes objetivos específicos con el fin de concretar el objetivo general planteado:

a. Determinar el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.
b. Determinar el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.
c. Determinar el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.
d. Determinar el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.

## 1.5. Hipótesis

Dado que, el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna tiene protocolos básicos de seguridad, este proceso es realizado de la forma tradicional, con el uso de llaves físicas (llaves de cerrojos) para el ingreso respectivo, permitiendo el ingreso de personas no autorizadas con intenciones negativas para la entidad.

Es probable que, la propuesta del uso de un Sistema de Reconocimiento de Iris basado en Deep Learning mejorará el nivel de seguridad para el proceso de control de

acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, en tiempo real.

### 1.5.1. Hipótesis general

El Sistema de Reconocimiento de Iris basado en Deep Learning mejora significativamente el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna – Tacna 2020.

### 1.5.2. Hipótesis específicas

a. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
b. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
c. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
d. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

# CAPÍTULO II: MARCO TEÓRICO

## 2.1. Antecedentes del estudio

Los temas de Reconocimiento de Iris y de Control de Acceso, son temas mundialmente estudiados e investigados, del cual podemos encontrar diversas fuentes y enfoques donde estos temas son tratados: tesis, papers, artículos científicos, libros, entre otros.

A continuación, se muestran diferentes estudios e investigaciones realizados a nivel internacional, nacional y local:

### 2.1.1. Internacional

- Tann et al. (2019), autores del artículo de investigación titulado “A Resource-Efficient Embedded Iris Recognition System Using Fully Convolutional Networks”, cuyo trabajo fue realizado en la Universidad de Brown, Estados Unidos, utilizando como población los conjuntos de datos de iris: CASIA Interval v4 y IITD. La población fue dividida en dos partes: 80% destinado al entrenamiento y validación de las imágenes de iris, y el 20% destinado al proceso de pruebas. Los autores dan a conocer que, la investigación tiene como finalidad la propuesta de un flujo de reconocimiento de iris de extremo a extremo de uso eficiente de los recursos, que consiste en la segmentación basada en FCN (Fully Convolutional Networks), ajuste de contorno, seguido de la codificación y normalización basados en los principios de Daugman. Así mismo, proponen una metodología de codiseño entre el hardware y software de tres pasos, que consiste en una exploración arquitectónica de FCN, cuantificación de precisión y aceleración de hardware. El modelo propuesto presenta un mejor rendimiento, requiriendo 50 veces menos FLOP por inferencia, mientras se logra una nueva precisión de segmentación del iris. El acelerador DFP (punto fijo dinámico) propuesto, alcanza una velocidad de hasta 8,3 veces más rápido, mientras se usa menos recursos (hasta un 15% menos).
- Y. H. Li et al. (2019), autores del artículo de investigación titulado “An Efficient and Robust Iris Segmentation Algorithm Using Deep Learning”, cuyo trabajo fue realizado en el Departamento de Ciencias Computacionales e Ingeniería Informática, en la Universidad Nacional Central, Taoyuan, Taiwan, utilizando como población el conjunto de datos de iris: CASIA-Iris-Thousand,

que contiene 20000 imágenes de iris de 1000 personas. La población fue dividida en dos partes: 12000 imágenes destinados al entrenamiento, 8000 imágenes destinados a las pruebas. Los autores dan a conocer que, la investigación tiene como finalidad la propuesta de un método de algoritmos combinados basados en el aprendizaje y en el borde para la segmentación del iris. Diseñan un modelo R-CNN más rápido, con tan solo seis capas para lograr la ubicación y clasificación del ojo humano. Con el uso de Faster R-CNN, la región de la pupila se localiza utilizando un modelo de mezcla gaussiana. Así mismo, utilizan un algoritmo de selección de punto límite para encontrar los puntos límite del limbo, donde el límite circular del limbo se construye usando los puntos límites encontrados. Los resultados experimentales demostraron que el método propuesto logró el 95,49% de precisión en el proceso de segmentación del iris.

- Ren et al. (2019), autores del artículo de investigación titulado “Alignment Free and Distortion Robust Iris Recognition”, cuyo trabajo fue realizado en la Universidad de China, Beijing, China, utilizando como población los conjuntos de datos de iris: ND-LG4000, CASIA V4-Lamp, CASIA-Iris-M1-S2. El conjunto de datos ND-LG4000 consta de 29986 imágenes de iris de 1352 personas, donde la cantidad de imágenes de entrenamiento se estableció en 15012, y la cantidad de imágenes de pruebas se estableció en 14974. El conjunto de datos CASIA V4-Lamp consta de 16212 imágenes de iris de 819 personas, donde la cantidad de imágenes de entrenamiento se estableció en 8115, y la cantidad de imágenes de pruebas se estableció en 8097. El conjunto de datos CASIA-Iris-M1-S2 consta de 12000 imágenes de iris de 200 personas, donde la cantidad de imágenes de entrenamiento se estableció en 6000, y la cantidad de imágenes de pruebas se estableció en 6000. Los autores dan a conocer que, la investigación tiene como finalidad la propuesta de una solución unificada de niveles de características, tanto para la alineación libre como para la distorsión del reconocimiento robusto del iris humano. Proponen un modelo de Deep Learning denominado AFINet (Alignment Free Iris Network), que utiliza un codificador VLAD (Vector de descriptores agregados localmente) llamado NetVLAD para desacoplar las correlaciones entre las representaciones locales y sus posiciones espaciales, y convoluciones deformables para superar la distorsión del iris. Los resultados experimentales demostraron que el modelo propuesto AFINet superó los métodos de reconocimiento de iris de última generación.

- Zheng et al. (2019), autores del artículo de investigación titulado “A Robust Iris Authentication System on GPU-Based Edge Devices using Multi-Modalities Learning Model”, cuyo trabajo fue realizado en la Universidad de Malasia, Malasia, utilizando como población el conjunto de datos de iris: UTiris, con un total de 1540 imágenes. Los autores dan a conocer que, la investigación tiene como finalidad la propuesta de un modelo de red neuronal de ajuste fino basado en el modelo de red neuronal Mask R-CNN e Inception V4, que integra todas las funciones de: detección, extracción y reconocimiento del iris, como un sistema de reconocimiento de iris. El marco propuesto presenta las características de escalabilidad y disponibilidad, aprendiendo durante su ejecución. El modelo propuesto ha sido entrenado con diferentes espectros de muestra, como son las bases de datos biométricas de iris de Longitud de Onda Visible (VW) e Infrarrojo (NIR). Los resultados experimentales demuestran que el modelo propuesto logra el 99,10% promedio de precisión.
- Lozej et al. (2019), autores del artículo de investigación titulado “Influence of Segmentation on Deep Iris Recognition Performance”, cuyo trabajo fue realizado en la Universidad de Liubliana, Eslovenia, utilizando como población los conjuntos de datos de iris: CASIA Thousand y SBVPI. El conjunto de datos CASIA Thousand consta de 20000 imágenes de iris de 1000 personas, donde la cantidad de imágenes para el entrenamiento se estableció en 14000, la cantidad de imágenes de validación se estableció en 4000, y la cantidad de imágenes de pruebas se estableció en 2000. El conjunto de datos SBVPI consta de 3708 imágenes de iris de 110 personas, donde la cantidad de imágenes para el entrenamiento se estableció en 1422, y la cantidad de imágenes de validación se estableció en 656. Se estableció un conjunto de datos de iris combinado entre ambos conjuntos de datos con el resto de las imágenes de iris. Los autores dan a conocer que, la investigación tiene como finalidad explicar la importancia de la segmentación del iris en el rendimiento de los modelos de aprendizaje profundo utilizando un pipeline simple de dos etapas que consiste en una segmentación y un paso de reconocimiento. Los resultados del experimento demuestran que, la precisión de la segmentación influye en el rendimiento del reconocimiento, donde el conjunto de datos, al ser de orígenes diferentes (conjunto de datos combinado de iris), se logra un mayor porcentaje de acierto con el proceso de segmentación: 98,91% a 100%.

- Proenca & Neves (2019), autores del artículo de investigación titulado “Segmentation-Less and Non-Holistic Deep-Learning Frameworks for Iris Recognition”, cuyo trabajo fue realizado en la Universidade da Beira Interior, Portugal, utilizando como población tres conjuntos de datos de iris: CASIA-4-Lamp, CASIA-4-Thousand, WVU. El conjunto de datos CASIA-4-Lamp consta de 822 imágenes. El conjunto de datos CASIA-4-Thousand consta de 2000 imágenes. El conjunto de datos WVU consta de 638 imágenes. Los autores dan a conocer que, la investigación tiene como finalidad la propuesta de un método de reconocimiento que dispensa las fases de segmentación del iris, detección de ruido y normalización. Se basaron en modelos de clasificación de Deep Learning para discriminar entre comparaciones genéticas y de imposición. Las normalizaciones del iris son transformadas a coordenadas polares, sin realizar el proceso de segmentación, considerando también la pupila. Los resultados del experimento demuestran que, para el conjunto de datos CASIA-Iris v4-Lamp, el porcentaje de acierto es de 99%; para el conjunto de datos CASIA-Iris V4-Thousand, el porcentaje de acierto es de 98,10%; para el conjunto de datos WVU, el porcentaje de acierto es de 96,90%. En comparación con otros modelos del estado del arte, el modelo propuesto presenta mayor porcentaje de acierto y menos tasa de error.
- Vargas (2016), autor de la tesis “Diseño de un Prototipo de Control de Acceso del Personal mediante Reconocimiento Facial en 3D para Empresas Públicas o Privadas”, cuyo trabajo fue realizado en Riobamba, Ecuador, utilizando como población a la Empresa Pública Cementera de Chimborazo EP (EPCE EP), y seis personas como muestra, de forma que, al hallar una media y comparar los resultados, éstos sean válidos y confiables. Utiliza como instrumento a encuestas, y el nivel de investigación es Experimental. El autor da a conocer que, la investigación tiene como finalidad diseñar un prototipo de control de acceso mediante reconocimiento facial para agilizar el proceso de acceso, porque para que una persona se registre, se demora en un promedio de 1 segundo, causando una demora en el ingreso debido a la aglomeración de personas. Con el desarrollo del sistema de control de acceso, se logró mejorar el tiempo de respuesta debido a la no aglomeración de las personas al ingresar a la entidad. Para la implementación del proyecto de investigación se utilizó una cámara Webcam Genius HD Facecam 1000x 1,3 Mpx Micrófono, una computadora Core i7, la plataforma de programación LabVIEW 2014 y la librería OpenCV Wrapper. Se notó la mejora en el tiempo que existe durante el proceso de autenticación en la zona de detección,

resultando 0,66 personas por segundo. En las pruebas dentro de un ambiente iluminado, se logró obtener niveles de aceptación mayores. Los resultados de la investigación demuestran que, el nivel de aprobación es de 90%, y la tasa de error es de 10%, según las estadísticas tabuladas.

### 2.1.2. Nacional

- Garfias (2018), autor de la tesis “Implementación de un Sistema Biométrico por Reconocimiento de Iris para el Registro y Control de Asistencia de los Internos en los Talleres del Establecimiento Penitenciario Ancón II”, cuyo trabajo fue realizado en la Universidad Nacional José María Arguedas, Apurímac, Perú, utilizando como población a los internos del establecimiento penitenciario Ancón II, considerando a 33 internos del taller de manualidades como muestra de investigación. Utiliza como instrumento a encuestas para obtener resultados de la implementación, y el diseño de experimentación es Cuasi – Experimental. El autor da a conocer que, la investigación tiene como finalidad la propuesta de un sistema de reconocimiento de iris para el control de asistencia de los internos del taller de manualidades, debido al problema observado en el trabajo que realiza el personal del INPE, donde se registra manualmente el control de asistencia y las horas de trabajo de los internos, siendo esta información vulnerable a alteraciones o pérdida. Para la implementación del proyecto se utilizó la solución Nano NXT, fabricado por la empresa Eyelock, para la lectura biométrica de los iris. Los resultados obtenidos dan a conocer que, la solución biométrica presentada ha mejorado significativamente el proceso de registro y control de asistencia, reduciendo el tiempo y mejorando la verificación de la identidad de los internos.
- Bravo (2019), autor de la tesis “Diseño e Implementación de un Sistema de Control de Acceso a los Campus de la Universidad Tecnológica del Perú - UTP”, cuyo trabajo fue realizado en la Universidad Tecnológica del Perú, Lima, Perú, utilizando como población a estudiantes de la misma universidad. Utiliza como instrumento a encuestas para obtener resultados del antes y después del sistema de control implementado, y el nivel de investigación es Experimental. El autor da a conocer que, la investigación tiene como finalidad la propuesta de una solución que permita optimizar y tecnificar el ingreso de los alumnos a las instalaciones de la casa de estudio, debido a los problemas observados por la falta de un proceso ágil de control de acceso, provocando demoras e insatisfacción de los estudiantes. Para la

implementación del proyecto se utilizó la tecnología NFC mediante tarjetas de identificación personalizadas, y el uso de molinetes instalados por un proveedor externo a la universidad. Se notó la mejora en el tiempo que existe durante el proceso de autenticación, ya que al sistema no le toma mucho tiempo en identificar a las personas. Los resultados de la investigación demuestran que, con la propuesta de investigación, se logró mejorar el flujo de alumnos a la universidad, tener un mayor control y reportes debido a las bitácoras de ingreso, prevención del ingreso de personas no pertenecientes a la universidad, y la reducción de hechos de suplantación y robos de identidad.

- San Martín (2019), autor de la tesis “Diseño e Implementación de un Sistema de Control de Acceso por Biometría”, cuyo trabajo fue realizado en Lima, Perú, utilizando como cantidad de población a la empresa PERÚ OFFSET EDITORES, y la cantidad de muestra al personal del área de mantenimiento de la empresa, siendo de cinco personas. Utiliza como instrumento a encuestas para obtener resultados del antes y después del sistema de control implementado, y el nivel de investigación es Experimental. El autor da a conocer que, la investigación tiene como finalidad la propuesta de un sistema con el objetivo de mejorar el nivel de seguridad en la empresa, enfocándose al área de mantenimiento, donde se encuentran materiales costosos. Utiliza como medio de llave de paso la huella digital y el rostro. Las herramientas utilizadas comprenden una tarjeta Raspberry Pi, la cual almacena toda la información de los usuarios, y es capaz de utilizar algoritmos para decidir si la persona tiene accesos o no. Los resultados de la investigación demuestran que, no existieron problemas en el proceso de autenticación mediante la huella digital, logrando en promedio el 98% de acierto, pero, durante el proceso de autenticación mediante el rostro, debido a un ambiente no controlado (iluminación o un ángulo incorrecto durante el proceso de toma de la imagen), se logró un promedio de acierto del 58%.

### 2.1.3. Local

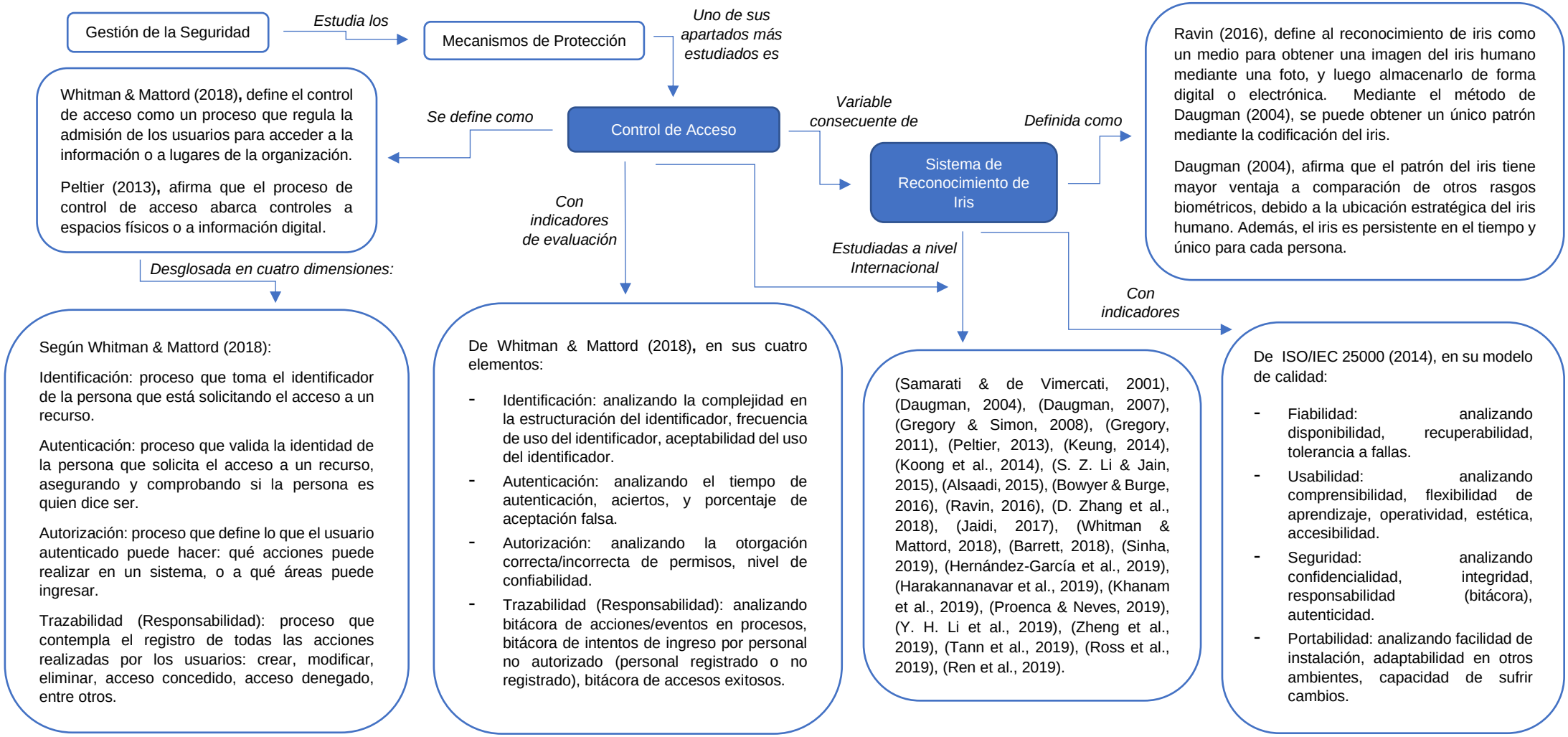
A nivel local no se encontraron estudios de investigación asociados al tema de Reconocimiento de Iris y Control de Acceso.

## 2.2. Bases teóricas

Para considerar una visión general del marco teórico y de las variables de investigación, en la Figura 2 se muestra un mapa de literatura donde se presentan las bases literarias.

**Figura 2**

*Mapa de literatura*



### 2.2.1. Sistema de reconocimiento de iris

#### 2.2.1.1. Iris humano

El iris es “la parte coloreada del ojo que se expande y se contrae para permitir más o menos luz” (Gregory & Simon, 2008, p. 92). El iris está conformado por una membrana que actúa como un diafragma dentro del ojo. Además, posee una apertura central llamada pupila, que, según la cantidad de luz, varía su tamaño.

“El iris posee una estructura muscular que se conoce como esfínter. La pupila funciona como un diafragma variando hasta 64 veces la luz que entra a la retina en 0,2 segundos” (Traipe, 2017, p. 13). La composición del iris y pupila comprende dos sistemas simpáticos: el sistema parasimpático tiene la función de contraer la pupila desde el músculo anular, y el sistema simpático tiene la función de dilatar la pupila desde el musculo radial. El iris proporciona el color de los ojos mediante pigmentadores que se encuentran dentro del mismo iris. El color de ojos varía según tres tipos de componentes biológicos presentes en el iris: el pigmento del epitelio del iris, la densidad celular del estroma del iris, y la melanina del estroma del iris.

Según Sánchez (2000), el iris es una estructura que presenta una apertura en la parte central, donde se encuentra la pupila, formando una pared entre las cámaras anterior y posterior del globo ocular, es decir, el iris se encuentra situado entre el cristalino y la córnea. Por otro lado, el iris está conformado de un estroma que contiene células pigmentadas y de un epitelio, donde se dilata o contrae actuando como un diafragma ocular, limitando el ingreso de la luz al ojo.

Según Ferreruela (2007), el iris es una estructura visible a través de la córnea que proporciona color a los ojos. En el centro del iris se encuentra la pupila, que es una abertura que sirve para el ingreso de la luz. La pupila es de color negro y varía de tamaño según la cantidad de luz que el ojo pueda percibir. El iris actúa como un diafragma y regula su tamaño dejando el pase de la luz. Durante la noche, por naturaleza, la pupila es de gran tamaño para poder percibir más luz, en cambio en el día, la pupila se mantiene en un tamaño menor debido a la gran cantidad de luz que se percibe.

##### 2.2.1.1.1. Estructura del iris humano

Según Geneser et al. (2015), el iris humano está conformado por cuatro capas:

- La lámina marginal anterior es una alteración de la parte trasera del estroma, cuya composición es de fibroblastos y melanocitos. Los fibroblastos componen una membrana continua de células que se prolongan de forma ramificada. Esta membrana cubre la superficie anterior del iris, comenzando desde el borde pupilar hasta la raíz del iris. Las ramificaciones de los fibroblastos se cruzan entre sí, pero dejando vacíos para que puedan ingresar el líquido y algunas partículas de tamaño de hasta 200 micrómetros. La capa limitante anterior o lámina marginal es “una condensación de células estromales y melanocitos” (Matilla, 2003, p. 3). Esta capa puede variar de forma considerable de grosor y de pigmentación, distinto en cada ojo, y así mismo, en diferentes zonas del iris. La capa limitante anterior puede estar muy poco visible o ausente, más que todo en las criptas iridianas.
- El estroma del iris está compuesto por tejidos conectivos laxos. Estos tejidos conectivos están compuestos por fibras colágenas demasiado delgadas, que están separadas por células. Estas células son los melanocitos y fibroblastos, aunque también se pueden encontrar los macrófagos y mastocitos. Dentro del estroma de la sección pupilar, por delante del epitelio anterior y el borde de la pupila, se logra encontrar una franja delgada circular de músculo liso denominado: esfínter de la pupila. Esta banda muscular lisa posee una similar estructura a las células musculares lisas, pero se diferencian debido al origen neuroectodérmico. El esfínter de la pupila produce una contracción por el exceso de luz que ingresa por la pupila, denominado reflejo fotomotor.

  Matilla (2003), señala que el estroma es una composición de tejidos conectivos y de vasos sanguíneos, melanocitos, nervios, y el esfínter de la pupila. Debido a las características tisulares que posee el estroma, esto le permite realizar una rápida contracción o expansión. En el estroma del iris se pueden apreciar dos grupos de células: tipo I, conformados por macrófagos con melanina fagocitada; y el tipo II, conformados por células neuroepiteliales y gránulos citoplasmáticos de melanina.
- El epitelio anterior es “una capa simple de células polarizadas cuya parte basal tiene características de músculo liso y sus elementos contráctiles se disponen en forma radial” (Speroni, 2016, p. 105). El epitelio anterior, también conocido como capa anterior no pigmentado, junto con el epitelio pigmentado posterior, conforman la zona anterior no sensible a la luz de la retina. El epitelio anterior está conformado por una cubierta hecha de células mioepiteliales; estas células mioepiteliales están conformadas por una zona

anterior llamada músculo basal, y por una zona posterior llamada epitelial apical. Los músculos basales se extienden de forma radial hasta el interior del estroma del iris, mediante prolongaciones que tiene un tamaño de hasta 60 micrómetros de longitud, conformando así el músculo que dilata la pupila.

El músculo que dilata la pupila tiene la estructura de una capa delgada muscular que se encuentra delante del epitelio pigmentado posterior. Este músculo es conformado por fibras simpáticas posganglionares, donde sus células se encuentran en el ganglio cervical superior.

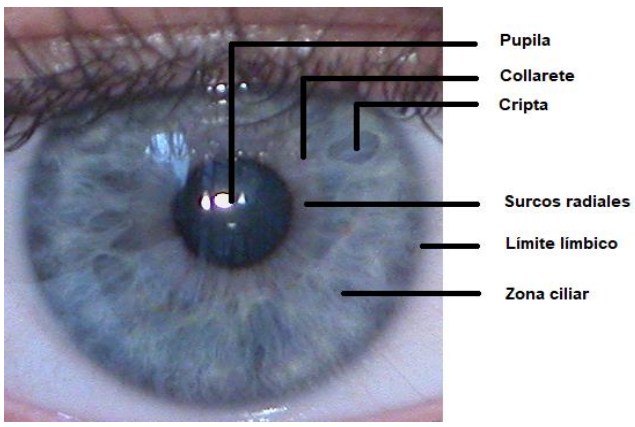
- El epitelio posterior, también conocido como epitelio posterior pigmentado, está compuesto por una cubierta de células cilíndricas, donde el citoplasma celular está ocupado por gránulos de melanina. Cerca al epitelio ciliar no pigmentado, los gránulos de pigmento disminuyen gradualmente hasta casi desaparecer.

  El epitelio posterior es una “una capa simple de células cúbicas o cilíndricas pigmentadas con melanina” (Speroni, 2016, p. 105). El epitelio posterior contiene dos capas celulares: epitelio pigmentado posterior, conformado por células cúbicas unidas entre sí por complejos de unión, cargados por gránulos de melanina; mioepitelio pigmentado, capa externa del epitelio posterior, compuesto por células cúbicas con citoplasma pigmentado, donde sus prolongaciones contienen miofibrillas, formando el músculo dilatador de la pupila.

El iris humano presenta diversas estructuras, texturas y formaciones, tal como se muestra en la Figura 3, donde cada uno de ellos cumplen funciones particulares, logrando la capacidad de visión humana mediante el control de luz.

**Figura 3**

*Características del iris humano*



#### 2.2.1.1.2. Patologías del iris humano

Según García (2011), existen patologías o anomalías del iris humano, los cuales son:

- La aniridia es “una condición de hipoplasia completa o parcial del iris e hipoplasia foveal, que produce una disminución de la agudeza visual y el nistagmo” (Hingorani et al., 2012, p. 1011). La aniridia es una anomalía panorámica que afecta a los tejidos de todo el ojo. Las personas que conllevan esta enfermedad tienen el tejido del iris alterado, viéndose como si solo tuvieran una gran pupila. Durante los años de vida de la persona, surgen otras enfermedades, como el glaucoma, cataratas y la opacificación corneal. Generalmente, la enfermedad se presenta luego de las seis semanas de nacimiento de la persona, pero con la respectiva atención médica, las personas mantienen una visión útil. La aniridia es “una alteración congénita que afecta al desarrollo del ojo. Se produce por mutaciones en el gen PAX6, gen responsable del desarrollo del ojo, tejido nasal y cerebro” (Rodríguez et al., 2007, p. 10). La aniridia es un problema bilateral, no solo afecta al iris, sino también a otras estructuras del ojo, como el cristalino, retina o la córnea, donde los principales síntomas son la baja agudeza visual y la fotofobia.
- “Coloboma es la palabra que se usa para describir una parte del ojo que todavía no está completamente formada” (Brown, 2010, p. 4). El coloboma es un defecto del iris humano, que es presentado desde cuando la persona nace. Lucen como una pupila secundaria o una ranura negra al lado de la pupila, también conocido como “ojo de gato” o “ojo de cerradura”, dándole una estructura irregular. Un coloboma pequeño puede ocasionar que la persona tenga una visión borrosa, doble visión, cadencia de la agudeza visual o imagen fantasma. Esta enfermedad no solo afecta a un solo ojo, puede afectar a ambos, y los efectos pueden o no ser iguales. Al coloboma del iris también se le define como el “inicio de cierre incompleto de la hendidura ocular fetal y suele situarse hacia abajo y hacia la línea media (nasal) y también puede asociarse al coloboma del cristalino, de la coroides y del nervio óptico” (Gálvez, 2000, p. 194). Cuando el desarrollo del iris y la pupila se interrumpe durante el proceso embrionario de la persona, indica que padecerá de un coloboma del iris, debido a que la pupila no es redonda. El nivel de agudeza y los campos visuales no siempre son afectados por el coloboma del iris, pero es probable que surja el síndrome de fotofobia, debido a que la pupila no puede cerrarse cuando existe un nivel alto de luz.

Este efecto provoca que las personas procuren cubrirse para evitar la luz durante el día (durante su rutina diaria), pero hay ciertas veces que las personas con este defecto necesitan dirigir la mirada a la luz brillante para reorganizar sus sentidos.

- “Los nódulos de Lisch son elevaciones bien definidas, en forma de domo que salen de la superficie del iris” (Moreno et al., 2014, p. 191). Los nódulos de Lisch es una alteración en la forma visual del iris, donde las personas que lo padecen son quienes presentan neurofibromatosis tipo 1 (NF1). Estos nódulos están compuestos por pequeños tumores de 1 a 2 milímetros de diámetro, tumores benignos que se denominan hamartomas. Los nódulos de Lisch son hamartomas presentes en la parte pigmentada el iris, sin presentar problemas en la visión, pero valorados en el diagnóstico. Estos hamartomas puedes ser visualizados mediante biomicroscopía, presentando un color marrón claro en la parte inferior del iris. Esta anomalía puede aparecer antes que los neurofibromas, pero son susceptibles a empeorar progresivamente con la edad (Martín-Begué et al., 2019). Los nódulos de Lisch pueden surgir cuando la persona pasa por la adolescencia, donde se presentan síntomas como dolor de cabeza, pérdida severa de la audición, escoliosis, convulsiones, adormecimiento del rostro. El 1% de la población con esta enfermedad sufre de retraso mental, dificultad en el aprendizaje e hiperactividad. La enfermedad de nódulos de Lisch puede ser diagnosticado mediante los exámenes de inspección en la piel, radiografías, pruebas genéticas (Salas et al., 2013).
- El xantogranuloma juvenil, conocido también con las siglas XGJ, es “una neoformación de aspecto papular o nodular, oval, firme, superficie lisa bien delimitada, eritematoso, de 0,5 a 2 cm de diámetro” (Martínez et al., 2002, p. 22). El xantogranuloma juvenil afecta a nivel ocular al iris, presentándose como un nódulo de color amarillento, asociado con un frecuente sangrado en la cámara anterior debido a la sangre presentada en la malla trabecular. Las estructuras tendientes para comprometer por esta enfermedad son los párpados, retina, conjuntiva, esclera, cuerpo ciliar, nervio óptico, glándula lagrimal, limbo esclerocorneal. Existen casos donde se han reportado la presencia de una masa dependiente al saco lagrimal, debido a infiltraciones de canto medial y fosa lagrimal (Camargo et al., 2003).
- La heterocromía de iris es “una alteración en el color y la estructura de iris. Aunque generalmente es benéfico, puede ser la única pista de un trastorno subyacente” (Gladstone, 1969, p. 184). La heterocromía de iris es una

anomalía que consiste en que el color de los iris de la persona es de colores diferentes. Esta enfermedad puede afectar al color de la piel y cabello, pero el caso donde se presenta con mayor frecuencia es en los ojos. La coloración de los ojos puede ser distinto en cada uno (conocido como heterocromía total), o una parte del iris diferente a ambos ojos (heterocromía parcial). La heterocromía se produce debido a la cantidad exagerada o muy poca de melanina en el cuerpo; la melanina es el componente que crea la pigmentación. Según Gladstone (1969), la heterocromía puede tomar dos formas: hipopigmentación del iris de cualquier color, con hipoplasia del iris; hiperpigmentación con hiperplasia del iris. El cambio de color del iris puede ser en un solo ojo o en los dos, con una coloración parcial o total. La heterocromía del iris puede recibir varias denominaciones, como: iris de varios colores, iris abigarrado o iris bicolor.

- La microcoria congénita es “un raro trastorno del desarrollo autosómico dominante del iris asociado con miopía y glaucoma juvenil de ángulo abierto” (Ramprasad et al., 2005, p. 934). Es una alteración oftalmológica con baja frecuencia de transmisión autosómica debido a la mala formación del músculo dilatador de la pupila. “La microcoria congénita, o miosis congénita, se define como una pupila pequeña con un diámetro de menos de 2 mm cuando el paciente mira un objeto distante” (Toulemont et al., 1995, p. 193). Según Al-Owaid et al. (2019), la microcoria congénita es un extraño desorden poco frecuente. El pequeño tamaño de la pupila no se inmuta ante respuestas grandes o leves de luz, incluso a las gotas dilatantes. “El análisis genético de algunos casos de microcorias reveló una deleción en el brazo largo del cromosoma 13 (13q31-q32)” (Al-Owaid et al., 2019, p. 1).

#### 2.2.1.2. Sistema biométrico

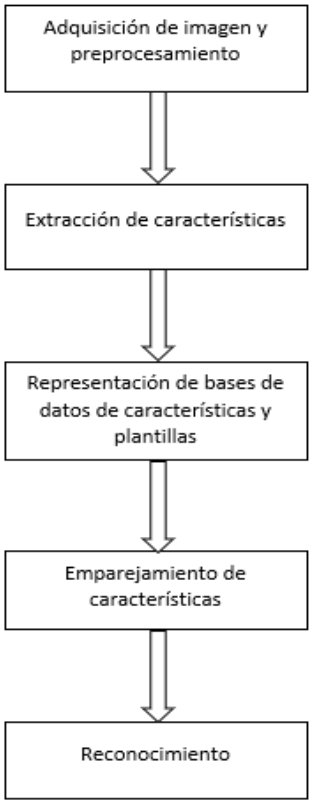
“El término biometría proviene del griego antiguo bios (vida) y metron (medida). La biometría se refiere a toda la clase de tecnologías y técnicas para identificar de manera única a los humanos” (Gregory & Simon, 2008, p. 9). La tecnología biométrica presenta varios enfoques, donde el objetivo principal es de favorecer una forma más segura a los métodos tradicionales existentes para controles de acceso, usados para la protección de bienes personales o empresariales. El uso de las tecnologías biométricas ha existido durante años en diferentes campos, por ejemplo, las organizaciones de inteligencia y militares han utilizado la tecnología biométrica para proveer mejoras en el control de accesos lógicos y físicos.

“Un sistema biométrico es un sistema informático implementado mediante la explotación de los métodos, técnicas y tecnologías de identificación biométrica correspondientes” (D. Zhang et al., 2018, p. 3). Estos sistemas se caracterizan por reconocer y extraer patrones de características de las personas a ser identificadas, para luego compararlos en un conjunto de plantillas almacenadas, y así poder decidir si la persona es quien dice ser. Estos sistemas pueden ser aplicados a dos campos: verificación, donde se decide si la persona es quien dice ser; identificación, donde se decide de quién son los datos biométricos de la persona verificada. Por lo tanto, el sistema biométrico puede estar compuesto de dos o varias clases de reconocimiento de patrones.

La Figura 4 muestra los pasos de un proceso de sistema biométrico común, desde la captura de la imagen correspondiente de la llave biométrica perteneciente a la persona a verificar, hasta el proceso de emparejamiento de rasgos biológicos y reconocimiento respectivo de la entidad a reconocer.

**Figura 4**

*Proceso biométrico*




*Nota*. Elaborado y traducido de Sinha (2019).

#### 2.2.1.2.1. Clasificación de sistemas biométricos

Según Sinha (2019), existen dos clasificaciones para los sistemas biométricos:

- “Los sistemas biométricos unimodales funcionan en rasgos individuales del individuo para su identificación y verificación” (como se cita en Sinha, 2019, p. 312). Esta clasificación solo utiliza un rasgo biométrico o una única fuente de información para poder verificar e identificar a una persona. Los sistemas biométricos unimodales han ido mejorando, pero aún se presentan problemas debido a rasgos biométricos no universales, falta de precisión y suplantación de identidad (Oloyede & Hancke, 2016).
- “Los sistemas biométricos multimodales no son más que una combinación de dos o más rasgos biométricos fisiológicos o conductuales” (Sinha, 2019, p. 313). Esta clasificación combina más de una característica biométrica para el proceso de identificación. Los sistemas biométricos multimodales no presentan el problema de no universalidad, resultando en un sistema de identificación más seguro y preciso (Oloyede & Hancke, 2016).

#### 2.2.1.2.2. Tipos de sistemas biométricos

Según Gregory & Simon (2008), existen dos tipos bases de biometría:

a. La biometría fisiológica es “el sistema de reconocimiento basado en características fisiológicas tiene una precisión relativamente alta” (como se cita en Koong et al., 2014, p. 3). La biometría de tipo fisiológica se caracteriza por medir una parte o estructura del cuerpo humano. Estas características están asociadas a rasgos estáticos de la persona, no tendientes a sufrir cambios durante el tiempo (Alsaadi, 2015). Según estudios de Gregory & Simon, (2008), Koong et al. (2014) y Sinha (2019), existen los siguientes tipos de sistemas biométricos dentro del grupo de biometría fisiológica:

    - La huella dactilar se registra y puede ser medido fácilmente gracias a los patrones únicos de características que utiliza.
    - El reconocimiento facial verifica a una persona automáticamente mediante una imagen digital. Es el método biométrico más natural.
    - El reconocimiento del iris usa la parte coloreada que rodea la pupila. Cada persona tiene un patrón de iris único. Es un método de rendimiento óptimo.

- El escáner de la mano utiliza las manos de las personas, ya que, casi no cambian durante los años. Esta técnica incluye el espesor, ancho, longitud y superficie de la mano.
- El escáner de retina usa patrones de vasos sanguíneos que tiene la retina, presentando patrones únicos por cada persona.
- El reconocimiento de oídos usa características del oído que no cambian con los años. Presenta una estabilidad confiable de nivel de seguridad.
- La huella del pie no necesita de dispositivos especiales, ni ambientes controlados. Este método calcula y compara los vectores de características que tienen los pies.

b. La biometría conductual está relacionado al estudio de medidas de patrones que son únicos en las acciones de las personas. Este tipo biométrico se caracteriza por el limitado uso de rasgos de comportamiento que ocupa una persona (Alsaadi, 2015). Según estudios de Gregory & Simon (2008), Koong et al. (2014) y Sinha (2019), existen los siguientes tipos de sistemas biométricos dentro del grupo de biometría conductual:

   - El reconocimiento de firma se basa en la dinámica de cómo la persona realiza su firma, midiendo la dirección, aceleración, presión y la cantidad de golpes.
   - La dinámica de pulsación de tecla se basa en el supuesto de que las personas tienen diferentes patrones de ritmo habitual de tipificado.
   - El reconocimiento de voz se basa en que, cada persona tiene una tonalidad diferente, basándose en las características de la voz, pero no dependiente de la pronunciación o sonido.
   - El reconocimiento del paso se basa en el patrón de caminar de una persona, capturando características para fines biométricos.

#### 2.2.1.2.3. Criterios de los sistemas biométricos

Según Oostdijk et al. (2016), los sistemas biométricos pueden ser medidos y clasificados en base a criterios o requerimientos. Los criterios son una fuente esencial para un sistema biométrico, donde un sistema biométrico puede obtener excelentes puntajes en algunos requerimientos, pero eso no significa que sea adecuado. Se refuerza la evaluación de los criterios mediante el seguimiento y cumplimiento de estándares, regulaciones y leyes.

Según estudios de Hernández-García et al. (2019), Mahfouz et al. (2017) y Oh et al. (2019), se identifican los siguientes criterios o requerimientos de un sistema biométrico:

- La universalidad es el criterio en el que, cada persona que utiliza el sistema biométrico debe tener la característica o rasgo biométrico para el proceso de autenticación.
- La unicidad es el criterio en el que, la característica o rasgo biométrico debe ser capaz de diferenciar a dos personas, para verificar si la persona es legítima o un impostor.
- La eficacia es el criterio en el que, los sistemas biométricos deben hacer lo que se supone que deben hacer. Este criterio se mide por la perfección y precisión.
- La eficiencia es el criterio en el que, los sistemas biométricos deben ser capaces de utilizar recursos necesarios en relación con la eficacia. Este criterio se mide por los recursos utilizados.
- La permanencia es el criterio en el que, la característica o rasgo biométrico debe perdurar en el tiempo, sin variar (o en lo más mínimo) de su forma origen.
- El coleccionismo es el criterio en el que, la característica o rasgo biométrico debe ser fácil de medir y obtener de las personas. Los datos obtenidos son medidos cuantitativamente.
- El desempeño es el criterio en el que, la precisión de la característica o rasgo biométrico debe poseer robustez y funcionalidad en el entorno asignado. Este criterio se basa en la solidez, velocidad de procesamiento y precisión del sistema biométrico utilizado.
- La aceptabilidad es el criterio en el que, las personas que utilizan el tipo de sistema biométrico asignado deben ser capaces de presentar la característica o rasgo biométrico.
- El esquivo de seguridad es el criterio en el que, el tipo de sistema biométrico asignado debe ser capaz de evitar acciones de falsificación u otro tipo de ataque de seguridad sobre las características o rasgos biométricos.
- La accesibilidad es el criterio en el que, el tipo de sistema biométrico asignado debe ser capaz de adaptarse al uso de personas con discapacidad u alguna otra limitación (vestimenta, características físicas, etc.) para el proceso de autenticación.

- La satisfacción es el criterio en el que, el tipo de sistema biométrico asignado debe ser capaz de cumplir las expectativas de las personas que lo utilizan.

#### 2.2.1.2.4. Comparación de sistemas biométricos

Los sistemas biométricos contemplan ventajas y desventajas. El funcionamiento de cada sistema biométrico es afectado por muchos factores externos o internos que pueden disminuir su desempeño.

En la Tabla 2 se indican las ventajas, desventajas y aplicaciones de diversos sistemas biométricos, donde, según la llave biométrica utilizada, presentan características particulares que, de alguna manera, influyen en su aplicación para la resolución de algún problema.

**Tabla 2**

*Ventajas, desventajas y aplicaciones de sistemas biométricos*

| Modalidad | Ventajas | Desventajas | Aplicaciones |
|---|---|---|---|
| Huella dactilar | - Más usado.<br>- Económico.<br>- Seguro y confiable.<br>- Intrusivo | - Cortes o cicatrices.<br>- Fácil engaño por dedo artificial.<br>- Expuesto a ruidos o suciedad. | - Control de fronteras.<br>- Control de acceso en empresas. |
| Rostro | – No intrusivo.<br>– Aceptado socialmente.<br>– Más rápido. | – Rasgo facial cambiante.<br>– No distinción entre gemelos.<br>– Depende de la luz. | – Control de acceso.<br>– Vigilancia.<br>– Identificación criminal. |
| Retina | – No falsificable.<br>– Seguro y confiable.<br>– Verificación rápida. | – No es fácil usar.<br>– Enfermedades oculares.<br>– Costoso. | – Alta seguridad.<br>– Diagnóstico oftalmológico. |

(continúa)

Tabla 2 (continuación)

| Modalidad | Ventajas | Desventajas | Aplicaciones |
|---|---|---|---|
| Iris | – Altamente preciso.<br>– No intrusivo.<br>– Rasgo biométrico persistente. | – Relativamente costoso.<br>– Enfermedades al iris.<br>– Aceptabilidad social media. | – Control de acceso.<br>– Seguridad nacional. |
| Geometría de la mano | – Fácil uso y duradero.<br>– No intrusivo.<br>– No afectado por humedad o textura de piel. | – No es único.<br>– Eficiente para adultos.<br>– Resultados no precisos. | – Centrales nucleares.<br>– Control de acceso militar. |

*Nota*. Adaptado y traducido de Sabhanayagam et al. (2018).

#### 2.2.1.3. Sistema de reconocimiento de iris

"Reconocimiento de iris, un medio para grabar una imagen del iris fotográficamente y almacenar los datos electrónicamente" (Ravin, 2016, p. 2054). Los sistemas de reconocimiento de iris están enfocados a diversas aplicaciones y usos, como el acceso a instalaciones, el rastreo de seres humanos perdidos, generación de informes de asistencia para grandes sistemas corporativos.

Los sistemas de reconocimiento de iris usan algoritmos, técnicas de software y sensores para analizar texturas pequeñas. Las imágenes de los vasos sanguíneos retinianos, esclerales, pueden ser enmascarados o falsificados fotográficamente, pero la composición morfológica del iris logra que este método sea el biométrico ocular preferido entre los demás métodos que usan rasgos del ojo humano (Ravin, 2016).

Los sistemas de reconocimiento de iris están sujetos a diversos desafíos, como los mencionados en Sinha (2019):

- Considerar puntos estratégicos claves para el reconocimiento de iris, con el fin de evitar limitaciones por la edad o enfermedades oculares.
- Diseño de técnicas y algoritmos que eviten el engaño, como una imagen impresa del iris en 2D o 3D.
- Captura incorrecta del iris debido a factores ambientales.

- Exploración de técnicas y algoritmos para el reconocimiento de iris usando aprendizaje profundo (Deep Learning).

El patrón del iris proporciona un enfoque poderoso para el reconocimiento biométrico. A pesar del tamaño del iris (11 milímetros estándar), y los problemas ocasionados por su tamaño, tiene una mayor ventaja debido a la variabilidad del patrón o rasgo biométrico presente en cada persona, la protección al encontrarse en el ojo, y su persistencia en el tiempo. La distorsión de la imagen del iris por la dilatación de la pupila, puede ser reversible en el proceso de codificación (Daugman, 2004).

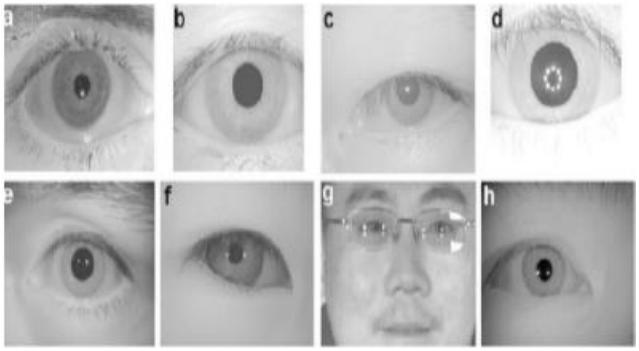
#### 2.2.1.3.1. Proceso del sistema de reconocimiento de iris

Según estudios de Harakannanavar et al. (2019) y Khanam et al. (2019), los procesos, pasos o etapas de un sistema de reconocimiento de iris son:

a. La adquisición de la imagen es el primer paso para el proceso de reconocimiento del iris. Se pueden utilizar diversas técnicas de adquisición con imágenes en alta calidad para obtener modelos precisos de las características biométricas del iris. En esta etapa, la cámara encargada de obtener la imagen del iris de la persona, se encuentra 50 cm o 100 cm del sujeto (Khanam et al., 2019). En la Figura 5 se puede visualizar diversas imágenes capturadas, el cual serán analizadas para identificar los límites del iris durante un proceso biométrico: límite con la pupila, áreas cubiertas por párpados, áreas reflectantes, sombras.

**Figura 5**

*Imágenes reales de iris*




*Nota*. Elaborado por Harakannanavar et al. (2019).

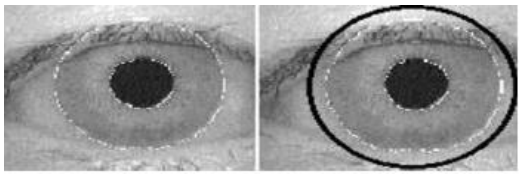
b. El pre-procesamiento tiene la tarea de mejorar la imagen adquirida en la etapa de “adquisición de la imagen del iris”; eliminar ruidos, normalizar la

imagen, aumentar la calidad de la imagen, para que el porcentaje de reconocimiento sea el adecuado (Khanam et al., 2019). La imagen capturada presenta porciones no deseadas, como pestañas, esclera, pupila, etc., junto a la ROI (región de interés). Al presentarse estos obstáculos, la imagen no debería ser procesada directamente tal como fue capturada. Además, la presencia de brillos y cambios en la distancia que existe entre la persona y la cámara, pueden reducir el porcentaje de reconocimiento (Harakannanavar et al., 2019).

c. Existen varios métodos para realizar el proceso de segmentación del iris en la imagen adquirida, pero los más usados o populares son el método basado en el operador integro-diferencial y el método basado en la transformación de Hough. Estos métodos están basados en el criterio de ajuste de curvas de los bordes de la imagen, pero solo se obtiene un mejor resultado en imágenes nítidas y de alta calidad (Harakannanavar et al., 2019). El método creado por Daugman (2007), es el más conocido. Este método usa operadores integro-diferenciales, variante al método por transformación de Hough. Estos operadores integro-diferenciales se encargar de detectar los bordes y límites del iris. Por otro lado, el método de transformación circular de Hough, permite obtener el radio y coordenadas presente en imágenes circulares, eficaz para diferenciar entre los límites del iris y la pupila. En la Figura 6 se visualiza el proceso de segmentación de una imagen de iris, donde se puede notar la limitación de los bordes de la pupila e iris para su posterior procesamiento.

**Figura 6**

*Imagen del iris segmentado*



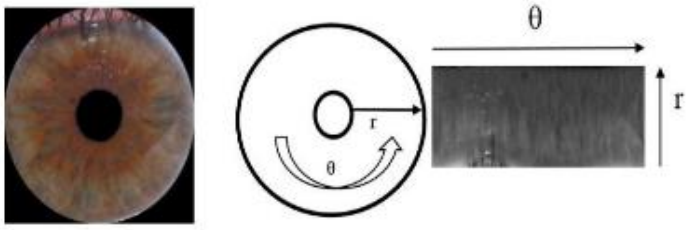
*Nota*. Elaborado por Harakannanavar et al. (2019).

d. La normalización tiene la tarea de transformar la imagen segmentada del iris, desde coordenadas cartesianas a coordenadas polares, logrando comparaciones justas. Existen dos métodos populares de normalización: lámina de hoja de goma de Daugman, y el registro de imágenes de Widles.

El método de lámina de hoja de goma de Daugman visualizada en la Figura 7, convierte la imagen del iris segmentado en una imagen rectangular, es decir, porciones segmentados del iris son transferidos a coordenadas pseudopolares adimensionales (Harakannanavar et al., 2019).

**Figura 7**

*Modelo de hoja de goma de Daugman*




*Nota*. Elaborado por Harakannanavar et al. (2019).

e. Las características especiales de la imagen son extraídas mediante el uso de métodos para generar una plantilla biométrica. Los métodos más usados son: filtro Gabor, y transformada Wavelet.
f. La plantilla resultante de la etapa de extracción de características se compara con la plantilla almacenada en la base de datos, encontrando las respectivas similitudes, y proceder a decidir si la persona es quien dice ser.

#### 2.2.1.3.2. Estándares del sistema de reconocimiento de iris

Según Bowyer & Burge (2016), los estándares de reconocimiento de iris son abiertos, tanto para la cámara que captura el iris, las propiedades y registros de la imagen. Los estándares de intercambio de datos de imagen son importantes para evitar la dependencia entre sistemas; puede existir sistemas biométricos que usen estándares documentados, o estándares propietarios, siendo este último fatal cuando se requiere el intercambio de datos entre empresas u organizaciones.

La Tabla 3 describe los diversos estándares aplicables al procesamiento de imágenes de iris para procesos biométricos, con la finalidad de generar formatos compatibles entre sistemas.

**Tabla 3**

*Estándares de imagen de iris*

| Estándar | Descripción |
|---|---|
| INCITS 379 | Formato de transferencia de imagen de iris |
| ISO/IEC 19794 | Formato de transferencia de información biométrica. Parte 6: Datos de imagen de iris. |
| ANSI/NIST-ITL 1-2007 | Formato de información para la transferencia de huella dactilar, rostro facial y otra información biométrica tipo 17. |
| ISO/IEC 29794 | Calidad de muestra biométrica. Parte 6: Datos de imagen de iris. |
| ISO/IEC 29109 | Metodología de prueba de conformidad para intercambio de datos biométricos y formatos definidos en ISO/IEC 19794 - 6 |

*Nota*. Adaptado de Bowyer & Burge (2016).

En la antigüedad, los sistemas biométricos eran escasos, es decir, solo se conocían ciertos tipos de sistemas biométricos. El sistema biométrico más conocido, en ese entonces, era el reconocimiento por huellas dactilares. Debido a estudios realizados sobre otras formas de poder reconocer a las personas utilizando biometría, se logró la creación de algoritmos para el reconocimiento por iris. Estos algoritmos creados y patentados por John Daugman, servirían para la creación de diversos sistemas de reconocimiento de iris conocidos hoy en día.

En la actualidad, existen diversas publicaciones científicas que refuerzan el tipo de sistema biométrico por reconocimiento de iris. Investigadores de diferentes países, publican nuevos métodos y técnicas para mejorar el proceso de reconocimiento de iris, mejorar el rendimiento y la velocidad de procesamiento. La inteligencia artificial está jugando un papel importante en las investigaciones publicadas por diferentes investigadores, sobre todo el aprendizaje profundo (Deep Learning), donde utilizan la inteligencia artificial para el proceso de segmentación o mejoramiento de la imagen del iris obtenido en el proceso de adquisición. En el Perú, las investigaciones enfocadas al reconocimiento de iris son casi nulas; los investigadores de trabajos de investigación o artículos científicos se enfocan más a otros tipos de sistemas biométricos, desconociendo la gran capacidad que tiene el reconocimiento por iris. Además, la

misma sociedad es adversa al conocimiento sobre el beneficio que posee el método biométrico por iris.

En el futuro, los sistemas biométricos serán indispensables para las empresas y demás organizaciones, donde serán enfocados para diversas tareas primordiales, no solo para seguridad. Las características únicas del cuerpo humano facilitan que existan sistemas biométricos seguros. Con las nuevas tecnologías, métodos y técnicas, se podrá contrarrestar la falsificación mediante objetos no vivos (máscaras, rasgo biométrico impreso, fotografía, entre otros). El avance de la tecnología permitirá conocer nuevos órganos o partes del cuerpo humano con características únicas que servirán como rasgo biométrico para el proceso de reconocimiento, y no solo características del cuerpo humano, también de características conductuales únicas de cada persona.

### 2.2.2. Control de acceso

"Control de acceso es el proceso de mediación de cada solicitud a los recursos y datos mantenidos por un sistema y determinar si la solicitud debe otorgarse o denegarse" (Samarati & de Vimercati, 2001, p. 137). La decisión de otorgar los accesos correspondientes a las personas se aplica mediante políticas de seguridad establecidas. Las políticas de seguridad a aplicar son diversas, dependiendo de criterios para definir qué debe y qué no debe otorgarse, garantizando la seguridad de la organización.

Según Gregory & Simon (2008), dentro del contexto biométrico, el control de acceso permite la gestión de quién puede utilizar un recurso en particular. El control de acceso no solo aplica para sistemas informáticos, también puede ser aplicado a controles físicos, tales como el ingreso a ciertas áreas de una organización mediante el control de puerta, o acceso a un automóvil.

Según S. Z. Li & Jain (2015), define dos tipos de controles de acceso: el control de acceso lógico, y el control de acceso físico. El control de acceso lógico es el medio utilizado para la protección de la información de redes, teléfonos, computadoras. En este método se pueden usar diversos tipos de autenticadores, tales como datos biométricos, tokens, contraseñas. El control de acceso físico es el uso de la biometría para lograr la identificación de las personas y permitir el acceso a las áreas de la organización. Existen empresas que utilizan tecnologías biométricas, como el reconocimiento de huella digital o reconocimiento de iris para el control de accesos en puntos claves de entrada y salida.

#### 2.2.2.1. Tipos de control de acceso

Los sistemas de control de acceso garantizan que personas autorizadas puedan tener acceso a cierta información y/o accesos a instalaciones. El objetivo de los sistemas de control de acceso es impedir que usuarios no autorizados modifiquen información importante de la empresa, o se cometan robos de bienes materiales.

Según Peltier (2013), existen tres tipos de controles de acceso:

- Los controles de seguridad de tipo administrativo (también conocidos como procedimientos) son políticas y procedimientos implementados para orientar a las personas a que puedan manejar la información de forma responsable y confidencial. Esos procedimientos y políticas dan a conocer a las personas el cómo gestionar la empresa y cómo realizar las tareas diarias asignadas. Los controles de seguridad de tipo administrativo se logran cumplir con la ayuda de controles técnicos/lógicos o controles físicos (Keung, 2014). Los controles administrativos incluyen procesos, comprobación de antecedentes, capacitaciones, políticas, verificación de hábitos de trabajo, supervisiones. Este tipo de control de acceso es recomendado para amenazas internas; el robo de información por parte del mismo personal sigue estando en aumento. Debido al incremento en la movilidad de los empleados en las empresas, es necesario implementar controles de acceso más rigurosos para proteger toda la información vital. Por ejemplo, implementar el protocolo de seguridad de cancelación de cuentas de usuarios cuando ellos ya no trabajan en la empresa o están de vacaciones, es una estrategia bastante recomendada para mitigar amenazas internas, como el robo de información o suplantación de identidad por parte de otro usuario que tiene conocimiento de la contraseña de seguridad.
- “Los controles de seguridad física son medios y dispositivos para controlar el acceso físico a información confidencial y para proteger la disponibilidad de la información” (como se cita en Keung, 2014). Las computadoras, dispositivos e instalaciones de comunicaciones (incluyendo la información), son considerados activos vitales, y por consecuente, deben ser protegidos ante cualquier amenaza. Actualmente, existen controles físicos implementados en diferentes empresas, tales como sistemas de acceso físico que incluyen al personal de seguridad, control de acceso de puertas, circuitos cerrados de televisión, lugares restringidos, sistemas de detección de intrusos, entre otros. El personal de seguridad, cámaras de vigilancia, bloqueo de computadoras y la separación de funciones, cumplen un rol

importante para la disuasión de amenazas cuando no existen controles de accesos (Peltier, 2013). El recurso humano de seguridad, y los sistemas tecnológicos de acceso y vigilancia logran mejorar la seguridad dentro de la empresa, debido al método biométrico utilizado actualmente por los sistemas de control de acceso. Las empresas necesitan controles físicos que monitoreen, controlen, administren el acceso de las personas. Cada área de la empresa debe estar correctamente clasificada dependiendo del nivel de amenaza que podrían recibir, diferenciando los permisos que debería tener cada usuario, según su función. Actualmente, existen diversos métodos o mecanismos que permiten a las empresas tener un mayor control de los accesos y privilegios en sus instalaciones, detectando y alertando intrusos no deseados o personas no autorizadas.

- Los controles lógicos, o también denominados controles técnicos, son restricciones del acceso a algún sistema. Este tipo de control se basa en ciertas características de software y hardware facilitadas en un sistema ayudando a controlar la seguridad y mantener la integridad de la información (Keung, 2014). Los controles de tipo lógico no permiten el acceso a los sistemas, protegiendo la información que estos sistemas manejan, información que son importantes dentro de una organización (Peltier, 2013). Por ejemplo, las tarjetas inteligentes son controles lógicos o técnicos que permiten el acceso físico a una instalación o iniciar sesión en alguna computadora o red de la empresa. Dentro de las políticas de seguridad en la empresa, debe estar contemplado la actividad continua de monitorear y registrar las actividades realizadas por los controles de acceso, para ayudar al equipo de seguridad a encontrar y disminuir vulnerabilidades.

#### 2.2.2.2. Elementos del control de acceso

Según Whitman & Mattord (2018), el proceso de control de acceso está constituido por cuatro etapas, también conocidos colectivamente por las siglas IAAA en inglés (identification, authentication, authorization, accountability):

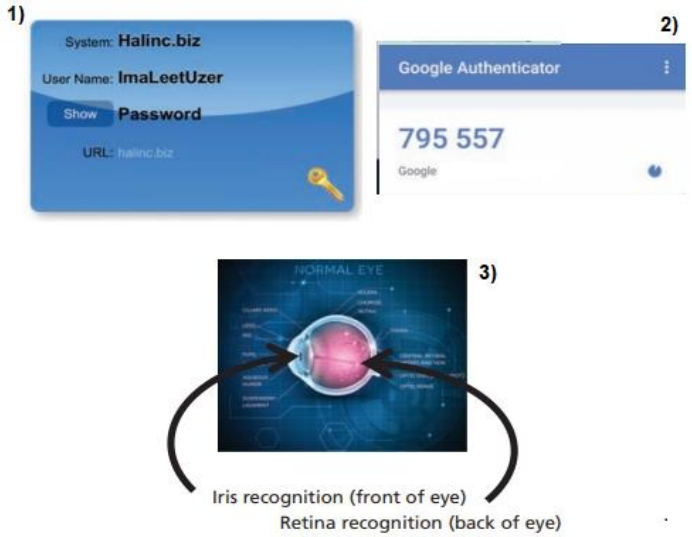
a. “La identificación es un mecanismo que proporciona información sobre una entidad no verificada, llamada suplicante, que desea tener acceso a una entidad conocida” (Whitman & Mattord, 2014, p. 346). El identificador debe ser único y diferente para cada persona. Algunas empresas disponen políticas de seguridad para la creación del identificador, combinando el nivel y área de trabajo del usuario, tanto personas internas como externas, que

necesitan ingresar a ciertas áreas de la empresa para realizar alguna acción. Un sistema de información tiene ciertas funciones que permiten reconocer a los usuarios, de forma individual. “La identificación es el primer paso para obtener acceso a material protegido, y sirve como base para la posterior autenticación y autorización” (Whitman & Mattord, 2018, p. 10). El proceso de identificación y autenticación son importantes para lograr la correcta autorización de accesos por parte de los usuarios.

b. La autenticación es el proceso de validar la supuesta identidad de un solicitante. Asegura que la entidad que solicita acceso es la entidad que dice ser” (Whitman & Mattord, 2014, p. 346). El proceso de autenticación se realiza mediante el control establecido para comprobar que el usuario es quien dice ser. Para el proceso de autenticación, los usuarios revelan sus credenciales, como el número de identificación personal (PIN), una contraseña, o alguna palabra clave que les permita autenticarse ante un sistema. En la Figura 8 se muestran los tres tipos de mecanismos de autenticación descritos por Whitman & Mattord (2018), donde cada tipo está compuesto de características particulares para proveer la comprobación o autenticación de identidad de una persona:

**Figura 8**

*Mecanismos de autenticación*




*Nota*. Adaptado de Whitman & Mattord (2018). 1: Algo que una persona sabe; 2: Algo que una persona tiene; 3: Algo que una persona puede producir.

- “Algo que una persona sabe” es el tipo de autenticación que comprueba que la identidad de la persona sea la correcta mediante el uso de una contraseña, PIN, frase clave, u otro elemento para comprobar su identidad. Una contraseña debería ser complicada de averiguar o adivinar por otra persona, para ello, las empresas crean políticas de cómo crear contraseñas más seguras.
- “Algo que una persona tiene” es el tipo de autenticación que comprueba la identidad de la persona mediante un elemento, como una tarjeta o token criptográfico.
- “Algo que una persona puede producir” es el tipo de autenticación que comprueba la identidad de la persona mediante el uso de la biometría. Existen diversos métodos de biometría, como la huella digital, impresión de la mano, geometría de la mano, rostro, iris, retina, entre otros.

c. El proceso de autorización define lo que el usuario autenticado puede hacer, tales como acceder, modificar o eliminar algún contenido de información. Por ejemplo, para el manejo de autorizaciones, las organizaciones crear listas de control de accesos o grupos de autorización, o esquemas de autorización para el manejo de información en bases de datos. Whitman & Mattord (2014), describe tres maneras de manejar las autorizaciones:

   - Autorización para cada persona autenticada, verificando la entidad y otorgando los accesos respectivos.
   - Autorización para los miembros de un grupo, verificando las entidades y otorgando los accesos respectivos mediante una lista de membresías.
   - Autorización en múltiples sistemas, donde un sistema central verifica la entidad y otorga los accesos respectivos mediante un conjunto de credenciales. Este conjunto de credenciales es compatible con todos los sistemas dentro del dominio de autorización.

d. La trazabilidad o responsabilidad contempla los registros del sistema, reportes y bitácoras, registrando información como intentos fallidos y modificaciones en el sistema. Estos registros sirven para lograr detectar intrusos, puntos clave de vulnerabilidad, o rastrear el uso indebido de un recurso (Whitman & Mattord, 2014). La trazabilidad o responsabilidad se presenta cuando la empresa quiere conocer qué acciones se realizaron en un sistema, dónde y cuándo. Estos registros ayudan al personal de seguridad verificar si la persona está realizando sus respectivas acciones asignadas, o intenta realizar acciones que no están dentro de sus funciones.

Un sistema de control de accesos tiene que ser capaz de monitorear, mediante registros o historiales, todas las acciones del personal de una empresa, tanto el ingreso a instalaciones o manipulación de información importante. Según Gregory (2011), estos registros pueden o deben considerar los siguientes puntos:

- Entrada exitosa, donde cada entrada de un empleado debe ser registrado.
- Entrada sin éxito, donde todos los eventos de "Acceso Denegado" deben registrarse. Estos eventos deben ser evaluados de inmediato para comprobar si una persona está intentando acceder a zonas no permitidas o información privilegiada, o si una persona externa a la empresa está intentando acceder usando tarjetas o códigos ilegítimos.
- Actividad imposible, donde los registros deben contemplar el monitoreo de accesos múltiples por el mismo usuario, debido a que el usuario no puede estar (físicamente) en dos lugares diferentes al mismo tiempo.
- Alteración del lector, donde el sistema debe registrar cualquier anomalía o alteración en el lector que permite dar el acceso a un área.
- Fallas en el equipo, donde cualquier falla en los equipos deben ser registrados. Esto ayudará al personal de seguridad identificar equipos en mal estado o intentos de manipulación.
- Cambios en la configuración de seguridad, donde todos los cambios en la configuración de las zonas de seguridad u otro privilegio lógico del usuario deben registrarse.
- Cambios generales en la configuración del sistema, donde se debe registrar cualquier cambio realizado en la configuración general del sistema, incluyendo el usuario que realiza tales acciones.

#### 2.2.2.3. Modelos de control de acceso

Según estudios de Jaidi (2017) y Whitman & Mattord (2018), existen los siguientes modelos de control de acceso:

- El modelo de control de acceso discrecional (DAC) permite la restricción de los accesos a los recursos en función a la identidad de la persona o grupo de personas. La persona dueña del recurso otorga los accesos a los demás usuarios del sistema. Se denomina control discrecional porque "la gestión de los derechos de acceso queda a discreción de los usuarios" (Jaidi, 2017, p.

86). Los controles de acceso discrecional son implementados a discreción del usuario. Los mismos usuarios son capaces de proporcionar los accesos a los recursos de su disposición.

- El modelo de control de acceso obligatorio (MAC) permite el control de los recursos en base al conocimiento del nivel de seguridad, asociando un nivel de seguridad a cada usuario. El sistema de seguridad se encarga de otorgar los respectivos accesos verificando el nivel de cada usuario. Los controles de acceso obligatorio clasifican los accesos o permisos en niveles de clasificación. Cuando el método de control de acceso obligatorio es implementado en una empresa, los usuarios tienen un control restringido de los recursos, es decir, no tienen un control total.
- El modelo de control de acceso basado en roles (RBAC) permite el control de los recursos en base al principio de roles asignados. “Un rol representa una función dentro de una organización” (Jaidi, 2017, p. 86). Este modelo asigna los accesos verificando el rol o roles que tiene cada usuario.
- X-BAC son extensiones para la familia RBAC. Dentro de los modelos X se encuentra: el modelo ORBAC, marco conceptual para satisfacer las necesidades de seguridad en comunicaciones sanitarias sensibles; el modelo RBAC+, modelo dinámico para el control de acceso a bases de datos web; GEO-RBAC, modelo para el control de información espacial.
- El modelo de confidencialidad de Bell-LaPadula es un modelo que proporciona confidencialidad mediante el uso del modelo de control de acceso obligatorio (MAC), autorización de seguridad y clasificación de información. El modelo de confidencialidad de Bell-LaPadula idea un enfoque conceptual donde “el sistema que se está modelando siempre pueda estar en una condición seguridad conocida, es decir, este tipo de modelo es demostrablemente seguro” (Whitman & Mattord, 2018, p. 447). Las normas y reglas proporcionadas por el modelo de confidencialidad de Bell-LaPadula restringen el paso de información de alto nivel a un nivel más bajo.
- El modelo de integridad de Biba es un “modelo de control de acceso que es similar a BLP y se basa en la premisa de que los niveles más altos de seguridad son más dignos de confianza” (Whitman & Mattord, 2018, p. 448). El objetivo del modelo de integridad de Biba es proporcionar un control de acceso que garantice el adecuado nivel de integridad de los recursos. Este modelo asigna niveles de integridad a los usuarios y recursos en base a dos propiedades: integridad simple, donde el usuario tiene acceso de lectura a

un recurso si el nivel del usuario es igual o menor al nivel del recurso; integridad, donde el usuario tiene acceso de escritura a un recurso si el nivel del usuario es superior o igual al nivel del recurso.

- El modelo de integridad de Clark-Wilson se basa en control de cambios. Este modelo implanta un sistema de relaciones usuario-programa-recurso, donde el usuario no cuenta con accesos directos al recurso, sino que utiliza un programa intermediario. El objetivo del modelo de integridad de Clark-Wilson es generar un entorno seguro, donde la seguridad es probada mediante la utilización de actividades separadas.
- El modelo de control de acceso Graham-Denning describe ocho derechos o privilegios de protección, denominados comandos, que pueden ser ejecutados por los usuarios para lograr un efecto en otro usuario o recurso. Estos derechos son: crear objeto, crear usuario, eliminar objeto, eliminar usuario, leer derecho de acceso, otorgar derecho de acceso, eliminar derecho de acceso, transferir derecho de acceso.
- El modelo Harrison-Ruzzo-Ullman proporciona un procedimiento que permite el cambio de privilegios, y la eliminación o agregación de usuarios y recursos. Este modelo está basado en una matriz de control de acceso, incluyendo un conjunto de comandos y privilegios genéricos.
- El modelo Brewer-Nash, también conocido como Muralla China, proporciona un método para evitar conflictos de intereses ocasionados por el acceso a información privilegiada. Este método es conocido como Muralla China porque se crea una pared o muro lógico entre la información y el usuario. Cuando dos usuarios presentan los mismos privilegios o nivel de acceso, ambos no pueden acceder a la misma información.

#### 2.2.2.4. Problemas comunes en control de acceso

El nivel de seguridad dentro de una organización debe tratarse de forma adecuada, respetando los niveles de seguridad y derechos (privilegios) de las personas, tanto empleadores como personas externas a la empresa. Gregory (2011), menciona los problemas más comunes presentes en controles de acceso y cómo manejarlos:

- Las organizaciones deben implementar procesos útiles para la terminación de accesos de los usuarios que ya no trabajan en sus instalaciones. Todas las identificaciones físicas de los usuarios terminados deberían ser recuperadas por la empresa y ser desactivadas.

- Las organizaciones deben establecer procedimientos para los hechos cuando el personal extravía su identificación, evitando que otra persona pueda acceder o suplantar la identidad de otro usuario.
- Las organizaciones deben establecer protocolos y procedimientos para los hechos cuando el personal olvida su identificación.
- Algunas áreas de la empresa necesitan tener buena ventilación y calefacción centralizada, debido a la concurrencia de personas en esas áreas. Esto puede ocasionar que la presión del aire o el mismo ambiente influya en el proceso de seguridad, sobre el control de las puertas. El ambiente puede ocasionar que la puerta no se cierre por completo, ocasionando que cualquier persona ingrese sin autenticarse. Es recomendable que los sistemas de seguridad puedan detectar cuando una puerta está mal cerrada.
- Algunas puertas son más propensas de ocasionar falsas alarmas, especialmente cuando los sensores de movimiento no exploran completamente el área donde se encuentran instalados. Para reducir las falsas alarmas en las áreas donde ocurre este problema con frecuencia, es recomendable utilizar múltiples sensores de movimiento con rangos más amplios.

#### 2.2.2.5. Amenazas en la seguridad y en el control de acceso

Las empresas constantemente sufren ataques físicos y lógicos, donde el objetivo de estos ataques es robar o perjudicar al personal, información o sistemas de información. Whitman & Mattord (2018), menciona 12 categorías generales de amenazas que las empresas deben considerar para aplicar y diseñar las respectivas estrategias de prevención, para controlarlos de forma física y lógica:

- Las empresas desarrollan la propiedad intelectual dentro de sus actividades comerciales. Estas propiedades pueden ser derechos de autor, secretos comerciales, patentes, marcas. La propiedad intelectual de cada empresa está constantemente en amenaza debido a su uso indebido, atentando a la seguridad de la información. La mayoría de los empleados necesitan tener acceso a diversos tipos de propiedad intelectual para cumplir con sus labores, lo que puede ocasionar el robo de ciertas propiedades intelectuales de la empresa.
- La mayoría de los sistemas de información de las organizaciones están interconectadas con otros sistemas interdependientes de soporte. Los sistemas interdependientes de soporte, en cualquier momento, puede sufrir

interrupciones debido a cambios climáticos u otro imprevisto, provocando la degradación de los servicios que brinda la empresa.

- Las personas que no están autorizadas al acceso de un activo, y tratan de acceder de cualquier forma para poder recuperar el activo objetivo, este acto es clasificado como espionaje o traspaso. Estas personas pueden usar diversos métodos para acceder a la información, aprovechándose de vulnerabilidades en la seguridad de la empresa.
- Las fuerzas naturales pueden presentar amenazas a los activos de las organizaciones. Estas amenazas no pueden ser controladas ni advertidas por el personal de seguridad. Existe una variedad de fuerzas naturales, como inundaciones, incendios, terremotos, plagas, rayos, entre otros, afectando a la información, equipos que mantienen la información, y al mismo personal de la empresa.
- En esta categoría comprenden las acciones del personal que son intencionales, maliciosas o por desconocimiento del proceso. Las personas cometen errores en sistemas de información, en el manejo de la información o en dispositivos de seguridad. Por ello, las empresas deberían capacitar al personal y crear procedimientos fáciles de comprender por los empleadores. Cualquier error humano, ya sea el más mínimo, podría ocasionar daños graves.
- La extorsión de información o cyberextorsión comprende acciones con el objetivo de robar información mediante canales electrónicos. Las personas que realizan estos actos utilizan métodos básicos (como el spam), o métodos más avanzados (como el desarrollo de virus informáticos).
- En esta categoría comprenden las acciones de sabotaje a sistemas informáticos o actos de vandalismo que perjudiquen los activos o imagen de la empresa. Estos ataques pueden ser desde actos de vandalismo por parte de los mismos empleadores o actos organizados. El acto que mayor perjudica a una empresa es el daño a la imagen institucional.
- Los ataques de software comprenden acciones que atentan contra la información de la empresa. Estos actos implementan técnicas y métodos de ingeniería social y habilidades informáticas. Cuando se produce la infección a un solo sistema informático de la empresa, provocaría la infección de los demás sistemas mediante la red.
- Las fallas o errores técnicos de hardware son ocasionados cuando un fabricante brinda equipos defectuosos a una empresa. Estas fallas pueden ocasionar que los equipos trabajen de manera irregular, disminuyendo el

nivel de calidad del servicio que brinda la empresa. Los equipos defectuosos pueden presentar los fallos de forma intermitente, lo cual deberían ser revisados o renovados inmediatamente.

- Las fallas o errores técnicos de software son provocados “intencionalmente” por empleados (programadores) de una empresa, dejando “huecos” vulnerables por razones malignas, o errores por la integración de sistemas, donde se pueden revelar fallas no probadas.
- Contar con infraestructura tecnológica obsoleta, puede ocasionar que la integridad de la información se vea perjudicada. Así mismo, los sistemas son más lentos y poco confiables, donde el nivel de servicio de la empresa será altamente criticado.
- Esta categoría es constante en todas las organizaciones. El robo físico podría ser controlado mediante el uso de técnicas de seguridad física, como puertas de control, personal de seguridad, sistemas biométricos, entre otros. Sin embargo, el robo lógico o electrónico es más complejo, debido a que el acto no siempre es evidente.

#### 2.2.2.6. Mejores prácticas en control de acceso

Las organizaciones suelen desarrollar sus políticas o procedimientos tratando de abarcar todos los puntos clave que son más propensos a sufrir ataques, pero al no tener un adecuado conocimiento o solo centrarse en puntos considerados “importantes”, no se abarca la seguridad total de la empresa: un simple fallo o “hueco” en la seguridad, podría ser perjudicial para la empresa y para sus clientes o socios.

Debido a esto, Gregory (2011) y Whitman & Mattord (2018), mencionan una serie de mejores prácticas a considerar para la gestión y manejo de controles de acceso:

- Alinear los objetivos de seguridad con los objetivos de la organización. Un buen programa de seguridad permitirá el apoyo y alineación de los objetivos de seguridad con los objetivos y metas de la empresa.
- Establecer puntos y acuerdos de seguridad, indicados por el departamento de seguridad, dentro del procedimiento de contratación de nuevo personal.
- Deshabilitar y remover cualquier acceso o privilegio de seguridad de los usuarios que ya no se encuentren prestando servicio en la empresa. Así mismo, todas las identificaciones físicas deberán ser retornadas a la empresa.

- Establecer políticas para personas que prestan servicios de terceros, auditores, entre otros. Esta categoría de personal debe ser cuidadosamente gestionada para evitar amenazas a los bienes e información de la empresa.
- Realizar evaluaciones periódicas de riesgos para identificar nuevas amenazas.
- Usar criptografía para el tratamiento de información en la empresa es altamente recomendable. Así mismo, usar criptografía en los identificadores físicos disminuye la posibilidad de clonación y suplantación de identidad.
- Monitorear los registros y bitácoras de los accesos a sistemas o zonas seguras. Esto significa escanear cada registro de acciones para encontrar actividades inusuales, tanto de las personas como de los mismos equipos de control de acceso.
- Utilizar autenticación de tipo multifactor para acceder a zonas de alta seguridad. Combinar dos técnicas de acceso mejora la seguridad y evita que intrusos puedan acceder a los privilegios de otra persona con alguna identificación extraviada.
- Educar a los empleados en la importancia y el uso correcto de los sistemas de control de acceso, para proteger a la empresa y protegerse a sí mismos.
- Prevenir anti-passback para evitar accesos no válidos y prevenir el uso de identificadores clonados.
- Integrar los componentes de seguridad con el dominio de la empresa para un mejor control de todos los recursos de la organización. Optar por un sistema de control de dominio, por ejemplo, Active Directory, otorgando de manera más eficaz los respectivos accesos a los usuarios de una forma más rápida, evitando la demora en agregar o quitar privilegios.
- La empresa debe tener un pensamiento de mejora continua, tratando de mejorar sus procesos y políticas de seguridad, como también los equipos y capacitaciones a los empleadores, para estar un paso delante de personas inescrupulosas que intentan hacer daño a la empresa.

#### 2.2.2.7. Estándares en control de acceso

En la Tabla 4 se visualizan los diversos estándares de seguridad aplicables para procesos de control de acceso, tanto a recursos lógicos (sistemas, archivos digitales, servidores, etc.), y recursos físicos (archivos físicos, espacios físicos de la organización, etc.).

**Tabla 4**

*Estándares para controles de acceso*

| Categoría | Sub Categoría | Estándar |
|---|---|---|
| Gestión de Identidad, Autenticación y Control de Acceso (PR.AC) | PR.AC-1: Las identidades se emiten, gestionan, comprueban, revocan y auditan para usuarios, procesos y dispositivos. | - CIS CSC: 1, 5, 15, 16<br>- COBIT 5: DSS05.04, DSS06.03<br>- ISA 62443-2-1:2009: 4.3.3.5.1<br>- ISA 62443-3-3:2013: SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9<br>- ISO/IEC 27001:2013: A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3<br>- NIST SP 800-53 Rev. 4: AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11 |
| | PR.AC-2: El acceso físico a los recursos tangibles e intangibles se gestionan y protegen. | - COBIT 5: DSS01.04, DSS05.05<br>- ISA 62443-2-1:2009: 4.3.3.3.2, 4.3.3.3.8<br>- ISO/IEC 27001:2013: A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8<br>- NIST SP 800-53 Rev. 4: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8 |
| | PR.AC-4: Se gestionan los privilegios incorporando el principio de separación de funciones y principios de menor privilegio. | - CIS CSC: 3, 5, 12, 14, 15, 16, 18<br>- COBIT 5: DSS05.04<br>- ISA 62443-2-1:2009: 4.3.3.7.3<br>- ISA 62443-3-3:2013: SR 2.1<br>- ISO/IEC 27001:2013: A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5<br>- NIST SP 800-53 Rev. 4: AC-1, AC-2, AC-3, AC- 5, AC-6, AC-14, AC-16, AC-24 |

(continúa)

Tabla 4 (continuación)

| Categoría | Sub Categoría | Estándar |
|---|---|---|
| Gestión de Identidad, Autenticación y Control de Acceso (PR.AC) | PR.AC-6: Las identidades de las personas se prueban, vinculan y afirman en interacciones. | - CIS CSC: 16<br>- COBIT 5: DSS05.04, DSS05.05, DSS05.07, DSS06.03<br>- ISA 62443-2-1:2009: 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4<br>- ISA 62443-3-3:2013: SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1<br>- ISO/IEC 27001:2013: A.7.1.1, A.9.2.1<br>- NIST SP 800-53 Rev. 4: AC-1, AC-2, AC-3, AC- 16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3 |
| | PR.AC-7: Todos los activos están autenticados en relación con el riesgo de operación. | - CIS CSC: 1, 12, 15, 16<br>- COBIT 5: DSS05.04, DSS05.10, DSS06.10<br>- ISA 62443-2-1:2009: 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 |

*Nota*. Adaptado de Barrett (2018).

### 2.2.2.8. Proceso Interno de Control de Acceso al Almacén del Área de Tesorería del Gobierno Regional de Tacna

El Gobierno Regional de Tacna contempla diversos procesos internos para el manejo y administración de sus operaciones cotidianas, ya sean regulados por normativa que aplica a todas las sedes, o divulgados según cada gerencia, subgerencia o área de la misma entidad, de forma particular.

El área de Tesorería del Gobierno Regional de Tacna sigue procedimientos normados y/o divulgados por la misma área. Uno de estos procesos internos del área contempla el proceso de acceso a los almacenes o ambientes donde se encuentran documentos, y demás, necesarios para procesos internos / externos de otras áreas, o procesos de auditoría.

El proceso de control de acceso que contempla el área de Tesorería para el acceso a su almacén, es un procedimiento interno que la misma área sigue, sin documentación publicada. Por ende, al no contar con una documentación referencial que pueda ser citada, se ha realizado una comunicación hablada con un miembro de la subgerencia de Tesorería, donde detalló el proceso interno que es manejado por el área de Tesorería del Gobierno Regional de Tacna para el acceso al almacén ubicado en la sede Hipólito Unanue, el cual se describe a continuación:

a. En la Sede Central del Gobierno Regional de Tacna, el jefe o encargado del área de Tesorería, autoriza y proporciona la llave a la persona para el respectivo acceso al almacén ubicado en la sede Hipólito Unanue. Al no tener la llave de acceso, ésta es solicitada a Seguridad. Comúnmente, el jefe o encargado del área de Tesorería es quien resguarda la llave de acceso.
b. La persona se dirige al almacén ubicado en la sede Hipólito Unanue mediante el uso del transporte del Gobierno Regional de Tacna.
c. En la Sede Hipólito Unanue del Gobierno Regional de Tacna, la persona se presenta ante el personal de seguridad ubicado en la puerta de ingreso a la sede, presentando sus credenciales y motivo de acceso.
d. La persona ingresa al almacén mediante el uso de la llave proporcionada por el jefe o encargado del área de Tesorería.
e. Después de realizar sus operaciones, la persona procede a abandonar y asegurar el almacén, para luego dirigirse a la sede central, mediante el uso del transporte del Gobierno Regional de Tacna.
f. En la Sede Central del Gobierno Regional de Tacna, la persona se presenta ante el personal de seguridad ubicado en la puerta de ingreso a la sede, presentando sus credenciales y motivo de acceso.
g. La persona devuelve la llave al jefe o encargado de la misma área.

Cabe señalar que, durante el proceso de control de acceso al almacén del área de Tesorería, el registro de los accesos que se otorgan para acceder al espacio físico, no es registrado en su totalidad. Este registro, que es de forma manual, muy pocas veces es realizado solo cuando el acceso se le da a un personal externo al área de Tesorería, pero la mayoría de veces, solo es verbal.

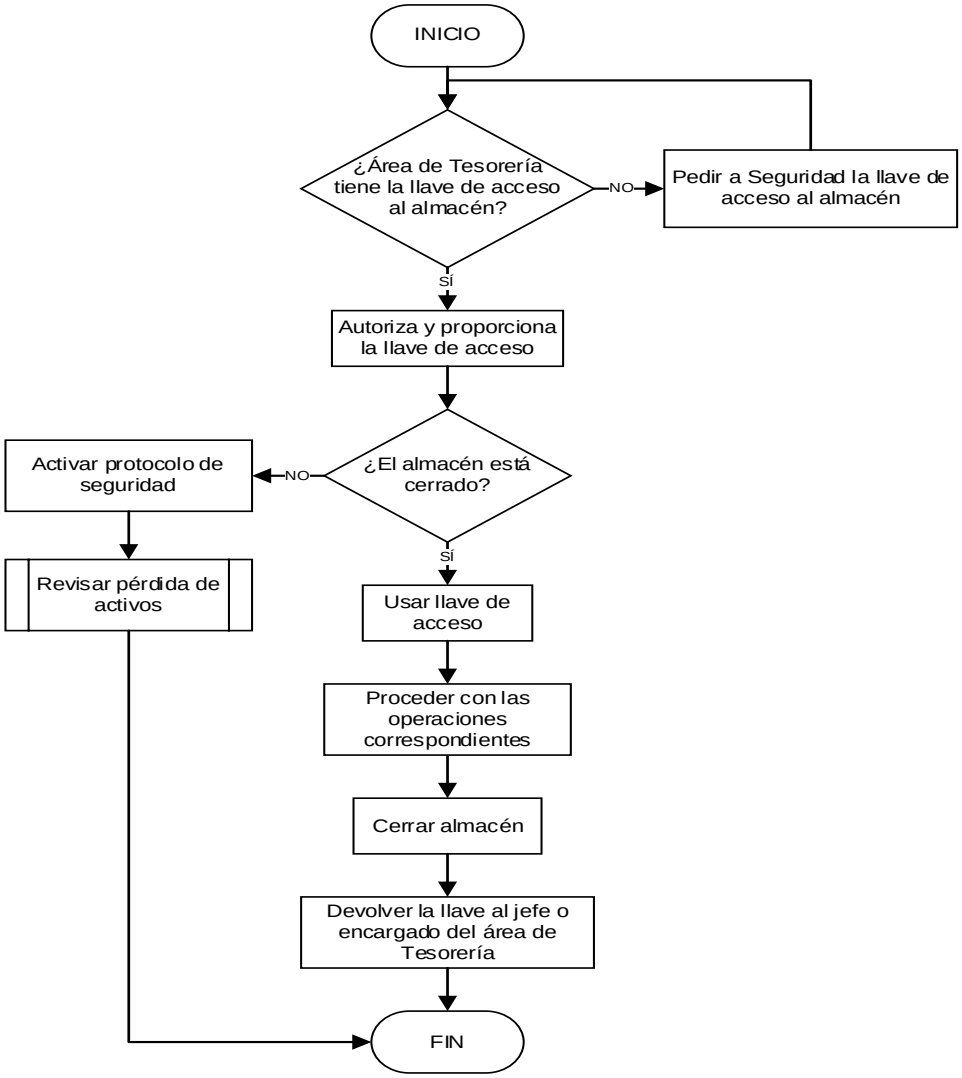
La solución actual que está instalada, y que cumple el rol de control para el acceso al espacio físico que corresponde al almacén del área de Tesorería del Gobierno Regional de Tacna, está constituida por una simple cerradura de doble pivote incrustada en la puerta, con su respectiva llave. No ha sido posible indicar los costos reales y de mantenimiento de la solución actual, debido a la imposibilidad en acceder a la

información detallada de costos que ejecuta el Gobierno Regional de Tacna para el respectivo control de acceso. Del mismo modo, la información detallada de costos no se encuentra publicada en su portal de transparencia.

En la Figura 9 se muestra el diagrama de flujo de procesos donde se indican los pasos del proceso actual de control de acceso descrito anteriormente, desde la otorgación de la llave de acceso a la persona que ingresará al almacén, hasta la respectiva entrega de los documentos y devolución de la llave de acceso proporcionada.

**Figura 9**

*Proceso interno de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna*



### 2.2.3. Deep Learning

#### 2.2.3.1. Machine Learning

Machine Learning o aprendizaje automático “es una forma de IA que permite que un sistema aprenda de los datos en lugar de a través de la programación explícita” (Hurwitz & Kirsch, 2018, p. 4). Machine Learning usa varios algoritmos para aprender de los datos, y poder realizar predicciones de los resultados. Cuando los algoritmos de Machine Learning reciben datos de entrenamiento de calidad, se pueden crear modelos más exactos. El aprendizaje automático, actualmente, es muy esencial para la creación de modelos analíticos.

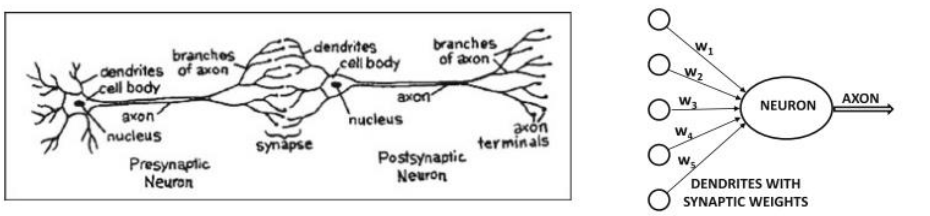
“El aprendizaje automático es la programación de computadoras para optimizar un criterio de rendimiento utilizando datos de ejemplo o experiencias pasadas” (Alpaydin, 2020, p. 3). Los modelos de Machine Learning puede ser: predictivos, para el uso de predicciones; descriptivos, para el conocimiento de datos.

El aprendizaje automático se basa en teorías de estadística y no mucho en modelos matemáticos, porque el objetivo principal del aprendizaje continuo es inferir a partir de muestras. El desempeño de los algoritmos de Machine Learning puede ser tan esencial como la precisión en predicciones. Las soluciones de Machine Learning tienen diferentes enfoques, como el reconocimiento, visión o robótica, ayudando a las organizaciones en sus objetivos.

Machine Learning está comprendido por neuronas artificiales, simulando neuronas biológicas, donde la unidad (nodo o neurona) se denomina perceptrón (Alom et al., 2019). En la Figura 10 se observa la comparación entre neuronas biológicas reales de un ser vivo (imagen izquierda), y neuronas artificiales (inteligencia artificial) simulando neuronas biológicas (imagen derecha).

**Figura 10**

*Comparación estructural entre neuronas biológicas y neuronas artificiales*




(a) Biological neural network (b) Artificial neural network

*Nota*. Elaborado por Aggarwal (2018).

#### 2.2.3.1.1. Enfoques de Machine Learning

Machine Learning requiere de técnicas para poder mejorar su precisión predictiva. Para encontrar y usar las respectivas técnicas, primero se debe precisar la naturaleza del problema comercial, ya que existen diferentes enfoques según la cantidad de datos a procesar. Según Hurwitz & Kirsch (2018), existen cuatro enfoques del aprendizaje continuo:

- El aprendizaje supervisado empieza con un conjunto de datos y el entendimiento de cómo están clasificados tales datos, para encontrar patrones y aplicar un análisis. Los datos tratados están etiquetados, definiendo el significado de cada dato. Debido a que los datos están etiquetados, las personas que realizan el modelo de Machine Learning entienden a detalle cada dato.
- El aprendizaje no supervisado es recomendable cuando la situación del problema no necesita datos etiquetados. La clasificación de los datos se basa según los patrones o grupos con mismas características.
- El aprendizaje reforzado es un tipo de modelo conductual. Los algoritmos utilizados en este enfoque reciben una retroalimentación de los datos analizados, logrando un mejor resultado. El aprendizaje reforzado no está entrenado con el conjunto de datos de muestra, sino que es entrenado en base a prueba y error.
- Una red neuronal de Machine Learning comprende una capa inicial de entrada, seguida de varias capas ocultas, y una capa final de salida. El aprendizaje profundo utiliza redes neuronales con múltiples capas interconectadas para poder aprender de los datos ingresados. El aprendizaje profundo necesita más datos de entrada que los que requiere un modelo de Machine Learning habitual.

#### 2.2.3.1.2. Tipos de algoritmos de Machine Learning

Según Hurwitz & Kirsch (2018), existen los siguientes tipos de algoritmos de Machine Learning que los científicos de datos pueden seleccionar según el contexto del problema en cuestión:

- Los algoritmos bayesianos facilitan codificar conocimientos previos de cómo deberían estar los modelos sin tomar en cuenta lo que indiquen los datos. Estos algoritmos son esenciales cuando no se cuenta con grandes cantidades de datos para ser entrenados en un modelo.

- Los algoritmos de agrupamiento son más sencillos de utilizar, donde los datos se agrupan por patrones similares. Los objetos dentro de un clúster tienen las mismas características, muy diferentes a los demás clústeres. El algoritmo de agrupamiento interpreta los parámetros ingresados de los objetos, y los agrupa según patrones.
- Los algoritmos de árbol de decisión se basan en una estructura ramificada para la visualización de los resultados obtenidos de una decisión. Los nodos del árbol de decisión definen un posible resultado, donde los porcentajes de cada nodo aumenta o disminuye la probabilidad de que ocurra el resultado.
- La reducción de dimensionalidad mejora los datos a ser analizados. Los algoritmos eliminan datos redundantes, valores no útiles o atípicos, con el fin de tener datos más limpios.
- Los algoritmos basados en instancias son utilizados cuando nuevos puntos de datos son requeridos para su clasificación en base a la similitud con los datos de entrenamiento. Estos algoritmos no cuentan con una etapa de entrenamiento.
- Los algoritmos de regresión lineal son utilizados para tareas estadísticas. Estos algoritmos ayudan a los analistas a establecer las respectivas relaciones entre puntos de datos. Los algoritmos de regresión lineal son útiles para la predicción de valores futuros, siempre y cuando existan datos históricos. Si no se conoce el contexto del problema y de lo datos, la predicción no será la correcta.
- La regularización evita el problema de sobreajuste en modelos de Machine Learning. Esta técnica reduce la complejidad de los modelos que son más propensos a sufrir overfitting. Cuando un modelo presenta overfitting, la predicción será incorrecta.
- Los algoritmos de aprendizaje automático basado en reglas usan diferentes reglas relacionales para la descripción de datos. Los sistemas basados en reglas son más sencillos de entender y utilizar. Pero, cuando los sistemas son tendientes a ser operacionales, el enfoque basado en reglas se vuelve más complejo.

#### 2.2.3.2. Deep Learning

Deep Learning o aprendizaje profundo “está diseñado para emular cómo funciona el cerebro humano para que las computadoras puedas ser entrenadas para lidiar con abstracciones y problemas que están mal definidos” (Hurwitz & Kirsch, 2018, p. 17).

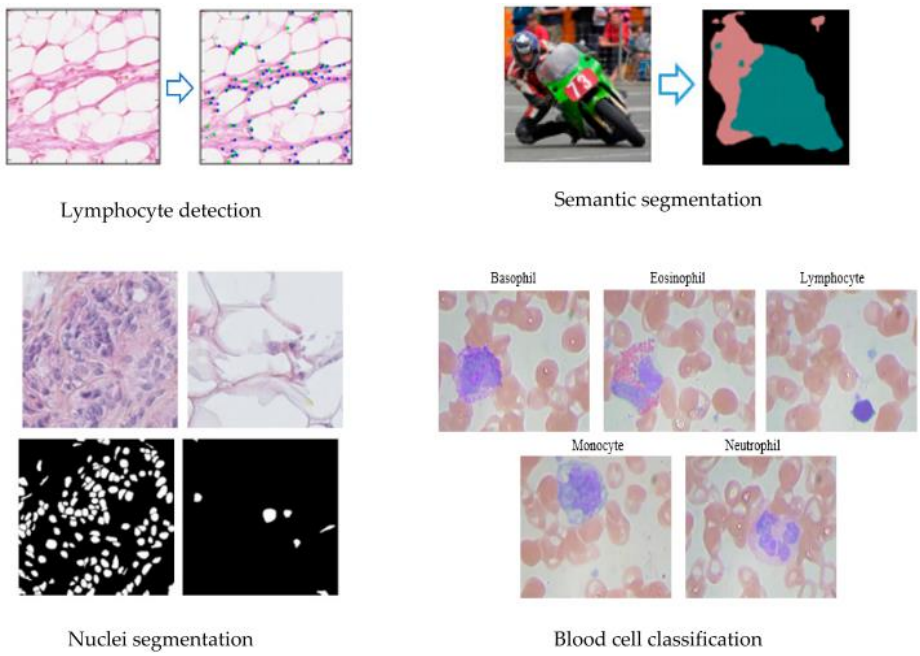
Una persona, a mínima edad, puede diferenciar los rostros de diferentes personas. En cambio, una computadora tendría que realizar mucho procesamiento para diferenciar entre las personas. Este tipo de red es comúnmente utilizado en aplicaciones de imágenes, visión por computadora, voz, entre otros.

El aprendizaje profundo utiliza redes jerárquicas para el proceso de aprendizaje, combinando (o no) algoritmos supervisados o no supervisados. “El aprendizaje profundo, a menudo, se llama una disciplina del aprendizaje automático” (Hurwitz & Kirsch, 2018, p. 18). La estructura neuronal del aprendizaje profundo es similar a las redes neuronales tradicionales, solo que tendrá más capas ocultas. Si el problema es complejo, entonces habrá más capas ocultas.

El aprendizaje profundo se caracteriza por el conjunto poderoso de modelos en los que se puede enfocar. Estos modelos de aprendizaje profundo están compuestos por diversas transformaciones continuas de datos que se procesan de arriba hacia abajo. Así mismo, los frameworks de Deep Learning están jugando un papel muy importante para ayudar a las personas a diseñar modelos más sencillos de aprendizaje profundo, tales como Torch, Caffe, Theano, Tensorflow, Keras, entre otros (A. Zhang et al., 2020). En la Figura 11 se muestran algunas de las diversas aplicaciones de Deep Learning que utilizan procesos de visión computacional para solucionar diferentes problemas de la realidad, ya sea utilizando frameworks o modelos tradicionales.

**Figura 11**

*Ejemplos del uso de Deep Learning*



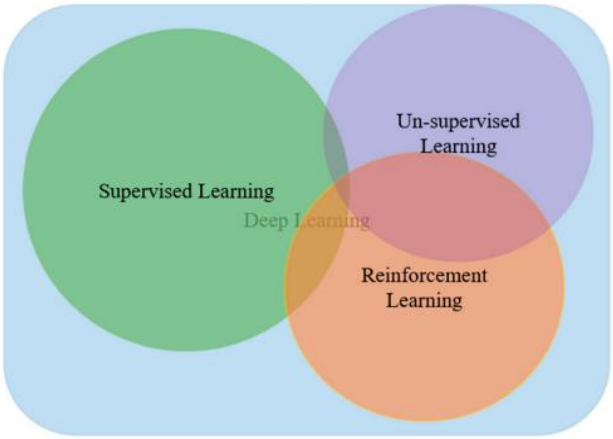

*Nota*. Elaborado por Alom et al. (2019).

#### 2.2.3.2.1. Enfoques de Deep Learning

En la Figura 12 se visualizan los enfoques de Deep Learning indicados por Alom et al. (2019), agrupándolos en tres grandes grupos de aprendizaje, cada uno con un propósito y necesidad particular.

**Figura 12**

*Enfoques de Deep Learning*




*Nota*. Elaborado por Alom et al. (2019).

- El aprendizaje supervisado profundo utiliza datos etiquetados. El entorno de esta técnica está conformado por un conjunto de entradas y salidas. El agente inteligente se encargará de modificar los parámetros de la red neuronal de forma iterativa para obtener un mejor resultado en las salidas. Existen diversos enfoques dentro del aprendizaje supervisado, como las redes neuronales convolucionales (CNN), redes neuronales recurrentes (RNN), redes neuronales profundas (DNN).
- El aprendizaje profundo sin supervisión utiliza datos sin que se encuentren etiquetados. El agente inteligente aprende características comunes para relacionar los datos de entrada. La agrupación, técnicas generativas, y reducción de la dimensionalidad, son considerados enfoques dentro del aprendizaje profundo sin supervisión. Dentro de la familia del enfoque de aprendizaje profundo, se encuentran las máquinas de Boltzmann restringidas (RBM), codificadores automáticos (AE), redes adversas generativas (GAN), y las redes neuronales recurrentes (RNN).
- El aprendizaje de refuerzo profundo es utilizado para entornos desconocidos. Este enfoque empezó con Google Deep Mind en 2013, utilizando desde esa fecha, varios métodos propuestos para el aprendizaje

reforzado. El aprendizaje de refuerzo profundo “también se denomina aprendizaje semi-supervisado” (Alom et al., 2019, p. 3). Existen diversas técnicas de tipo no supervisado y semi-supervisado que emplean este tipo de enfoque. Dependiendo del contexto del problema, se puede elegir el tipo de aprendizaje reforzado que se necesita utilizar. Si se cuenta con demasiados datos y parámetros, se puede utilizar el aprendizaje de refuerzo profundo (DRL).

#### 2.2.3.2.2. ¿Por qué usar Deep Learning?

Deep Learning o aprendizaje profundo es una técnica o método que tiene diferentes enfoques, utilizado comúnmente para aplicaciones de visión por computadora. Alom et al. (2019), explica el por qué utilizar deep learning en las aplicaciones de inteligencia artificial:

- Deep Learning presenta un enfoque de aprendizaje universal, debido a que este método puede ser aplicado a problemas de negocio, o a cualquier dominio de aplicación.
- Deep Learning es robusto, debido a que el diseño de aprendizaje profundo no necesita características diseñadas exactamente. Las tareas consideradas óptimas son aprendidas por el modelo de aprendizaje profundo, resultando en un modelo más sólido a variaciones naturales proporcionados por los datos de entrada.
- Deep Learning es generalizado, debido a que el enfoque del aprendizaje profundo puede ser utilizado en diferentes aplicaciones, o usar el modelo con diferentes datos. A este enfoque se le denomina transferencia de aprendizaje, y puede ser útil cuando no se cuenta con muchos datos.
- Deep Learning es escalable. Microsoft desarrolló un modelo de aprendizaje profundo denominado ResNet, con 1202 capas, que puede ser implementado, a menudo, en una escala de supercomputación.

#### 2.2.3.2.3. Red Neuronal Profunda (DNN)

Las redes neuronales profundas, o por sus siglas en inglés DNN, son “una versión avanzada de las redes neuronales artificiales convencionales (ANN)” (Balas et al., 2019, p. 152). Una red neuronal artificial está compuesta por múltiples capas, que procesan información sin procesar mediante funciones de activación. Cada neurona está asociado a sesgos y pesos. Las redes neuronales profundas han tenido grandes éxitos

en procesamiento de imágenes, procesamiento del lenguaje natural, y reconocimiento (biometría) (Balas et al., 2019).

Las redes neuronales profundas puedes ser diseñados con múltiples capas ocultas, ubicados entre la capa de entrada y la capa de salida de la red neuronal. Este tipo de red utiliza varias neuronas que reciben señales como entrada. Estas señales son integradas linealmente con los pesos, y transferidos sobre las tareas no lineales para dar como resultado las respectivas salidas (Dargan et al., 2019).

Cuando se habla de redes neuronales profundas, se supone que la red neuronal tendrá múltiples capas ocultas, que servirán para la extracción de características de los datos de entrada y para el cálculo de funciones complejas. Al ser una red profunda, la cantidad de datos de entrada deberá ser mayor para un mejor resultado en la salida de la red.

Según Shrestha & Mahmood (2019), la implementación de una red neuronal (de cualquier enfoque) está desarrollado en base a los siguientes pasos (en orden): adquirir los respectivos datos para entrenamiento y pruebas; entrenar la red neuronal; realizar predicciones con los datos de prueba. Los más expertos recomiendan separar los datos en: datos de entrenamiento, datos de pruebas, datos de validación.

Alom et al. (2019), describe funciones y técnicas que están presentes en una red neuronal profunda para obtener un mejor resultado:

- El descenso de gradiente es un algoritmo de optimización utilizado en redes neuronales para la minimización de cualquier función. Este algoritmo se ha utilizado en redes neuronales artificiales desde hace dos décadas.
- El descenso de gradiente estocástico (SGD) es utilizado para el entrenamiento de redes neuronales profundas. Este método solo utiliza una entrada de ejemplo por cada iteración. Si en la red neuronal existen demasiadas iteraciones, el descenso de gradiente estocástico podría no ser el mejor.
- Las redes neuronales profundas habitualmente están entrenadas con el algoritmo de propagación hacia atrás (Back-Propagation). Este algoritmo usa el descenso de gradiente para la disminución de errores, ajustando los pesos de la red neuronal basados en la derivada parcial del error que existe en cada peso.
- Momentum es un método que proporciona una mejora en el rendimiento del proceso de entrenamiento con el enfoque de descenso de gradiente estocástico (SGD). Este método podría ser eficaz para salir de pequeños

mínimos locales, donde una red neuronal sin Momentum se detendría. El objetivo principal de Momentum es de usar un promedio móvil del gradiente para evitar el uso de valor actual del mismo gradiente.

- La tasa de aprendizaje es un elemento necesario en el desarrollo de una red neuronal profunda. Este elemento es el tamaño del paso que es considerado durante el proceso de entrenamiento de la red, haciéndolo más rápido. Seleccionar la tasa de aprendizaje para la red neuronal es un poco complicado y sensible. Una tasa de aprendizaje mayor provocará que la red comience a divergir en lugar de converger. Caso contrario, la red se demorará en entrenarse, o simplemente se detendrá.
- La decadencia o pérdida de peso es utilizado para redes neuronales profundas, como un enfoque de regularización. Este método ayuda a prevenir el sobreajuste o overfitting de la red.

#### 2.2.3.2.4. Red Neuronal Siamesa (SNN)

Una red neuronal siamesa, o por sus siglas en inglés SNN, “es una clase de arquitectura de redes neuronales que contienen dos o más subredes (CNN) que comparten todos sus parámetros y pesos” (como se cita en Gulyaev & Filchenkov, 2020, p. 243). Las áreas de aplicación son aquellas donde se requiere encontrar similitudes o relaciones entre dos objetos.

Según O’ Mahony et al. (2019), los atributos de las redes neuronales siamesas contienen:

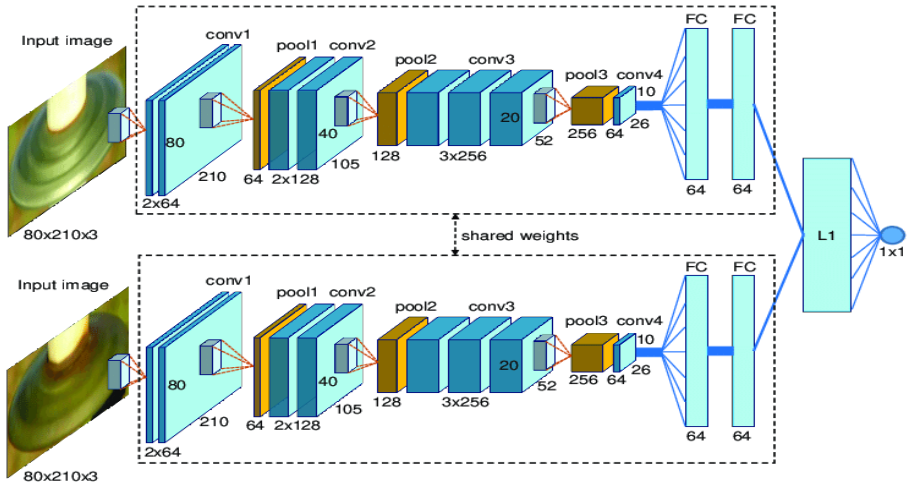
- Son capaces de aprender ciertas características genéricas de imágenes para realizar predicciones de imágenes de clases desconocidas, incluso si estas imágenes desconocidas tienen pocos ejemplos para su clasificación.
- Cuentan con la aptitud para realizar un entrenamiento de los objetos mediante técnicas de optimización estándar en base a una función de pérdida, determinando la respectiva similitud.
- Son capaces de ser efectivos con tan solo poco conocimiento específico del dominio u objetos.
- Son capaces de manejar una gran cantidad de datos.

El desarrollar un modelo que clasifique las imágenes mediante One-Shot Learning (aprendizaje de una sola toma), supone el hecho de que el modelo aprenda a discriminar entre las clases del conjunto de datos, es decir, establecer cuán probable es que una imagen pertenezca a la misma clase de otra imagen. El puntaje resultante

de la comparación entre las dos imágenes a discriminar, es verificado mediante un umbral, confirmando o no la imagen de prueba ante el conjunto de datos de identidades almacenadas (O' Mahony et al., 2019). En la Figura 13 se visualiza la arquitectura de una red neuronal siamesa aplicada a un problema de comparación y reconocimiento de imágenes, del cual se puede observar las diversas capas ocultas y sus respectivos tipos.

**Figura 13**

*Ejemplo de una red neuronal siamesa (SNN)*




*Nota*. Elaborado por Sampedro et al. (2019).

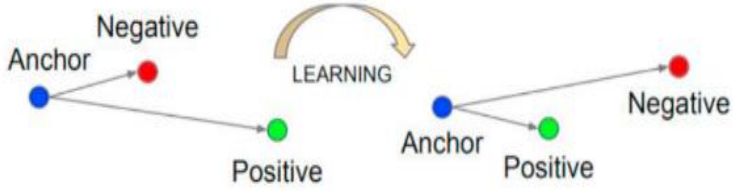
O' Mahony et al. (2019), definen los siguientes conceptos utilizados en una red neuronal siamesa:

- Dos imágenes "A" y "B" son comparados mediante el cálculo de la distancia "d". Si el resultado de la distancia "d" es menor a un umbral establecido (hiperparámetro), significa que las dos imágenes pertenecen a la misma clase. La distancia utilizada se denomina "distancia euclidiana" o "distancia euclidiana al cuadrado".
- La función de pérdida de triplete es una técnica avanzada donde se obtiene tres tipos de imágenes: "A", que representa a la imagen de anclaje; "P", que representa a una imagen positiva; "N", que representa a una imagen negativa. Esta función denota que la distancia entre dos muestras de la misma clase es más pequeña que la de diferentes clases, considerando un margen (hiperparámetro) para "juntar" la imagen de anclaje "A" con la imagen positiva "P", y alejar la imagen de anclaje "A" con la imagen negativa "N", evitando resultados triviales. En la Figura 14 se visualizan los tres tipos de

imágenes que participan dentro de la función de pérdida de triplete, resaltando la diferencia de distancia o similitud entre imágenes pertenecientes a la misma clase, y clases distintas.

**Figura 14**

*Función de pérdida de triplete*




*Nota*. Elaborado por O' Mahony et al. (2019).

### 2.2.3.2.5. Red Neuronal Convolucional (CNN)

Una red neuronal convolucional, o por sus siglas en inglés CNN, "es una red neuronal con múltiples capas y se basa en la corteza visual animal" (Dargan et al., 2019, p. 3). Las áreas de aplicación de las redes neuronales convolucionales comprenden aquellos orientados al procesamiento de imágenes y reconocimiento de patrones. Las capas anteriores de la red detectan características como los bordes de la imagen, y las capas superiores son utilizados para las características de alto nivel. Luego se aplica un proceso que disminuye la dimensionalidad de las características procesadas.

Según Shrestha & Mahmood (2019), una red neuronal está basado en la corteza visual humana y es una red comúnmente utilizada en visión por computadora. Este tipo de arquitectura de red profunda también es utilizada en áreas del lenguaje de procesamiento natural (PNL). Cada capa convolucional de la red realiza el proceso de extracción de características, siendo más refinada en cada capa que va desde la capa de entrada hasta la capa de salida.

Según Yamashita et al. (2018), una red neuronal convolucional está compuesto por los siguientes elementos:

- La capa convolucional es un elemento importante dentro de la arquitectura de redes neuronales convolucionales con el propósito de extraer características. Esta capa consiste en combinaciones de operaciones lineales y no lineales, operaciones de convolución y funciones de activación. La capa convolucional "forma la unidad fundamental de un ConvNet en lo que respecta a la mayor parte del cálculo" (Sakib et al., 2018, p. 2). Cuando

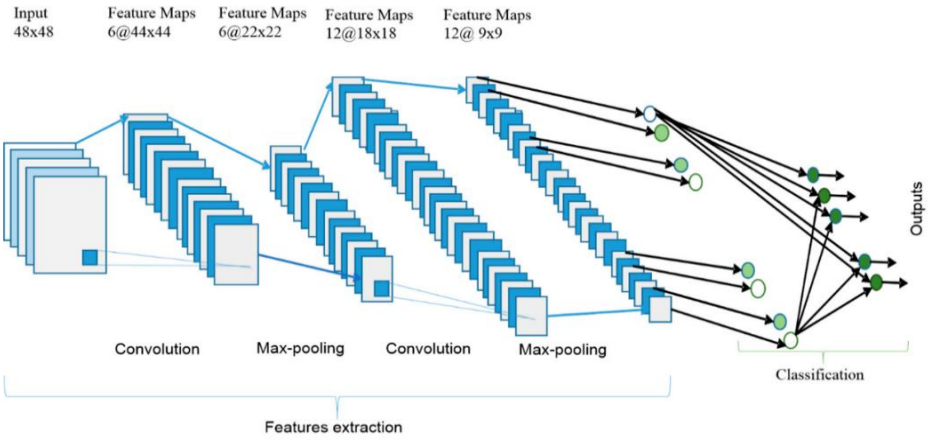
la capa convolucional recibe la información, ésta invoca los filtros (también denominados kernels) mediante la dimensionalidad espacial de datos para generar un mapa de activación en 2D. Las salidas del proceso de convolución son procesados mediante funciones de activaciones no lineal. Estas funciones de activación pueden ser TANH, sigmoides o la función ReLU, siendo esta última mayor utilizada para el entrenamiento de redes neuronales debido a la rapidez que proporciona. Así mismo, la función SOFTMAX se puede aplicar a la última capa para mejorar aún más el rendimiento de la red (Sakib et al., 2018).

- La capa de agrupamiento proporciona la disminución de muestras, reduciendo la dimensionalidad de los mapas de características, disminuyendo la cantidad de parámetros que se aprenderán posteriormente. “Las operaciones de agrupación reducen las dimensiones de los mapas de características” (Sakib et al., 2018, p. 3). Se sugiere que las capas de agrupamiento se deban colocar después de una capa convolucional, donde la salida de la capa convolucional es la entrada de la capa de agrupamiento. Existen diversas operaciones de agrupación, como. agrupación máxima (max-pooling), agrupación promedio, agrupación espectral, agrupación estocástica, agrupación de pirámides espaciales, agrupación de normas L2, agrupación sin orden de múltiples escalas (Sakib et al., 2018).
- El mapa de características de la última capa convolucional se “aplana”, es decir, esta capa se convierte a una dimensión 1D, y se conecta a una o varias capas completamente conectadas, también llamadas capas densas, dando como resultado la probabilidad de clasificación de cada clase. Generalmente, la última capa completamente conectada tiene la misma cantidad de nodos de salida que la cantidad de clases a predecir. La salida de la capa completamente conectada es transferida a una capa de salida donde se podrá utilizar una función SOFTMAX o sigmoide para la predicción de las clases entrenadas (Sakib et al., 2018).

La Figura 15 muestra la arquitectura de una red neuronal convolucional artificial, donde se observan las capas ocultas, extracciones de características mediante la aplicación de kernels (filtros), la sección de aplanamiento de la red, y el respectivo proceso de clasificación / detección según el dato de entrada inicial.

**Figura 15**

*Arquitectura de una red neuronal convolucional (CNN)*




*Nota*. Elaborado por Alom et al. (2019).

### 2.2.3.2.6. Arquitecturas Populares de CNN

Según Alom et al. (2019), Sakib et al. (2018) y Shrestha & Mahmood (2019), las arquitecturas CNN más populares son:

- La configuración básica de LeNet está compuesto por dos capas convolucionales, dos capas de submuestreo, dos capas completamente conectadas y una capa de salida con conexión gaussiana.
- La configuración de AlexNet está compuesto por una primera capa convolucional que realiza el proceso de convolución y el proceso de agrupación máxima (max-pooling) con normalización de respuesta local, utilizando 96 filtros de 11 x 11. El tamaño de los filtros de la agrupación máxima es de 3 x 3. Luego se utiliza filtros de 5 x 5. Al final de la red, existen dos capas completamente conectadas con activación SOFTMAX.
- La arquitectura ZFNet es una mejora a la arquitectura AlexNet. ZFNet usa kernels de 7 x 7, en vez de kernels de 11 x 11 (utilizados en AlexNet), con el fin de reducir el número de pesos.
- La arquitectura de VGGNet está compuesto por dos capas convolucionales que utilizan la función de activación ReLU, una capa de agrupación máxima, y varias capas completamente conectadas que utilizan la función de activación ReLU. La última capa de la arquitectura es una capa SOFTMAX para clasificar las clases entrenadas. Existen cuatro modelos de VGGNet: VGG-E, VGG-11, VGG-16, VGG-19.
- La característica principal de GoogleNet es la reducción de parámetros dentro de la red en el módulo de inicio llamado Inception-v1 (de 60 millones

de parámetros de AlexNet, a 4 millones). Actualmente, GoogleNet ha ido mejorando, implementando actualizaciones en su módulo Inception, con la versión más actual: Inception-v4.

- La arquitectura ResNet tiene conexiones de omisión únicas, y utiliza normalización por lotes (batch normalization). Esta arquitectura no presenta capas completamente conectadas al final de la red. La desventaja presentada por esta red es en el rendimiento; debido a la gran cantidad de parámetros que procesa, el rendimiento es costoso.
- La arquitectura DenseNet está constituido por capas neuronales convolucionales densamente conectadas. Esta arquitectura presenta varios bloques densos y de transición, que son colocados entre dos bloques densos adyacentes.
- La arquitectura Inception se utiliza en redes neuronales convolucionales (CNN), permitiendo un mejor cálculo y la reducción de la dimensionalidad con convoluciones de 1 x 1. Esta arquitectura fue desarrollada para prevenir grandes gastos computacionales, el sobreajuste y otros problemas comunes.

#### 2.2.3.2.7. Limitaciones de Deep Learning

Deep Learning ha progresado significativamente en los últimos años, incluso superando la capacidad del ser humano en la clasificación de imágenes. Pero, existen diversas dificultades técnicas que limitan la capacidad del aprendizaje profundo. Las redes neuronales requieren grandes cantidades de datos de entrenamiento para obtener un mejor resultado, consumiendo enormemente mayores recursos que de un ser humano realizando las mismas tareas.

Aggarwal (2018), describe dos limitaciones importantes en redes neuronales de aprendizaje profundo:

- En tareas como la clasificación de imágenes, donde el rendimiento ha excedido a la capacidad humana, ha demostrado debilidades en establecer la cantidad de muestras. El aprendizaje profundo necesita muchos datos de entrada para poder clasificar de forma correcta. Por ejemplo, una persona puede aprender la diferencia entre objetos del mundo real si necesidad de ver o “entrenar” muchas imágenes del mismo objeto; en cambio, el aprendizaje profundo sí. Desarrollar nuevas formas de transferencia de

aprendizaje puede mejorar el tiempo y disminuir la cantidad de datos de entrenamiento.

- Las aplicaciones de aprendizaje profundo, comúnmente, realizan sus procesos en hardware de alto rendimiento, causando demasiado gasto de energía. Por ejemplo, una aplicación de aprendizaje profundo utiliza más de 1kW; el cerebro humano utiliza solo 20W de energía. Actualmente, se han desarrollado diversos algoritmos que disminuyen el consumo de energía de los procesos de aprendizaje profundo. Además, reducir la cantidad de conexiones neuronales mejora la eficiencia energética y ayuda en la regularización de la red neuronal.

#### 2.2.3.2.8. Aplicaciones de Deep Learning

Según Dargan et al. (2019), existe una variedad de aplicaciones que pueden ser desarrollados con el uso de Deep Learning:

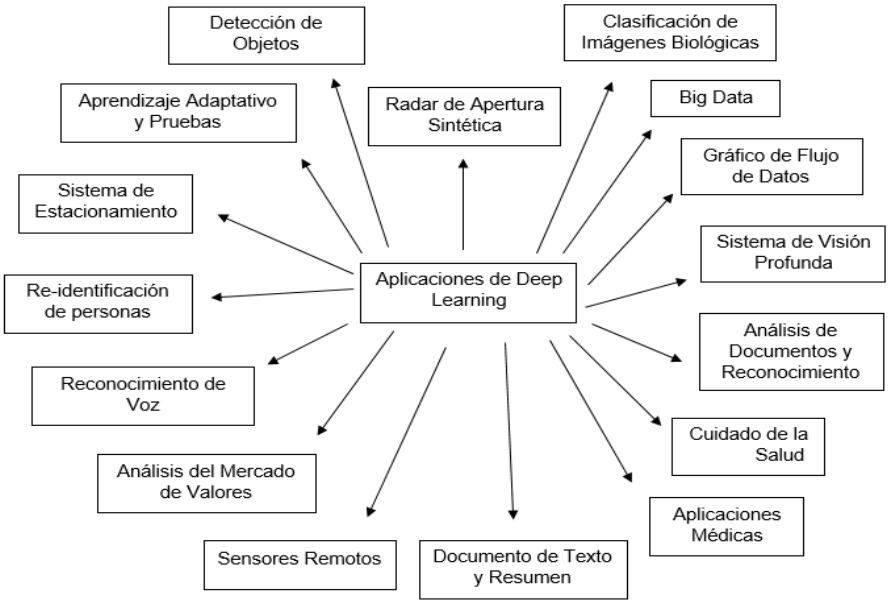
- La aplicación de Deep Learning en la industria automotriz apoya a las personas a identificar, aprender y examinar automáticamente propiedades de los vehículos.
- Los desafíos de aplicar Deep Learning en Big Data han sido aceptados por muchos investigadores. El aprendizaje profundo puede generar grandes resultados notables e identificar patrones desconocidos con alto nivel de abstracción, difícil de entender por las personas.
- La aplicación de Deep Learning permite crear aplicaciones de navegación autónoma. Se utiliza el aprendizaje profundo para ubicar el objeto en un marcador, ayudándose también de cámaras de profundidad. Así mismo, el aprendizaje profundo permite la creación de aplicaciones de video en tiempo real: detectar, identificar y rastrear objetos en un video.
- Existen diversas aplicaciones implementadas con aprendizaje profundo para el tratamiento de datos médicos. Varias propuestas de redes neuronales están enfocados a aplicaciones de atención médica, diagnóstico asistido, interpretación de imágenes, fusión de imágenes, registro y segmentación de imágenes, logrando una mejor atención médica y predicción de enfermedades.
- El aprendizaje profundo es mayormente utilizado para el reconocimiento y clasificación de imágenes, como el reconocimiento de rostros, huellas digitales, clasificación de objetos del mundo real, entre otros.

- El aprendizaje profundo también es utilizado con mayor frecuencia para la detección de objetos. Tanto para el reconocimiento, clasificación y detección de objetos, existen diversos conjuntos de datos de objetos del mundo real para poder entrenar una red neuronal, según el contexto del problema a resolver. Los conjuntos de datos más utilizados por investigadores son: ImageNet, Pascal Voc, CoCo. También se pueden generar conjuntos de datos personalizados utilizando alguna herramienta de segmentación.
- El concepto de aprendizaje profundo dentro de ciudades inteligentes está asociado al uso de tareas de detección, seguimiento y reconocimiento de objetos. Las herramientas implementadas con aprendizaje profundo deben procesar, en tiempo real, las imágenes y videos capturados para ser analizados.

En la Figura 16 se visualizan las diversas aplicaciones que se logran desarrollar e implementar mediante el uso de Deep Learning como herramienta principal para el procesamiento de datos e imágenes según la problemática o situación de la realidad a resolver o automatizar.

**Figura 16**

*Aplicaciones de Deep Learning*




*Nota*. Elaborado y traducido de Dargan et al. (2019).

## 2.3. Definición de Términos

### 2.3.1. Iris

El iris es una estructura visible a través de la córnea que proporciona color a los ojos. En el centro del iris se encuentra la pupila, que es una abertura que sirve para el ingreso de la luz. La pupila es de color negro y varía de tamaño según la cantidad de luz que el ojo pueda percibir. El iris actúa como un diafragma y regula su tamaño dejando el pase de la luz (Ferreruela, 2007).

### 2.3.2. Biometría

La formulación de la palabra biometría proviene del griego *bios* (vida) y *metron* (medida). La biometría comprende tecnologías y técnicas para identificar a las personas. La tecnología biométrica presenta varios enfoques, donde el objetivo principal es de favorecer una forma más segura a los métodos tradicionales existentes para controles de acceso, usados para la protección de bienes personales o empresariales (Gregory & Simon, 2008).

### 2.3.3. Reconocimiento de iris

El reconocimiento de iris representa un medio para obtener una imagen del iris humano mediante una foto, y luego almacenarlo de forma digital o electrónica. Los sistemas de reconocimiento de iris están enfocados a diversas aplicaciones y usos, como el acceso a instalaciones, el rastreo de seres humanos perdidos, generación de informes de asistencia para grandes sistemas corporativos (Ravin, 2016).

### 2.3.4. Control de acceso

El control de acceso representa un proceso donde las personas realizan una solicitud para obtener acceso a ciertos activos, según la otorgación o denegación de la herramienta de control de acceso. La decisión de otorgar los accesos correspondientes a las personas se aplica mediante políticas de seguridad establecidas (Samarati & de Vimercati, 2001).

### 2.3.5. Machine Learning

Machine Learning o aprendizaje automático es un tipo de inteligencia artificial que permite que un sistema pueda aprender un conjunto de datos mediante la programación

explícita. Machine Learning usa varios algoritmos para aprender de los datos, y poder realizar predicciones de los resultados (Hurwitz & Kirsch, 2018).

### 2.3.6. Deep Learning

Deep Learning o aprendizaje profundo emula el funcionamiento del cerebro humano para que las computadoras puedan ser entrenadas y enfrenten problemas del mundo real. Este tipo de red es comúnmente utilizado en aplicaciones de imágenes, visión por computadora, voz, entre otros (Hurwitz & Kirsch, 2018).

### 2.3.7. Aprendizaje supervisado profundo

El aprendizaje supervisado profundo utiliza datos etiquetados. El entorno de esta técnica está conformado por un conjunto de entradas y salidas. Existen diversos enfoques dentro del aprendizaje supervisado, como las redes neuronales convolucionales (CNN), redes neuronales recurrentes (RNN), redes neuronales profundas (DNN) (Alom et al., 2019).

### 2.3.8. Red neuronal convolucional

Una red neuronal convolucional, o por sus siglas en inglés CNN, es una red neuronal conformada por múltiples capas, basándose en la corteza visual. Las áreas de aplicación de las redes neuronales convolucionales comprenden aquellos orientados al procesamiento de imágenes y reconocimiento de patrones (Dargan et al., 2019).

### 2.3.9. Red neuronal siamesa

Una red neuronal siamesa, o por sus siglas en inglés SNN, es una red neuronal cuyo objetivo es determinar la similitud entre dos objetos (imágenes). Estas imágenes pasan por dos redes neuronales convolucionales (CNN) idénticas, que comparten los mismos parámetros y pesos. Usando el aprendizaje de una sola captura (One-Shot Learning) se considera el hecho de que no se necesita una gran cantidad de imágenes de una clase para ser determinada igual o no con respecto a otra clase almacenada (O' Mahony et al., 2019).

### 2.3.10.Raspberry Pi

Raspberry Pi es una computadora funcional de bajo costo y de dimensionalidad pequeña. Su funcionalidad similar a una computadora de escritorio o portátil permite un gran desempeño en diferentes tareas en las que sea programada. Raspberry fue creado en 2012 con el objetivo de brindar una herramienta educacional informática, siendo utilizado por estudiantes, aficionados o profesionales, creando dispositivos que interactúen con el mundo real. Todos los modelos de Raspberry Pi son compatibles entre sí, es decir, cualquier tarea programada en un modelo, puede ser ejecutada en otro modelo de Raspberry Pi (Halfacree, 2019).

# CAPÍTULO III: MARCO METODOLÓGICO

## 3.1. Tipo y nivel de la investigación

### 3.1.1. Tipo de investigación

El tipo de investigación es Aplicada. Este tipo de investigación “se distingue por tener propósitos prácticos inmediatos bien definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad” (Carrasco, 2005, p. 43). La investigación Aplicada “es llamada también constructiva o utilitaria, se caracteriza por su interés en la aplicación de los conocimientos teóricos a determinada situación y las consecuencias prácticas que de ella se deriven” (Sánchez & Reyes, 2006, p. 36).

Del mismo modo, la investigación sigue el tipo de investigación Explicativo. Este tipo de investigación garantiza la ampliación del conocimiento existente sobre temas poco conocidos.

### 3.1.2. Nivel de investigación

El nivel de investigación es Experimental. Este nivel de investigación “se realiza luego de conocer las características del fenómeno o hecho que se investiga (variables) y las causas que han determinado que tenga tales y cuales características, es decir, conociendo los factores que han dado origen al problema, entonces ya se le puede dar un tratamiento metodológico” (Carrasco, 2005, p. 42). Según Caballero (2009), el nivel de investigación Experimental comprende la investigación que se realiza una vez conocido las características del fenómeno (variables) y las causas que han determinado a que la investigación presente tales características.

Del mismo modo, la investigación sigue el nivel de investigación Comprensivo. Este nivel de investigación tiene como objetivo dar referencias a explicaciones de eventos por hechos o situaciones dadas.

## 3.2. Población y/o muestra de estudio

La Tabla 5 indica la población total de la presente investigación, con un total de 15 personas. Así mismo, en la Tabla 6 se especifica la muestra a considerar en base a la población total, donde, siendo la población una cantidad pequeña, se establece la población total como la muestra de investigación.

**Tabla 5**

*Población del área de Tesorería del Gobierno Regional de Tacna*

| Población | Total | Porcentaje |
|---|---|---|
| Área de Tesorería del Gobierno Regional de Tacna | 15 | 100% |

**Tabla 6**

*Población y muestra del área de Tesorería del Gobierno Regional de Tacna*

| Precisión de la estimación<br>Confianza del 95% y margen de error del 5% | |
|---|---|
| N | n |
| 15 | 15 |

### 3.3. Operacionalización de variables

#### 3.3.1. Definición de las variables

- La variable independiente de la presente investigación es “Sistema de Reconocimiento de Iris”. Ésta es la variable manipulada en la investigación, del cual, la operacionalización correspondiente es visualizada en la Tabla 7.

**Tabla 7**

*Variable independiente: Sistema de reconocimiento de iris*

| Variable | Definición Operacional | Dimensión | Indicador |
|---|---|---|---|
| Sistema de Reconocimiento de Iris | Medio para obtener una imagen del iris humano mediante una foto, y luego almacenarlo de forma digital o electrónica (Ravin, 2016). | Fiabilidad | - Disponibilidad del sistema<br>- Recuperabilidad del sistema<br>- Tolerancia a fallas |

(continúa)

Tabla 7 (continuación)

| Variable | Definición Operacional | Dimensión | Indicador |
|---|---|---|---|
| | | Usabilidad | - Comprensibilidad del uso del sistema<br>- Flexibilidad del aprendizaje en el uso del sistema<br>- Operatividad del sistema<br>- Estética del sistema<br>- Accesibilidad al sistema |
| | Mediante el método de Daugman (2004), se puede obtener un único patrón mediante la codificación del iris. | Seguridad | - Confidencialidad de los datos del sistema<br>- Integridad del sistema<br>- Trazabilidad de acciones del sistema<br>- Autenticación de usuarios en el sistema |
| | | Portabilidad | - Facilidad de la instalación del sistema<br>- Adaptabilidad del sistema en otros ambientes<br>- Capacidad del sistema en sufrir cambios |

- La variable dependiente de la presente investigación es “Control de Acceso”. Ésta es la variable medible en la investigación, del cual, la operacionalización correspondiente es visualizada en la Tabla 8.

**Tabla 8**

*Variable dependiente: Control de acceso*

| Variable | Definición Operacional | Dimensión | Indicador |
|---|---|---|---|
| Control de Acceso | Proceso que regula la admisión de los usuarios para acceder a la información o a lugares de la organización (Whitman & Mattord, 2018).<br>Peltier (2013), afirma que el proceso de control de acceso abarca controles a espacios físicos o a información digital. | Identificación | - Nivel de complejidad en la estructuración del identificador<br>- % de frecuencia del uso del identificador<br>- % de aceptabilidad del uso del identificador |
| | | Autenticación | - Tiempo de demora en el proceso de autenticación<br>- % de acierto en la autenticación<br>- % de aceptación falsa |
| | | Autorización | - % de acierto en la otorgación de permisos para el acceso al área requerida<br>- Nivel de confiabilidad en la otorgación de permisos<br>- % de accesos erróneos otorgados |
| | | Trazabilidad | - Bitácora de acciones/eventos en los procesos<br>- Bitácora de intentos de ingreso por personal no autorizado<br>- Bitácora de accesos garantizados al personal |

- La variable interviniente de la presente investigación es “Deep Learning”, del cual, la operacionalización correspondiente es visualizada en la Tabla 9.

**Tabla 9**

*Variable interviniente: Deep Learning*

| Variable | Definición Operacional | Indicador |
|---|---|---|
| Deep Learning | Proceso diseñado que establece un comportamiento similar al cerebro de la persona, para la resolución de problemas definidos incorrectamente (Hurwitz & Kirsch, 2018). | - Nivel de complejidad de la arquitectura de redes neuronales<br>- Tiempo de pre-procesamiento de imágenes en la arquitectura de redes neuronales<br>- Tiempo de post-procesamiento de imágenes en la arquitectura de redes neuronales<br>- Tiempo de predicción de una clase<br>- Porcentaje de precisión de la clase a predecir |

### 3.4. Técnicas e Instrumentos para la Recolección de Datos

Para el presente trabajo de investigación, se utilizó la técnica “Ficha de Evaluación” del instrumento “Prueba de Comprobación”. Esta técnica e instrumento sirvió para medir la variable dependiente “Control de acceso” en el proceso pre – post test de evaluación.

En el Anexo 2 se muestra la plantilla del instrumento utilizado para la recolección de información. Del mismo modo, la validación del instrumento por diversos expertos se muestra en el Anexo 3.

### 3.5. Procesamiento y Análisis de Datos

La acción principal del presente trabajo de investigación es verificar la veracidad de las hipótesis determinadas. La variable a ser medida es la variable dependiente “Control de acceso”, del cual, se utilizaron técnicas de análisis y estadística para medir la variable:

- Se aplicó la respectiva Ficha de Evaluación a la muestra de estudio, considerando dos etapas: evaluación de la variable dependiente según la situación actual (antes), evaluación de la variable dependiente según la aplicación del proyecto de investigación (después).

- Los datos recolectados mediante el instrumento indicado, fueron procesados para la respectiva representación en tablas, cuadros de frecuencias, gráficos de barra o circular, para mostrar los resultados descriptivos de las variables de estudio, mediante el uso de la herramienta IBM SPSS Statistics.
- El análisis de los datos fue esencial para la evaluación de la hipótesis general e hipótesis específicas.

# CAPÍTULO IV: RESULTADOS

Como fue expuesto en el capítulo anterior, la variable a medir es la variable dependiente de la investigación. Hernández & Mendoza (2018), indican que, la variable dependiente, para diseños experimentales, es la variable medible, evaluando el efecto en ésta mediante la causa de la acción e intervención de la variable independiente; y para la elaboración del instrumento recolector de datos, se debe considerar la variable medible u observable de la investigación, es decir, la variable dependiente.

Por la razón ya expuesta anteriormente, a continuación, se demuestran los resultados obtenidos durante la ejecución pre – post test de evaluación, de la variable dependiente medible “Control de Acceso” (la aplicación del respectivo instrumento de recolección de información para la evaluación correspondiente, se muestra en el Anexo 4).

## 4.1. Variable dependiente: Control de acceso

Los enunciados de cada indicador presentes en la dimensión, se califican bajo la escala de Likert, donde los valores definidos son: N: Nunca; MPV: Muy pocas veces; AV: A veces; CS: Casi siempre; S: Siempre; con un puntaje de 1 ~ 5. Del mismo modo, los enunciados se han definido en dos tipos: enunciados directos y enunciados indirectos.

Las tablas y gráficos estadísticos descritos y visualizados en los apartados siguientes, reflejan los indicadores para determinar el nivel de seguridad durante el proceso de control de acceso: proceso de control de acceso actual (evaluación directa con el propio personal), y proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris (evaluación mediante datos recopilados y analizados de la propia solución propuesta, visualizados, a detalle, en el Anexo 11).

### 4.1.1. Identificación

La dimensión “Identificación” asociada a la variable “Control de Acceso”, tiene tres indicadores, cada uno con su propio enunciado.

#### 4.1.1.1. Nivel de Complejidad en la Estructuración del Identificador

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere al nivel de complejidad utilizado durante la composición o estructuración del

identificador, proporcionado al personal para su autenticación durante el proceso de control de acceso.

*Enunciado N° 1: El identificador proporcionado presenta una estructura compleja.*

En la Tabla 10 y Figura 17, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 1 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

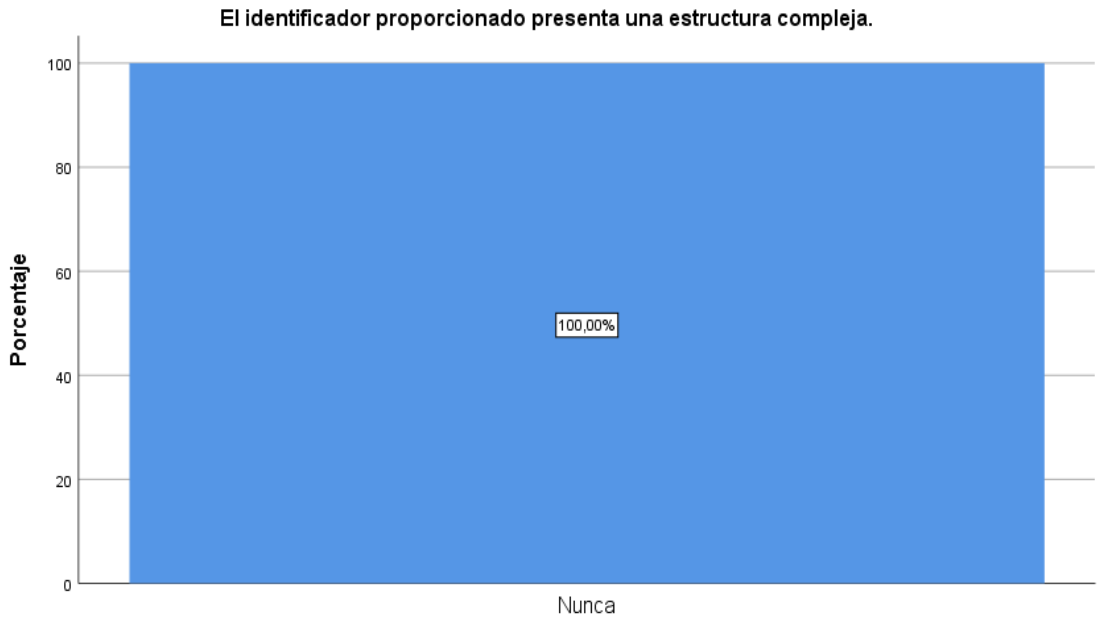
**Tabla 10**

*Resultados del enunciado 1 – proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 17**

*Resultados del enunciado 1 – proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 10 y Figura 17, con respecto a la complejidad usada en la composición o estructuración del identificador, donde se evalúa el identificador

utilizado para la respectiva autenticación durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, se considera que el identificador proporcionado para la respectiva autenticación, nunca presenta una composición o estructuración compleja. Como resultado, según la totalidad del personal evaluado, se señala que el identificador proporcionado y utilizado, llave de cerrojo, para la respectiva autenticación durante el proceso actual de control de acceso, nunca presenta un nivel de complejidad en su composición o estructuración debido a la simpleza de la llave.

En la Tabla 11 y Figura 18, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 1 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

**Tabla 11**

*Resultados del enunciado 1 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 18**

*Resultados del enunciado 1 – Proceso con sistema de reconocimiento de iris*

*Interpretación de resultados:*

Se observa en la Tabla 11 y Figura 18, con respecto a la complejidad usada en la composición o estructuración del identificador, donde se evalúa el identificador utilizado para la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, se considera que el identificador proporcionado para la respectiva autenticación, siempre presenta una composición o estructuración compleja. Como resultado, según la totalidad del personal evaluado, se señala que el identificador proporcionado y utilizado, iris humano, para la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, siempre presenta un nivel de complejidad en su composición y estructuración debido a las características biológicas e irreproducibles del iris.

#### 4.1.1.2. % de Frecuencia del Uso del Identificador

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere al porcentaje de frecuencia de uso del identificador por parte del personal para lograr su autenticación, durante el proceso de control de acceso.

*Enunciado N° 2: El personal utiliza el identificador para autenticarse.*

En la Tabla 12 y Figura 19, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 2 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

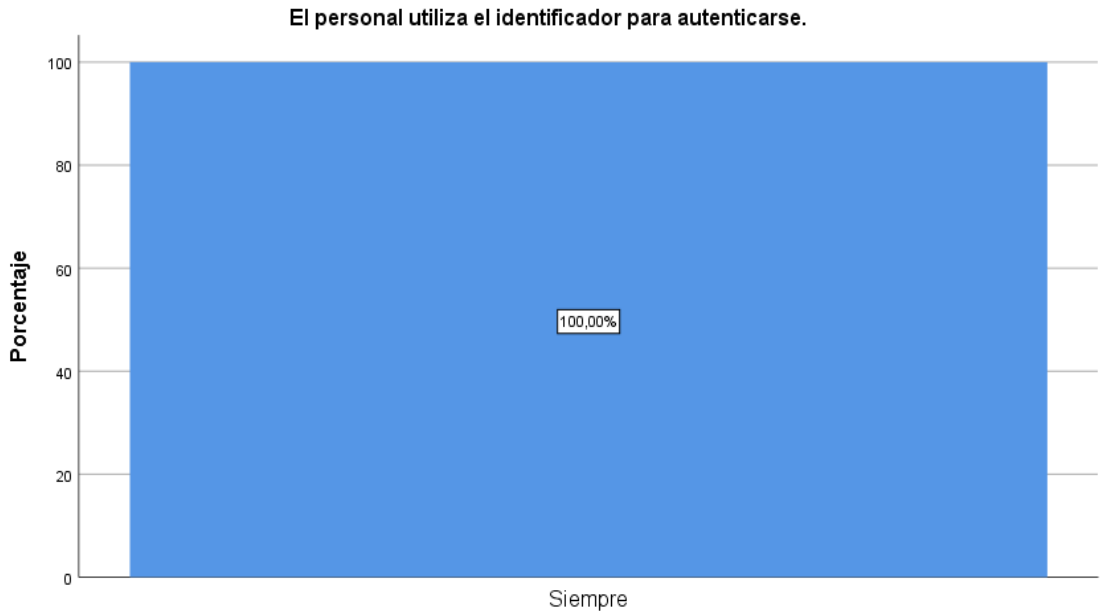
**Tabla 12**

*Resultados del enunciado 2 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 19**

*Resultados del enunciado 2 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 12 y Figura 19, con respecto a la frecuencia de uso del identificador para proceder con la respectiva autenticación durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, siempre se utiliza el identificador para la autenticación. Como resultado, según la totalidad del personal evaluado, siempre se utiliza el identificador, llave de cerrojo, para proceder con la respectiva autenticación durante el proceso actual de control de acceso, siendo este identificador obligatorio y requerido para acceder al lugar físico.

En la Tabla 13 y Figura 20, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 2 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

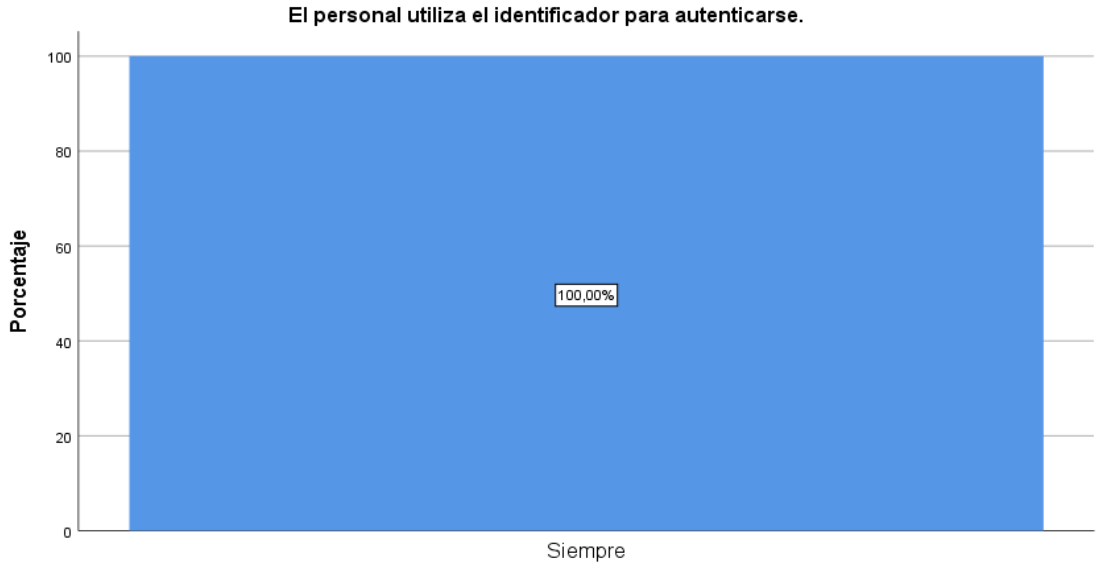
**Tabla 13**

*Resultados del enunciado 2 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 20**

*Resultados del enunciado 2 – Proceso con sistema de reconocimiento de iris*




*Interpretación de resultados:*

Se observa en la Tabla 13 y Figura 20, con respecto a la frecuencia de uso del identificador para proceder con la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre se utiliza el identificador para la autenticación. Como resultado, según la totalidad del personal evaluado, siempre se utiliza el identificador, iris humano, para proceder con la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, siendo este identificador indispensable y requerido.

#### 4.1.1.3. % de Aceptabilidad del Uso del Identificador

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere a la aceptabilidad y comodidad que siente el personal al usar el identificador para su autenticación, durante el proceso de control de acceso.

*Enunciado N° 3: El personal se siente cómodo y conforme al usar el identificador.*

En la Tabla 14 y Figura 21, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 3 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

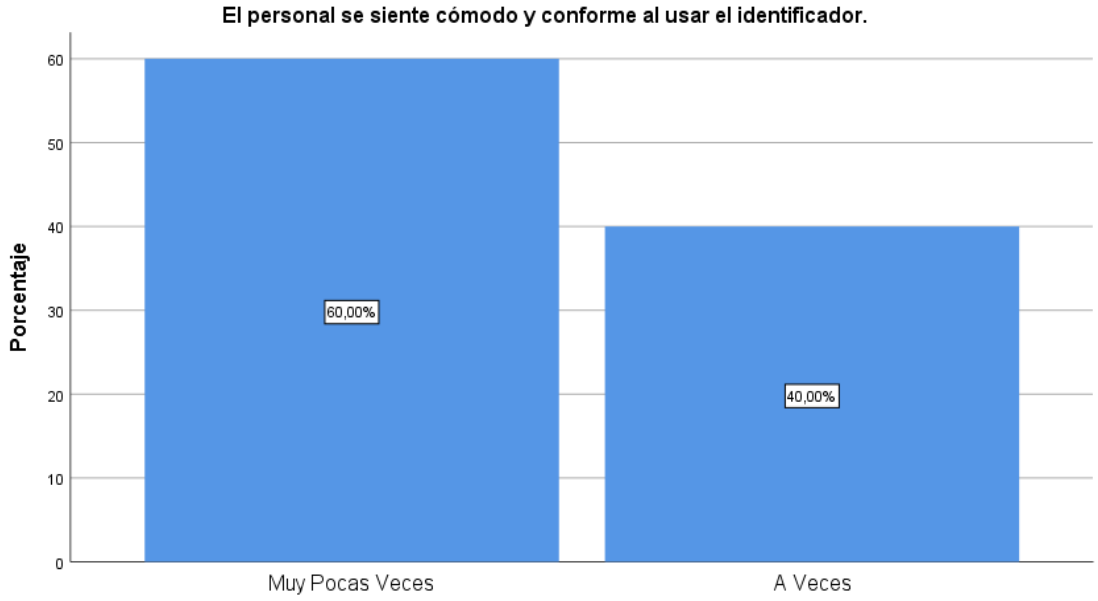
**Tabla 14**

*Resultados del enunciado 3 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Pocas Veces | 9 | 60,0 | 60,0 | 60,0 |
| | A Veces | 6 | 40,0 | 40,0 | 100,0 |
| | Total | 15 | 100,0 | 100,0 | |

**Figura 21**

*Resultados del enunciado 3 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 14 y Figura 21, con respecto a la aceptabilidad y comodidad que siente el personal al usar el identificador para proceder con la respectiva autenticación durante el proceso actual de control de acceso, que, según el 60,00% del total del personal evaluado, muy pocas veces existe comodidad y conformidad al usar el identificador, y según el 40,00% del total del personal evaluado, a veces existe comodidad y conformidad al usar el identificador. Como resultado, según la mayoría del personal evaluado, muy pocas veces existe comodidad y conformidad al usar el identificador, llave de cerrojo, para proceder con la respectiva autenticación durante el proceso actual de control de acceso, debido a la dependencia y recordatorio de portar la llave al lugar de acceso, ya que, sin ese identificador, el personal no será capaz de acceder al lugar físico.

En la Tabla 15 y Figura 22, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 3 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

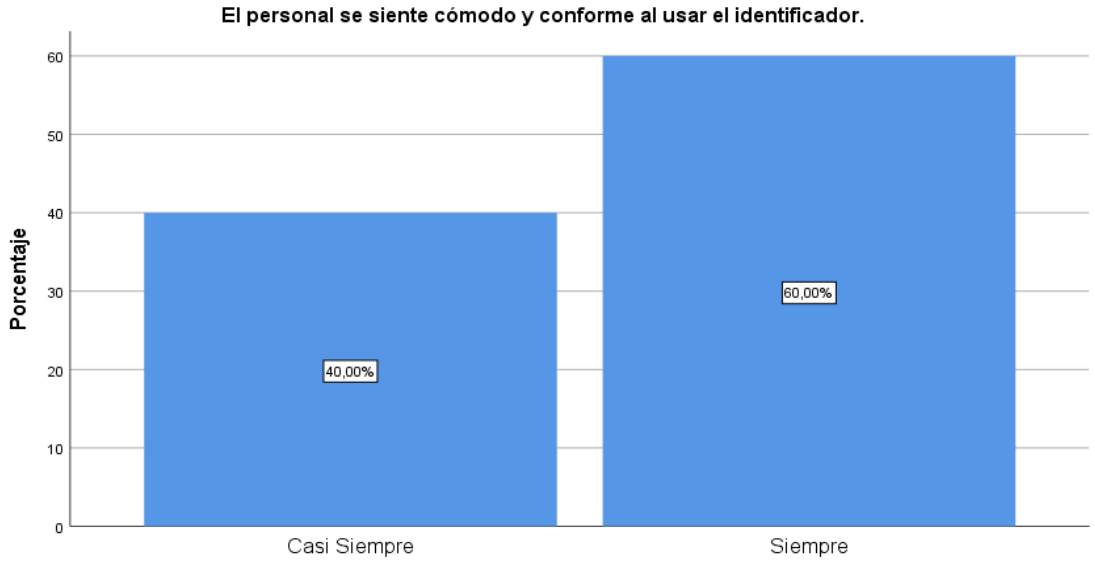
**Tabla 15**

*Resultados del enunciado 3 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Casi Siempre | 6 | 40,0 | 40,0 | 40,0 |
| | Siempre | 9 | 60,0 | 60,0 | 100,0 |
| | Total | 15 | 100,0 | 100,0 | |

**Figura 22**

*Resultados del enunciado 3 – Proceso con sistema de reconocimiento de iris*




*Interpretación de resultados:*

Se observa en la Tabla 15 y Figura 22, con respecto a la aceptabilidad y comodidad que siente el personal al usar el identificador para proceder con la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el 60,00% del total del personal evaluado, siempre existe comodidad y conformidad al usar el identificador, y según el 40,00% del total del personal evaluado, casi siempre existe comodidad y conformidad al usar el identificador. Como resultado, según la mayoría del personal evaluado, siempre siente comodidad y

conformidad al usar el identificador, iris humano, para proceder con la respectiva autenticación durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, debido a la portabilidad y simpleza que manifiesta el uso del iris como llave de paso, dejando de lado el recordar llevar y portar alguna llave física al lugar de acceso.

### 4.1.2. Autenticación

La dimensión “Autenticación” asociada a la variable “Control de Acceso”, tiene tres indicadores, cada uno con su propio enunciado.

#### 4.1.2.1. Tiempo de Demora en el Proceso de Autenticación

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere a la rapidez en el proceso de autenticación del personal mediante el uso del identificador, durante el proceso de control de acceso.

*Enunciado N° 4: El tiempo que ocupa el proceso de autenticación del personal es rápido.*

En la Tabla 16 y Figura 23, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 4 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

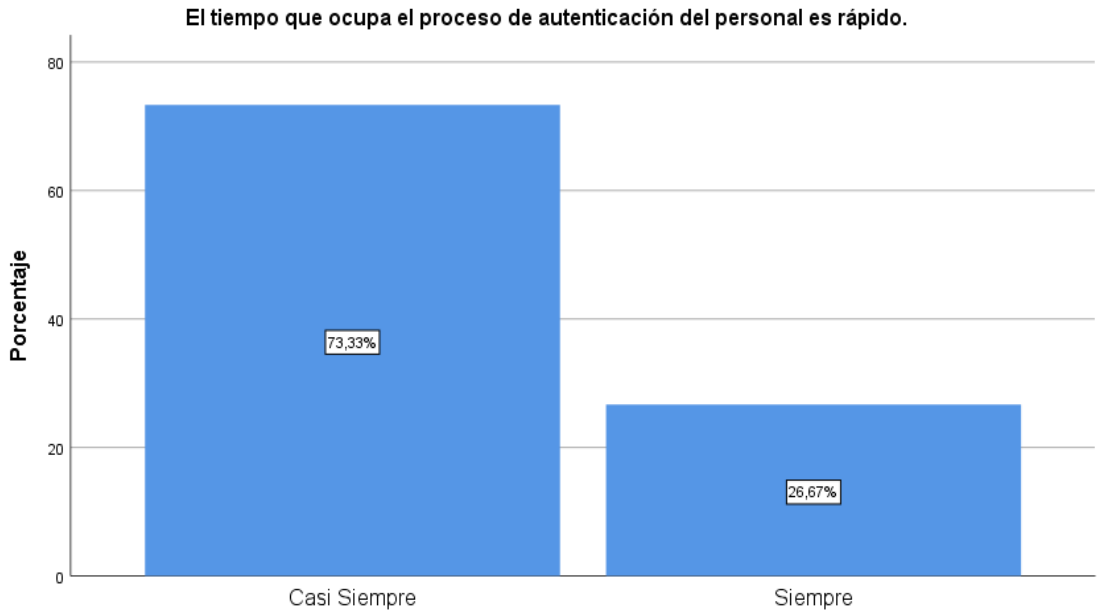
**Tabla 16**

*Resultados del enunciado 4 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Casi Siempre | 11 | 73,3 | 73,3 | 73,3 |
| | Siempre | 4 | 26,7 | 26,7 | 100,0 |
| | Total | 15 | 100,0 | 100,0 | |

**Figura 23**

*Resultados del enunciado 4 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 16 y Figura 23, con respecto al tiempo en el que el proceso de autenticación del personal se ejecuta para la respectiva autorización de permisos durante el proceso actual de control de acceso, que, según el 73,33% del total del personal evaluado, casi siempre es rápido el proceso de autenticación mediante el uso del identificador, y según el 26,67% del total del personal evaluado, siempre es rápido el proceso de autenticación mediante el uso del identificador. Como resultado, según la mayoría del personal evaluado, casi siempre es rápido el proceso de autenticación para la respectiva autorización de permisos durante el proceso actual de control de acceso, debido a que existe una pequeña demora que oscila entre el momento de inserción de la llave, y su respectiva verificación.

En la Tabla 17 y Figura 24, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 4 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

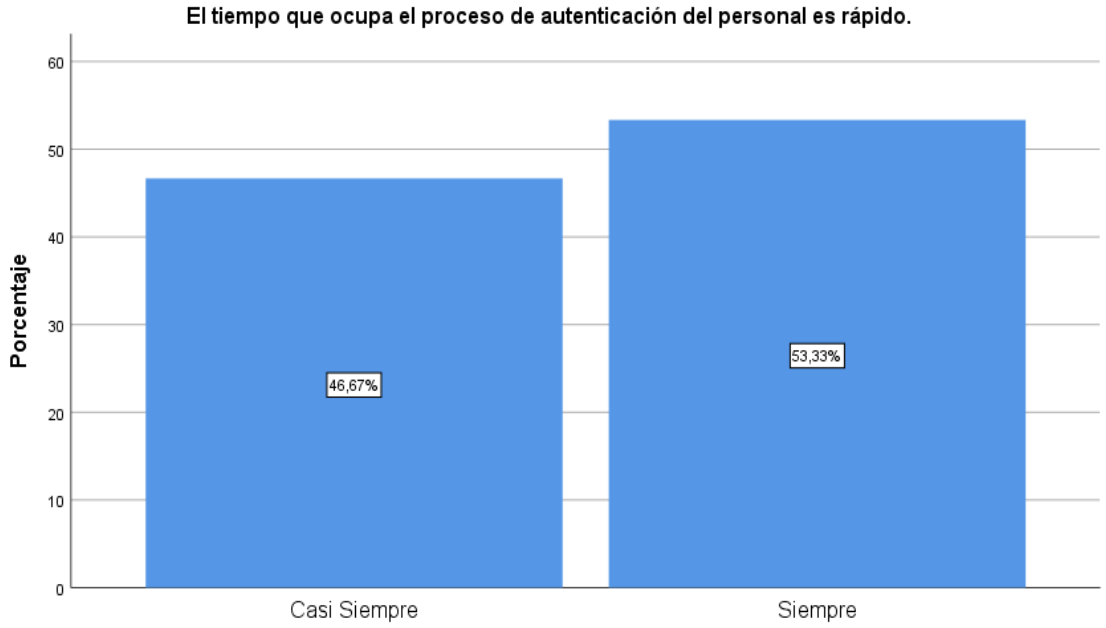
**Tabla 17**

*Resultados del enunciado 4 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Casi Siempre | 7 | 46,7 | 46,7 | 46,7 |
| | Siempre | 8 | 53,3 | 53,3 | 100,0 |
| | Total | 15 | 100,0 | 100,0 | |

**Figura 24**

*Resultados del enunciado 4 – Proceso con sistema de reconocimiento de iris*




*Interpretación de resultados:*

Se observa en la Tabla 17 y Figura 24, con respecto al tiempo en el que el proceso de autenticación del personal se ejecuta para la respectiva autorización de permisos durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el 53,33% del total del personal evaluado, siempre es rápido el proceso de autenticación mediante el uso del identificador, y según el 46,67% del total del personal evaluado, casi siempre es rápido el proceso de autenticación mediante el uso del identificador. Como resultado, según la mayoría del personal evaluado, siempre es rápido el proceso de autenticación para la respectiva autorización de permisos durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, debido a que existe, de igual manera, una pequeña demora en la validación y verificación del iris humano, a raíz de ciertos aspectos técnicos.

#### 4.1.2.2. % de Acierto en la Autenticación

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere al porcentaje de acierto en la autenticación del personal mediante el uso del identificador, durante el proceso de control de acceso.

*Enunciado N° 5: El personal es autenticado correctamente.*

En la Tabla 18 y Figura 25, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 5 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

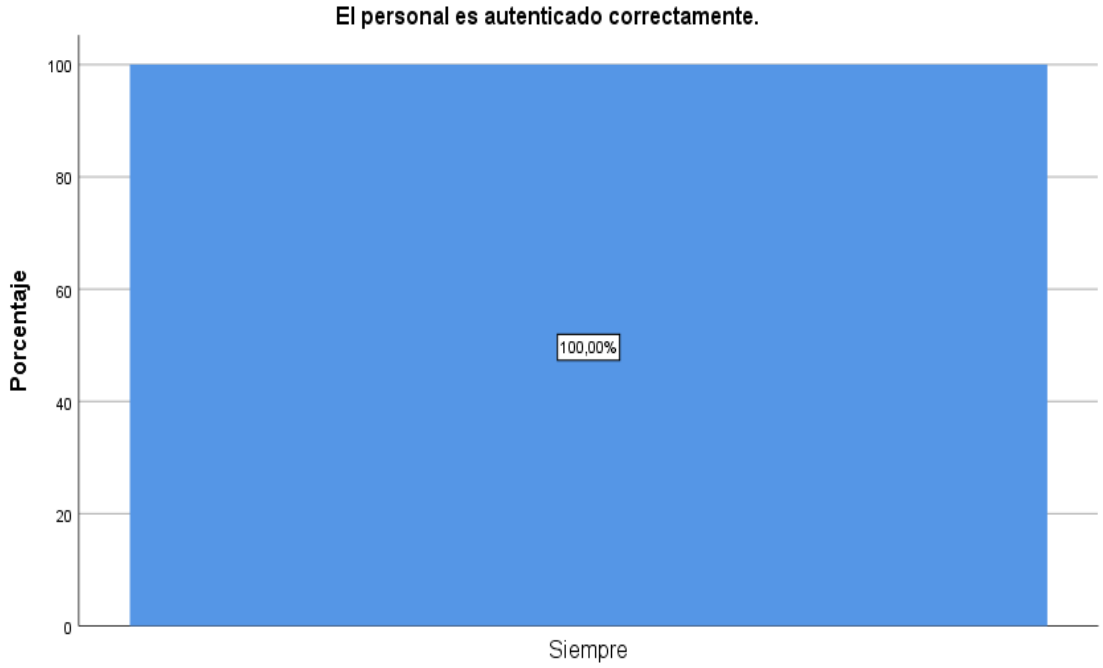
**Tabla 18**

*Resultados del enunciado 5 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 25**

*Resultados del enunciado 5 – Proceso actual*



*Interpretación de resultados:*

Se observa en la Tabla 18 y Figura 25, con respecto a la correcta autenticación del personal durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, siempre existe una correcta autenticación debido a la utilización de un único identificador global de acceso, llave de cerrojo, para todo el personal, que conlleva a una autenticación genérica. Como resultado, según la totalidad del personal evaluado, siempre existe una correcta autenticación del personal durante el proceso actual de control de acceso, permitiendo la autorización del personal, o no, al lugar físico.

En la Tabla 19 y Figura 26, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 5 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

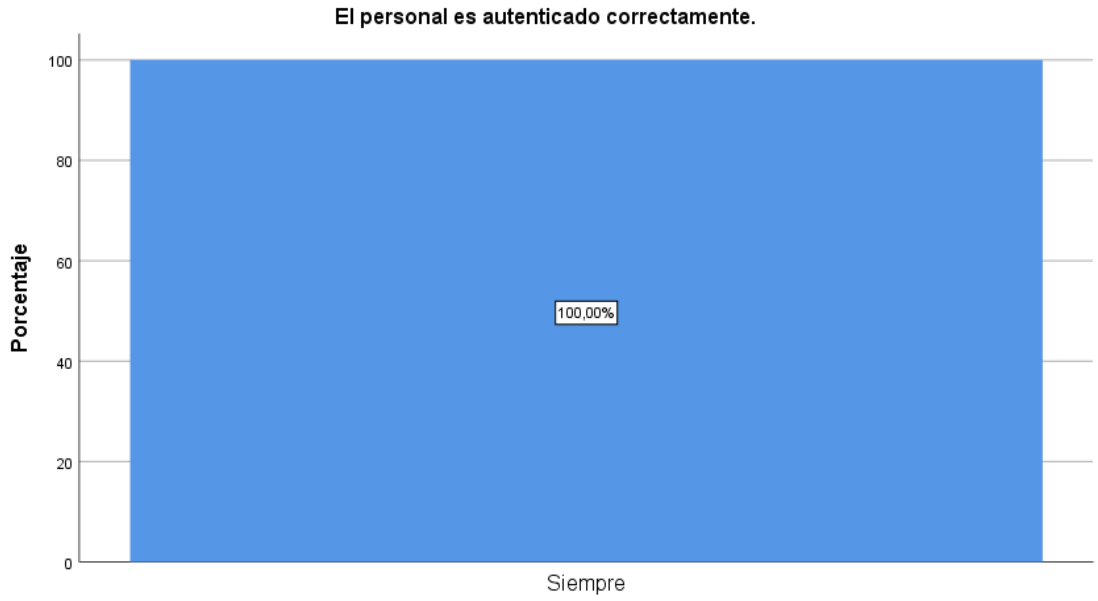
**Tabla 19**

*Resultados del enunciado 5 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 26**

*Resultados del enunciado 5 – Proceso con sistema de reconocimiento de iris*



*Interpretación de resultados:*

Se observa en la Tabla 19 y Figura 26, con respecto a la correcta autenticación del personal durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre existe una correcta autenticación debido a la utilización de un único identificador de acceso, iris humano, por cada personal, que conlleva a una autenticación individual. Como resultado, según la totalidad del personal evaluado, siempre es correcta la autenticación del personal durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, permitiendo la autorización del personal, o no, al lugar físico.

#### 4.1.2.3. % de Aceptación Falsa

Este indicador tiene asociado un enunciado indirecto en la Ficha de Evaluación, que refiere al porcentaje de autenticaciones correctas hechas al personal equivocado mediante el uso del identificador, durante el proceso de control de acceso.

*Enunciado N° 6: Existen falsos positivos en la autenticación del personal.*

En la Tabla 20 y Figura 27, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 6 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

**Tabla 20**

*Resultados del enunciado 6 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 27**

*Resultados del enunciado 6 – Proceso actual*


*Interpretación de resultados:*

Se observa en la Tabla 20 y Figura 27, con respecto a la existencia de falsos positivos en la autenticación del personal durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, siempre existen falsos positivos en la autenticación debido a la utilización de un único identificador de acceso, llave de cerrojo, para todo el personal, que conlleva a una autenticación genérica, suplantando la identidad de otras personas. Como resultado, según la totalidad del personal evaluado, siempre existen falsos positivos en la autenticación del personal durante el proceso actual de control de acceso al no haber una autenticación individual por persona.

En la Tabla 21 y Figura 28, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 6 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

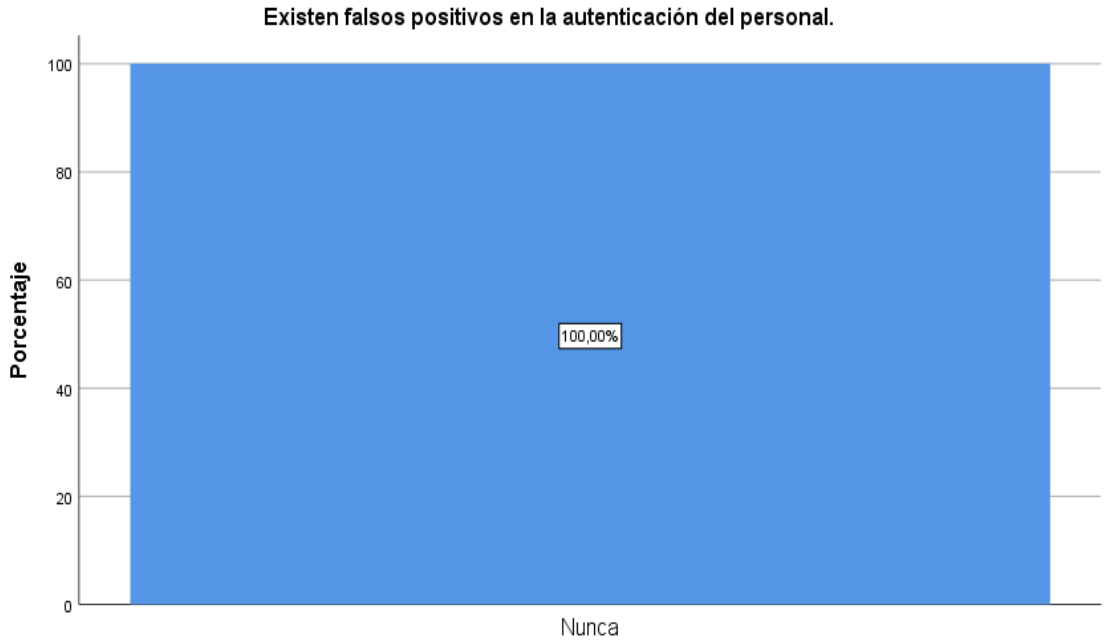
**Tabla 21**

*Resultados del enunciado 6 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 28**

*Resultados del enunciado 6 – Proceso con sistema de reconocimiento de iris*




*Interpretación de resultados:*

Se observa en la Tabla 21 y Figura 28, con respecto a la existencia de falsos positivos en la autenticación del personal durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, nunca existen falsos positivos en la autenticación debido a la utilización de un único identificador de acceso, iris humano, por cada personal, que conlleva a una autenticación individual. Como resultado, según la totalidad del personal evaluado, nunca existen falsos positivos en la autenticación del personal durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, no creando falsos positivos de autenticación.

### 4.1.3. Autorización

La dimensión “Autorización” asociada a la variable “Control de Acceso”, tiene tres indicadores, cada uno con su propio enunciado.

#### 4.1.3.1. % de Acierto en la Otorgación de Permisos para el Acceso al Área Requerida

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere al porcentaje de acierto en la otorgación correcta de los permisos del personal

mediante la autenticación dada por el identificador, durante el proceso de control de acceso.

*Enunciado N° 7: Los permisos del personal son otorgados correctamente.*

En la Tabla 22 y Figura 29, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 7 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

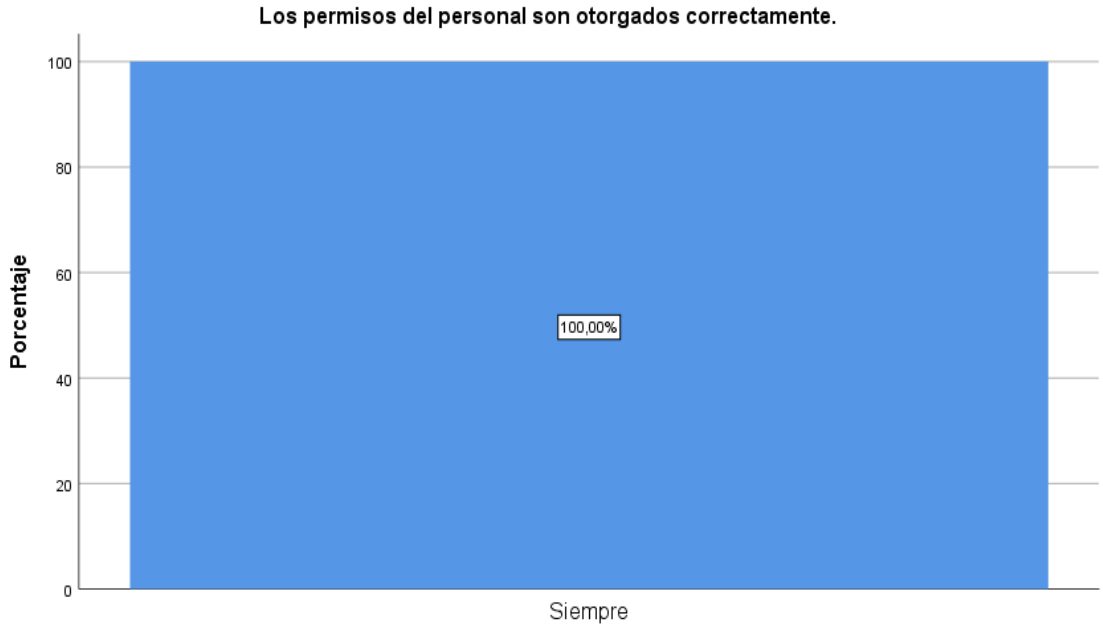
**Tabla 22**

*Resultados del enunciado 7 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 29**

*Resultados del enunciado 7 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 22 y Figura 29, con respecto a la otorgación correcta de permisos del personal dado por la autenticación del identificador durante el proceso

actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, siempre existe la otorgación correcta de permisos dado al personal debido a la utilización de un único identificador de acceso con autenticación genérica para todo el personal. Como resultado, según la totalidad del personal evaluado, siempre existe la otorgación correcta de permisos dado al personal durante la autorización en el proceso actual de control de acceso, permitiendo el acceso al lugar físico, pero sin conocer realmente la persona que ingresa al entorno debido a la autenticación genérica.

En la Tabla 23 y Figura 30, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 7 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

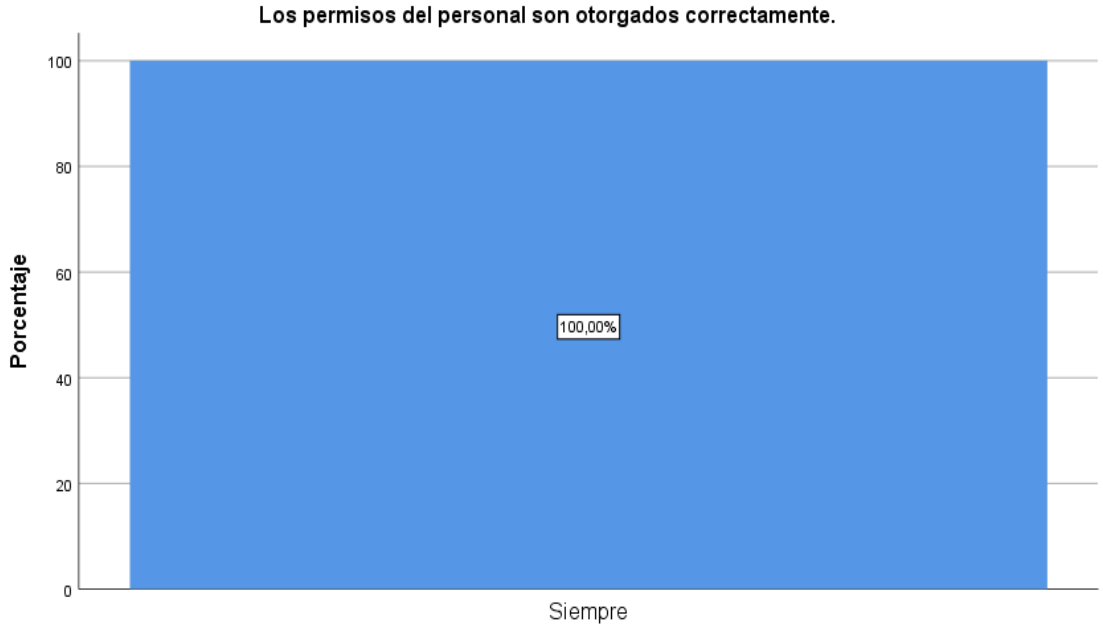
**Tabla 23**

*Resultados del enunciado 7 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 30**

*Resultados del enunciado 7 – Proceso con sistema de reconocimiento de iris*



*Interpretación de resultados:*

Se observa en la Tabla 23 y Figura 30, con respecto a la otorgación correcta de permisos del personal dado por la autenticación del identificador durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre existe la otorgación correcta de permisos dado al personal debido a la utilización de un único identificador de acceso con autenticación individual por cada persona. Como resultado, según la totalidad del personal evaluado, siempre existe la otorgación correcta de permisos dado al personal durante la autorización en el proceso de control de acceso mediante el sistema de reconocimiento de iris, permitiendo el acceso al lugar físico, conociendo realmente la persona que ingresa al entorno debido a la autenticación individual.

#### 4.1.3.2. Nivel de Confiabilidad en la Otorgación de Permisos

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere al nivel de confianza en la otorgación correcta de los permisos del personal mediante la autenticación dada por el identificador, durante el proceso de control de acceso.

*Enunciado N° 8: El personal confía en la otorgación correcta de los permisos.*

En la Tabla 24 y Figura 31, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 8 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

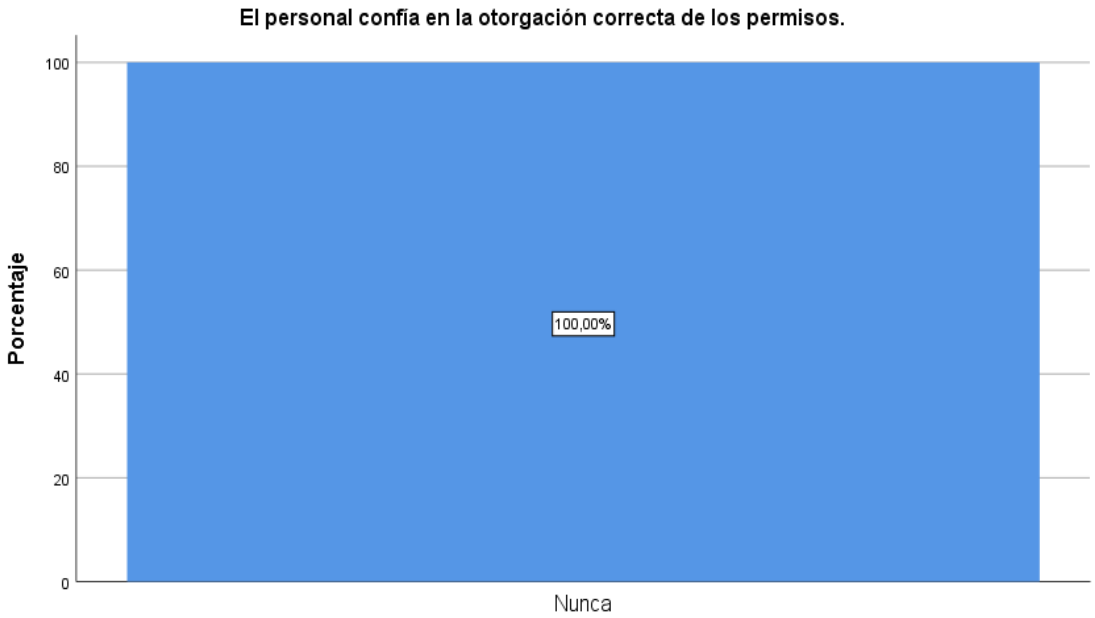
**Tabla 24**

*Resultados del enunciado 8 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 31**

*Resultados del enunciado 8 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 24 y Figura 31, con respecto a la confianza y seguridad que tiene el personal en la otorgación correcta de permisos dado por la autenticación del identificador durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, nunca existe confianza y seguridad en la otorgación correcta de permisos dado al personal, debido a la utilización de un único identificador de autenticación genérica para todo el personal, el cual no diferencia la identidad de cada persona. Como resultado, según la totalidad del personal evaluado, nunca existe confianza y seguridad en la otorgación correcta de permisos dado al personal durante la autorización en el proceso actual de control de acceso, ya que no se puede verificar qué personas, específicamente, son los que realmente ingresan al lugar físico, y si aún tienen accesos de ingresar o no.

En la Tabla 25 y Figura 32, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 8 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

**Tabla 25**

*Resultados del enunciado 8 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 32**

*Resultados del enunciado 8 – Proceso con sistema de reconocimiento de iris*


*Interpretación de resultados:*

Se observa en la Tabla 25 y Figura 32, con respecto a la confianza y seguridad que tiene el personal en la otorgación correcta de permisos dado por la autenticación individual del identificador durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre existe confianza y seguridad en la otorgación correcta de permisos dado al personal debido a la utilización de un único identificador de autenticación individual por cada trabajador, el cual diferencia la identidad de cada persona. Como resultado, según la totalidad del personal evaluado, siempre existe confianza y seguridad en la otorgación correcta de permisos dado al personal durante la autorización en el proceso de control de acceso mediante el sistema de reconocimiento de iris, ya que se logra que cada persona tenga sus propios permisos individuales.

#### 4.1.3.3. % de Accesos Erróneos Otorgados

Este indicador tiene asociado un enunciado indirecto en la Ficha de Evaluación, que refiere al porcentaje de permisos de accesos erróneos otorgados al personal debido a falsos positivos mediante la autenticación dada por el identificador, durante el proceso de control de acceso.

*Enunciado N° 9: Existen accesos erróneos otorgados al personal.*

En la Tabla 26 y Figura 33, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 9 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

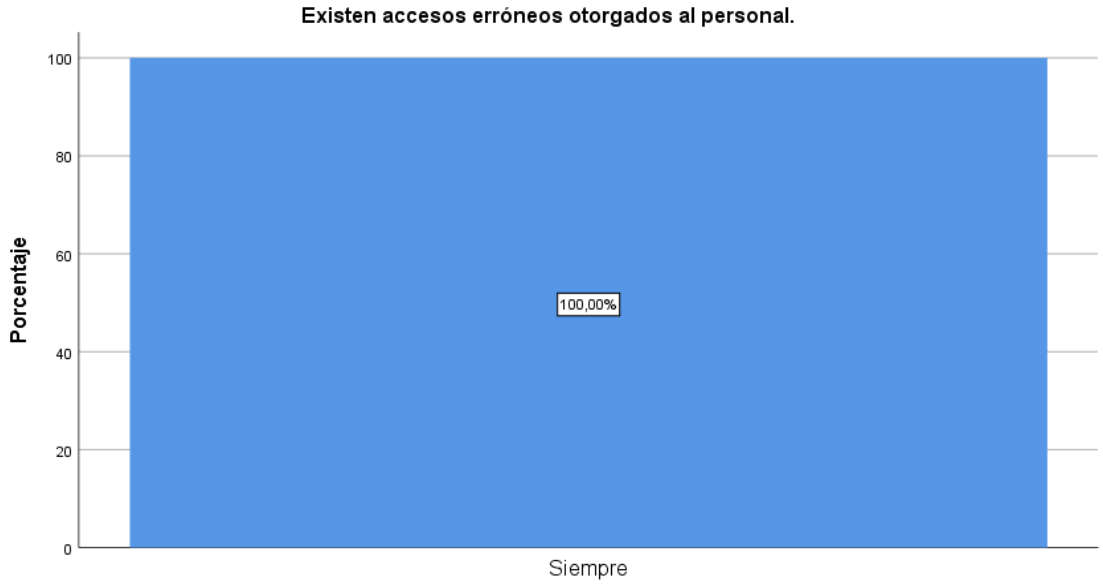
**Tabla 26**

*Resultados del enunciado 9 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 33**

*Resultados del enunciado 9 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 26 y Figura 33, con respecto a la existencia de accesos erróneos otorgados al personal debido a falsos positivos dado por la autenticación del identificador durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, siempre existen accesos erróneos otorgados al personal debido a falsos positivos por la utilización de un único identificador de autenticación genérica para todo el personal, el cual no diferencia la identidad de cada persona. Como resultado, según la totalidad del personal evaluado, siempre existen accesos erróneos otorgados al personal debido a falsos positivos durante la autorización en el proceso actual de control de acceso, ya que, al no existir un identificador individual, una persona está tomando los accesos de otra persona, sin darse cuenta.

En la Tabla 27 y Figura 34, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 9 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

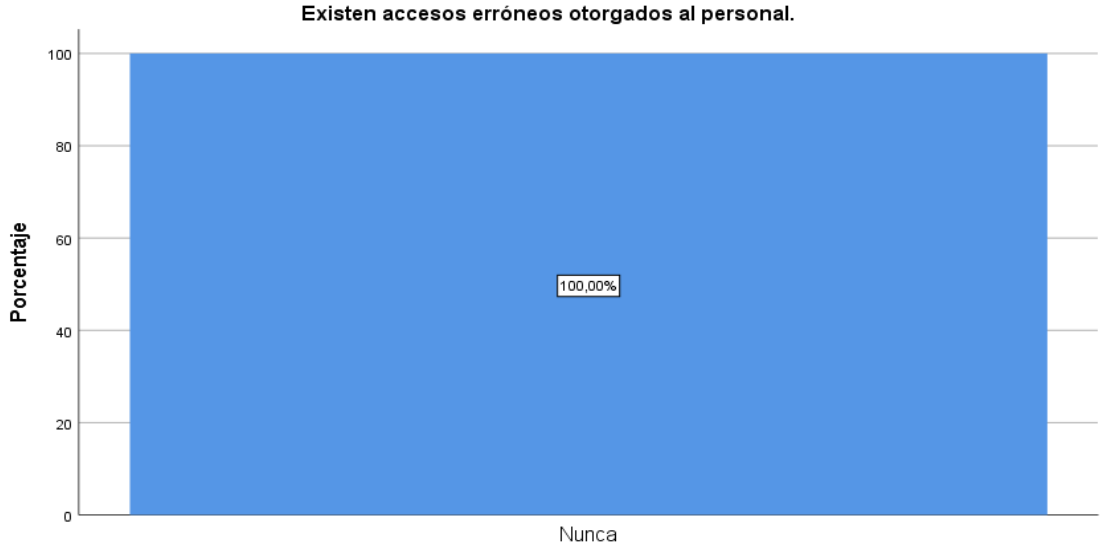
**Tabla 27**

*Resultados del enunciado 9 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 34**

*Resultados del enunciado 9 – Proceso con sistema de reconocimiento de iris*



*Interpretación de resultados:*

Se observa en la Tabla 27 y Figura 34, con respecto a la existencia de accesos erróneos otorgados al personal debido a falsos positivos dado por la autenticación individual del identificador durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, nunca existen accesos erróneos otorgados al personal debido a falsos positivos por la utilización de un único identificador de autenticación individual por cada trabajador, el cual diferencia la identidad de cada persona. Como resultado, según la totalidad del personal evaluado, nunca existen accesos erróneos otorgados al personal debido a falsos positivos durante la autorización en el proceso de control de acceso mediante el sistema de reconocimiento de iris, ya que, al existir un identificador individual, a cada persona se le otorga sus accesos correspondientes e individuales.

### 4.1.4. Trazabilidad

La dimensión “Trazabilidad” asociada a la variable “Control de Acceso”, tiene tres indicadores, cada uno con su propio enunciado.

#### 4.1.4.1. Bitácora de acciones / eventos en los procesos

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería, sistema de reconocimiento de iris o equipo lector biométrico) para anotar o registrar cualquier acción o evento ocurrido durante el proceso de control de acceso (accesos removidos, asignación de accesos al espacio físico, inhabilitación de personal en ingresar al espacio físico, llave no pertenece, cambio de llave, entre otros).

*Enunciado N° 10: Los registros de acciones / eventos durante el proceso de control de acceso, son registrados.*

En la Tabla 28 y Figura 35, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 10 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

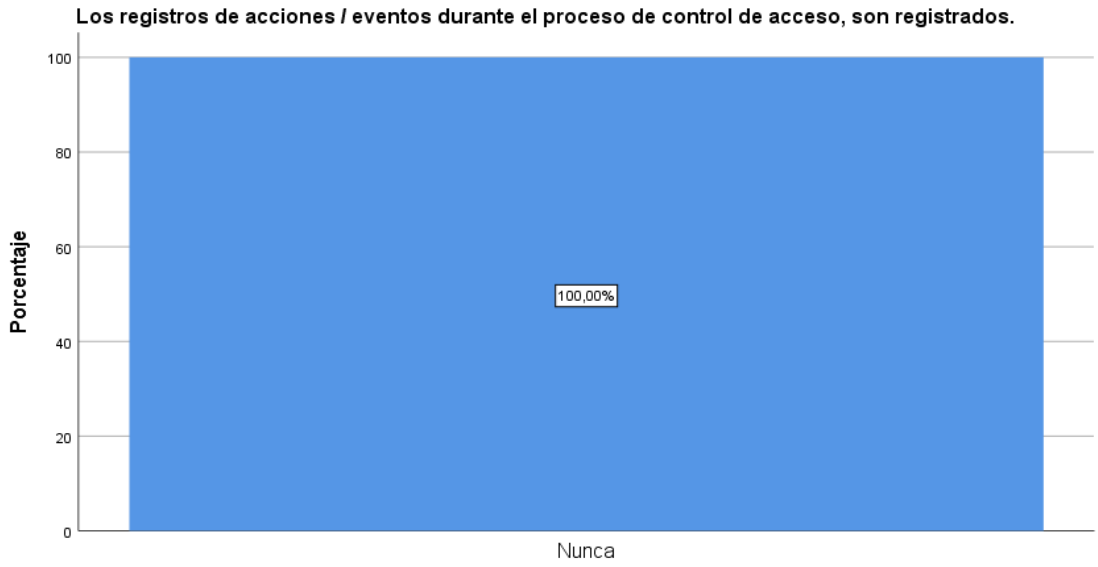
**Tabla 28**

*Resultados del enunciado 10 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 35**

*Resultados del enunciado 10 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 28 y Figura 35, con respecto a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería) para anotar o registrar cualquier acción o evento ocurrido durante el proceso actual de control de acceso, que, según el resultado del 100,00% del personal evaluado, nunca se anota o registra cualquier acción o evento ocurrido durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, nunca se anota o registra cualquier acción o evento ocurrido durante el proceso actual de control de acceso, ya que no existe algún proceso que rija tales acciones que se deberían realizar como parte de un proceso de control de acceso.

En la Tabla 29 y Figura 36, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 10 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

**Tabla 29**

*Resultados del enunciado 10 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 36**

*Resultados del enunciado 10 – Proceso con sistema de reconocimiento de iris*


*Interpretación de resultados:*

Se observa en la Tabla 29 y Figura 36, con respecto a la eventualidad que tiene el controlador de accesos (sistema de reconocimiento de iris o equipo lector biométrico) para anotar o registrar cualquier acción o evento ocurrido durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre se anota o registra cualquier acción o evento ocurrido durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, siempre se anota o registra cualquier acción o evento ocurrido durante el proceso de control de acceso mediante el sistema de reconocimiento de iris.

### 4.1.4.2. Bitácora de intentos de ingreso por personal no autorizado

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería, sistema de reconocimiento de iris o equipo lector

biométrico) para anotar o registrar los accesos no autorizados durante el proceso de control de acceso.

*Enunciado N° 11: Los registros de intentos de ingreso por personal no autorizado son registrados.*

En la Tabla 30 y Figura 37, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 11 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

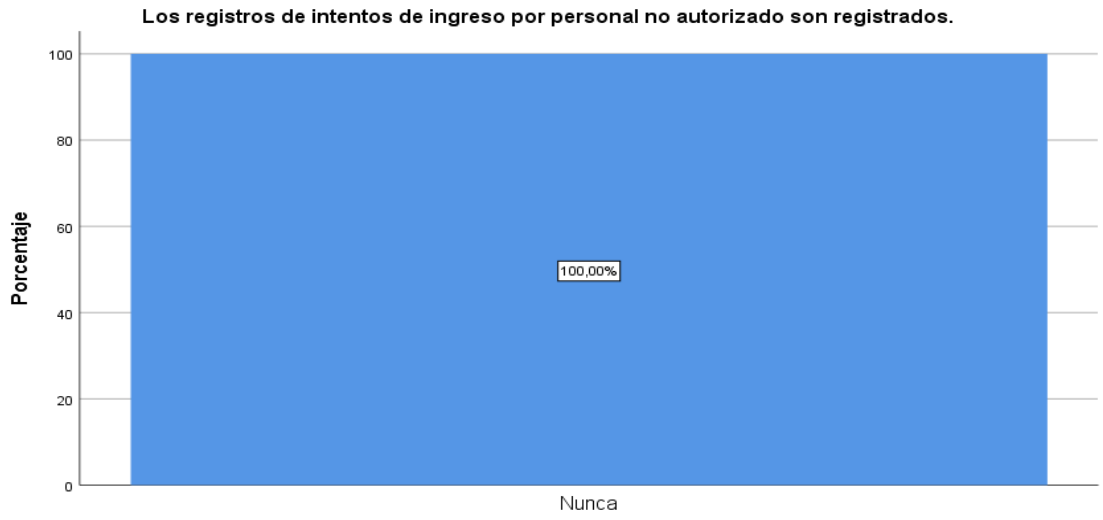
**Tabla 30**

*Resultados del enunciado 11 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 37**

*Resultados del enunciado 11 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 30 y Figura 37, con respecto a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería) para anotar o registrar los accesos no autorizados durante el proceso actual de control de

acceso, que, según el resultado del 100,00% del personal evaluado, nunca se anota o registra los accesos no autorizados durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, nunca se anota o registra los accesos no autorizados durante el proceso actual de control de acceso (esto es a causa de lo comentado en el Enunciado 10 – proceso actual).

En la Tabla 31 y Figura 38, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 11 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

**Tabla 31**

*Resultados del enunciado 11 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 38**

*Resultados del enunciado 11 – Proceso con sistema de reconocimiento de iris*


*Interpretación de resultados:*

Se observa en la Tabla 31 y Figura 38, con respecto a la eventualidad que tiene el controlador de accesos (sistema de reconocimiento de iris o equipo lector biométrico)

para anotar o registrar los accesos no autorizados durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre se anota o registra los accesos no autorizados durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, siempre se anota o registra los accesos no autorizados durante el proceso de control de acceso mediante el sistema de reconocimiento de iris.

#### 4.1.4.3. Bitácora de accesos garantizados al personal

Este indicador tiene asociado un enunciado directo en la Ficha de Evaluación, que refiere a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería, sistema de reconocimiento de iris o equipo lector biométrico) para anotar o registrar los accesos autorizados durante el proceso de control de acceso.

*Enunciado N° 12: Los registros de accesos garantizados al personal son registrados.*

En la Tabla 32 y Figura 39, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 12 del instrumento aplicado según el proceso de control de acceso actual, sin el uso del Sistema de Reconocimiento de Iris para el control de acceso.

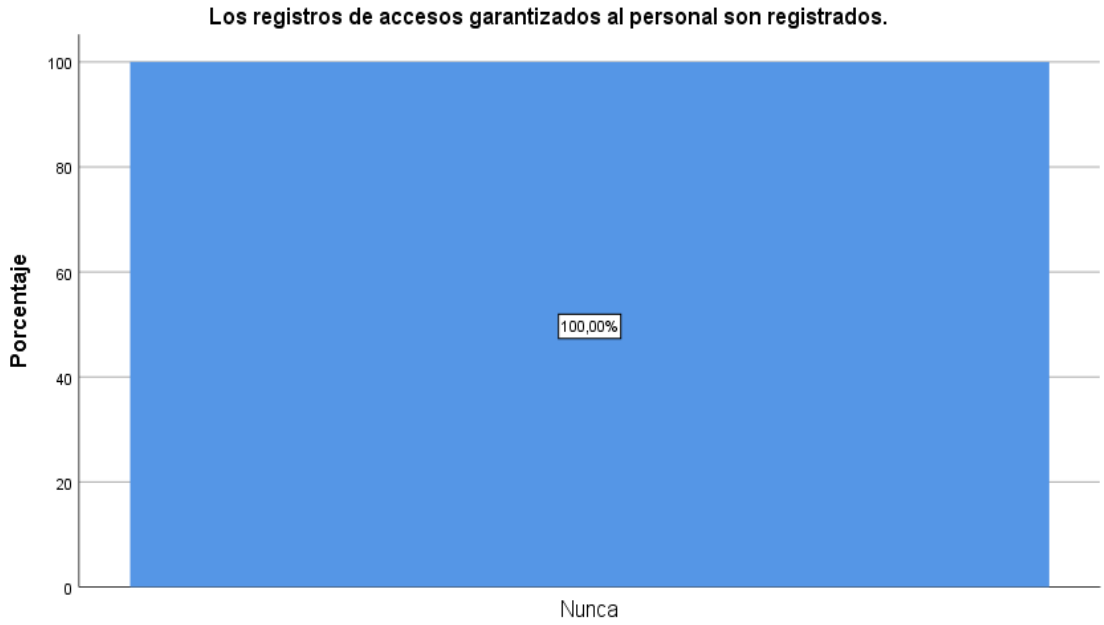
**Tabla 32**

*Resultados del enunciado 12 – Proceso actual*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Nunca | 15 | 100,0 | 100,0 | 100,0 |

**Figura 39**

*Resultados del enunciado 12 – Proceso actual*




*Interpretación de resultados:*

Se observa en la Tabla 32 y Figura 39, con respecto a la eventualidad que tiene el controlador de accesos (personal de seguridad, jefe o encargado de Tesorería) para anotar o registrar los accesos autorizados durante el proceso actual de acceso, que, según el resultado del 100,00% del personal evaluado, nunca se anota o registra los accesos autorizados durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, nunca se anota o registra los accesos autorizados durante el proceso actual de control de acceso (esto es a causa de lo comentado en el Enunciado 10 – proceso actual).

En la Tabla 33 y Figura 40, se pueden visualizar los datos estadísticos recopilados en base al resultado del Enunciado 12 del instrumento aplicado según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris propuesto.

**Tabla 33**

*Resultados del enunciado 12 – Proceso con sistema de reconocimiento de iris*

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Siempre | 15 | 100,0 | 100,0 | 100,0 |

**Figura 40**

*Resultados del enunciado 12 – Proceso con sistema de reconocimiento de iris*


*Interpretación de resultados:*

Se observa en la Tabla 33 y Figura 40, con respecto a la eventualidad que tiene el controlador de accesos (sistema de reconocimiento de iris o equipo lector biométrico) para anotar o registrar los accesos autorizados durante el proceso de control de acceso mediante el sistema de reconocimiento de iris, que, según el resultado del 100,00% del personal evaluado, siempre se anota o registra los accesos autorizados durante el proceso de control de acceso. Como resultado, según la totalidad del personal evaluado, siempre se anota o registra los accesos autorizados durante el proceso de control de acceso mediante el sistema de reconocimiento de iris.

## 4.2. Nivel de seguridad actual y nivel de seguridad con Sistema de Reconocimiento de Iris (SRICA)

La aplicación del instrumento Ficha de Evaluación para determinar el nivel de seguridad que existe en el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, resalta una gran diferencia en niveles de seguridad. El proceso o método actual presenta grandes brechas de seguridad física, el cual se ve reflejado en los bajos puntajes obtenidos mediante el instrumento de recolección de datos, donde se presentaron indicadores necesarios para la evaluación respectiva del nivel de seguridad.

La Tabla 34 muestra el resumen de los resultados recopilados según el proceso actual de control de acceso, del cual, se logra notar la deficiencia en niveles de seguridad en los valores calculados por la evaluación.

**Tabla 34**

*Resumen de resultados – Proceso actual*

| N° Personal | E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | E9 | E10 | E11 | E12 | Puntaje |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 2 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 3 | Nunca | Siempre | A Veces | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 30 |
| 4 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 5 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 6 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 7 | Nunca | Siempre | A Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 8 | Nunca | Siempre | Muy Pocas Veces | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 9 | Nunca | Siempre | Muy Pocas Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 28 |
| 10 | Nunca | Siempre | A Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 11 | Nunca | Siempre | Muy Pocas Veces | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 12 | Nunca | Siempre | Muy Pocas Veces | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 13 | Nunca | Siempre | A Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 14 | Nunca | Siempre | A Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| 15 | Nunca | Siempre | A Veces | Casi Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Nunca | Nunca | Nunca | 29 |
| Puntaje | 15 | 75 | 36 | 64 | 75 | 15 | 75 | 15 | 15 | 15 | 15 | 15 | |

Por otro lado, en la Tabla 35 se muestra el resumen de los resultados recopilados según el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, alcanzando altos puntajes, reduciendo la brecha de seguridad física, y cumpliendo con los indicadores necesarios para la evaluación en niveles de seguridad para el control de acceso.

**Tabla 35**

*Resumen de resultados – Proceso con sistema de reconocimiento de iris*

| N° Personal | E1 | E2 | E3 | E4 | E5 | E6 | E7 | E8 | E9 | E10 | E11 | E12 | Puntaje |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Siempre | Siempre | Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 59 |
| 2 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 3 | Siempre | Siempre | Casi Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 59 |
| 4 | Siempre | Siempre | Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 59 |
| 5 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 6 | Siempre | Siempre | Casi Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 58 |
| 7 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 8 | Siempre | Siempre | Casi Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 58 |
| 9 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 10 | Siempre | Siempre | Casi Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 58 |
| 11 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 12 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 13 | Siempre | Siempre | Casi Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 58 |
| 14 | Siempre | Siempre | Siempre | Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 60 |
| 15 | Siempre | Siempre | Casi Siempre | Casi Siempre | Siempre | Nunca | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | 58 |
| Puntaje | 75 | 75 | 69 | 68 | 75 | 75 | 75 | 75 | 75 | 75 | 75 | 75 | |

### 4.3. Contraste de hipótesis

Según los resultados obtenidos mediante el instrumento Ficha de Evaluación, donde se presentaron enunciados referentes a los indicadores que evalúan el nivel de seguridad para el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, la Tabla 36 muestra los puntajes totales obtenidos mediante la respectiva evaluación, tanto del proceso actual de control de acceso, y el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, indicando los puntajes esperados por dimensión y proceso, los puntajes obtenidos, y el porcentaje en niveles de seguridad alcanzado.

**Tabla 36**

*Puntaje total del control de acceso según indicadores*

| Control de Acceso | Dimensión | Puntaje Esperado | Puntaje Obtenido | Porcentaje (Nivel %) |
|---|---|---|---|---|
| Proceso actual tradicional de control de acceso | Identificación | 225 | 126 | 56,00 |
| | Autenticación | 225 | 154 | 68,44 |
| | Autorización | 225 | 105 | 46,67 |
| | Trazabilidad | 225 | 45 | 20,00 |
| | Total | 900 | 430 | 47,78 |
| Proceso de control de acceso mediante sistema de reconocimiento de iris | Identificación | 225 | 219 | 97,33 |
| | Autenticación | 225 | 218 | 96,89 |
| | Autorización | 225 | 225 | 100,00 |
| | Trazabilidad | 225 | 225 | 100,00 |
| | Total | 900 | 887 | 98,56 |

Para la contrastación de hipótesis general y específicos, se realizó la prueba estadística T de muestras relacionadas entre los resultados pre – post test de evaluación de la variable dependiente medible “Control de Acceso”.

- Nivel de significancia de 5%, es decir, 0,05.

#### 4.3.1. Hipótesis general

- Siendo la hipótesis general nula, el Sistema de Reconocimiento de Iris basado en Deep Learning no mejora significativamente el nivel de seguridad

para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

- Siendo la hipótesis general alterna, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora significativamente el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

La Tabla 37 muestra los grupos estadísticos que representan a las muestras del proceso actual de control de acceso, y proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, indicando datos estadísticos en contraste a la hipótesis general.

**Tabla 37**

*Grupo estadístico en contraste a la hipótesis general*

| | | Media | N | Desv. Desviación | Desv. Error promedio |
|---|---|---|---|---|---|
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso | 28,67 | 15 | ,617 | ,159 |
| | Proceso de control de acceso mediante sistema de reconocimiento de iris | 59,13 | 15 | ,915 | ,236 |

Así mismo, en la Tabla 38 se visualiza la ejecución de la prueba T de muestras relacionadas, entre la muestra del proceso actual de control de acceso, y muestra del proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, generando datos estadísticos para el respectivo contraste de hipótesis de la hipótesis general.

**Tabla 38**

*Prueba de muestras relacionadas en contraste a la hipótesis general*

| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | t | gl | Sig. (bilateral) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inferior | Superior | | | |
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso - Proceso de control de acceso mediante sistema de reconocimiento de iris | -30,467 | 1,187 | ,307 | -31,124 | -29,809 | -99,388 | 14 | ,000 |

Según la prueba de muestras relacionadas calculada, observamos que el p-valor es de 0,000. Como el valor de significancia establecida es de 0,05, podemos indicar que 0,000 < 0,05, rechazando la hipótesis general nula, y aceptando la hipótesis general alterna.

Por ende, se puede indicar que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora significativamente el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

### 4.3.2. Hipótesis específicas

#### 4.3.2.1. Identificación

- Siendo la hipótesis específica nula, el Sistema de Reconocimiento de Iris basado en Deep Learning no mejora el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
- Siendo la hipótesis específica alterna, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

La Tabla 39 muestra los grupos estadísticos que representan a las muestras del proceso actual de control de acceso, y proceso de control de acceso con el uso del

Sistema de Reconocimiento de Iris, indicando datos estadísticos en contraste a la hipótesis específica.

**Tabla 39**

*Grupo estadístico en contraste a la hipótesis específica N° 1*

| | | Media | N | Desv. Desviación | Desv. Error promedio |
|---|---|---|---|---|---|
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso | 8,40 | 15 | ,507 | ,131 |
| | Proceso de control de acceso mediante sistema de reconocimiento de iris | 14,60 | 15 | ,507 | ,131 |

Así mismo, en la Tabla 40 se visualiza la ejecución de la prueba T de muestras relacionadas, entre la muestra del proceso actual de control de acceso, y muestra del proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, generando datos estadísticos para el respectivo contraste de hipótesis de la hipótesis específica.

**Tabla 40**

*Prueba de muestras relacionadas en contraste a la hipótesis específica N° 1*

| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | t | gl | Sig. (bilateral) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inferior | Superior | | | |
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso - Proceso de control de acceso mediante sistema de reconocimiento de iris | -6,200 | ,862 | ,223 | -6,677 | -5,723 | -27,860 | 14 | ,000 |

Según la prueba de muestras relacionadas calculada, observamos que el p-valor es de 0,000. Como el valor de significancia establecida es de 0,05, podemos indicar que 0,000 < 0,05, rechazando la hipótesis específica nula N° 1, y aceptando la hipótesis específica alterna N° 1.

Por ende, se puede indicar que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

#### 4.3.2.2. Autenticación

- Siendo la hipótesis específica nula, el Sistema de Reconocimiento de Iris basado en Deep Learning no mejora el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
- Siendo la hipótesis específica alterna, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

La Tabla 41 muestra los grupos estadísticos que representan a las muestras del proceso actual de control de acceso, y proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, indicando datos estadísticos en contraste a la hipótesis específica.

**Tabla 41**

*Grupo estadístico en contraste a la hipótesis específica N° 2*

| | | Media | N | Desv. Desviación | Desv. Error promedio |
|---|---|---|---|---|---|
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso | 10,27 | 15 | ,458 | ,118 |
| | Proceso de control de acceso mediante sistema de reconocimiento de iris | 14,53 | 15 | ,516 | ,133 |

Así mismo, en la Tabla 42 se visualiza la ejecución de la prueba T de muestras relacionadas, entre la muestra del proceso actual de control de acceso, y muestra del

proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, generando datos estadísticos para el respectivo contraste de hipótesis de la hipótesis específica.

**Tabla 42**

*Prueba de muestras relacionadas en contraste a la hipótesis específica N° 2*

| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | t | gl | Sig. (bilateral) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inferior | Superior | | | |
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso - Proceso de control de acceso mediante sistema de reconocimiento de iris | -4,267 | ,594 | ,153 | -4,595 | -3,938 | -27,837 | 14 | ,000 |

Según la prueba de muestras relacionadas calculada, observamos que el p-valor es de 0,000. Como el valor de significancia establecida es de 0,05, podemos indicar que 0,000 < 0,05, rechazando la hipótesis específica nula N° 2, y aceptando la hipótesis específica alterna N° 2.

Por ende, se puede indicar que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

#### 4.3.2.3. Autorización

- Siendo la hipótesis específica nula, el Sistema de Reconocimiento de Iris basado en Deep Learning no mejora el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
- Siendo la hipótesis específica alterna, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autorización del

acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

La Tabla 43 muestra los grupos estadísticos que representan a las muestras del proceso actual de control de acceso, y proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, indicando datos estadísticos en contraste a la hipótesis específica.

**Tabla 43**

*Grupo estadístico en contraste a la hipótesis específica N° 3*

| | | Media | N | Desv. Desviación | Desv. Error promedio |
|---|---|---|---|---|---|
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso | 7,00 | 15 | ,000 | ,000 |
| | Proceso de control de acceso mediante sistema de reconocimiento de iris | 15,00 | 15 | ,000 | ,000 |

Así mismo, en la Tabla 44 se visualiza la ejecución de la prueba T de muestras relacionadas, entre la muestra del proceso actual de control de acceso, y muestra del proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, generando datos estadísticos para el respectivo contraste de hipótesis de la hipótesis específica.

**Tabla 44**

*Prueba de muestras relacionadas en contraste a la hipótesis específica N° 3*

| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | t | gl | Sig. (bilateral) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inferior | Superior | | | |
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso - Proceso de control de acceso mediante sistema de reconocimiento de iris | -8,000 | ,000 | ,000 | - | - | - | 14 | ,000 |

Según la prueba de muestras relacionadas calculada, observamos que el p-valor es de 0,000. Como el valor de significancia establecida es de 0,05, podemos indicar que 0,000 < 0,05, rechazando la hipótesis específica nula N° 3, y aceptando la hipótesis específica alterna N° 3.

Por ende, se puede indicar que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

#### 4.3.2.4. Trazabilidad

- Siendo la hipótesis específica nula, el Sistema de Reconocimiento de Iris basado en Deep Learning no mejora el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.
- Siendo la hipótesis específica alterna, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

La Tabla 45 muestra los grupos estadísticos que representan a las muestras del proceso actual de control de acceso, y proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, indicando datos estadísticos en contraste a la hipótesis específica.

**Tabla 45**

*Grupo estadístico en contraste a la hipótesis específica N° 4*

| | | Media | N | Desv. Desviación | Desv. Error promedio |
|---|---|---|---|---|---|
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso | 7,00 | 15 | ,000 | ,000 |
| | Proceso de control de acceso mediante sistema de reconocimiento de iris | 15,00 | 15 | ,000 | ,000 |

Así mismo, en la Tabla 46 se visualiza la ejecución de la prueba T de muestras relacionadas, entre la muestra del proceso actual de control de acceso, y muestra del proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris, generando datos estadísticos para el respectivo contraste de hipótesis de la hipótesis específica.

**Tabla 46**

*Prueba de muestras relacionadas en contraste a la hipótesis específica N° 4*

| | | Media | Desv. Desviación | Desv. Error promedio | 95% de intervalo de confianza de la diferencia | | t | gl | Sig. (bilateral) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inferior | Superior | | | |
| Nivel de seguridad en control de acceso | Proceso actual tradicional de control de acceso - Proceso de control de acceso mediante sistema de reconocimiento de iris | -8,000 | ,000 | ,000 | - | - | - | 14 | ,000 |

Según la prueba de muestras relacionadas calculada, observamos que el p-valor es de 0,000. Como el valor de significancia establecida es de 0,05, podemos indicar que 0,000 < 0,05, rechazando la hipótesis específica nula N° 4, y aceptando la hipótesis específica alterna N° 4.

Por ende, se puede indicar que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

### 4.4. Sistema de Reconocimiento de Iris para control de acceso – SRICA

SRICA, Sistema de Reconocimiento de Iris para control de acceso, es el proyecto diseñado y desarrollado para la presente investigación, el cual, está constituido de diversos procesos de software y hardware intercomunicados entre sí para proporcionar una herramienta de control de acceso a espacios físicos.

En los siguientes puntos, se describirán diversos aspectos que constituyen el SRICA: metodología de desarrollo de software adoptado, construcción del equipo lector de iris y estándar de seguridad fotobiológica para luces infrarrojo (IR), algoritmos de aprendizaje profundo para el procesamiento de imagen del iris humano, y el respectivo proceso de despliegue de la herramienta en las instalaciones del Gobierno Regional de Tacna.

### 4.4.1. Metodología de desarrollo de software

RUP, Proceso Racional Unificado, es una metodología de desarrollo de software tradicional que permite segmentar y agrupar los diversos pasos de desarrollo de sistemas en cuatro fases: inicio, elaboración, construcción y transición (cierre).

En el Anexo 5 se describe, a detalle, la metodología RUP adoptada para el respectivo desarrollo del proyecto, indicando los diferentes entregables o elementos de configuración de software comprendidos en cada fase de la metodología.

### 4.4.2. Equipo biométrico lector de iris y estándar IEC-62471

SRICA, cuenta con un equipo interconectado a diversos componentes electrónicos que controlan, físicamente, el acceso al espacio físico, el cual se instaló en la puerta de acceso del lugar para permitir o denegar la entrada de personas. Este equipo se encarga de capturar la imagen del iris de la persona, para, posteriormente, enviarlo a los diversos procesos y/o servicios del SRICA, el cual será procesada por los diferentes algoritmos de aprendizaje profundo, resultando en el permiso o denegación del acceso correspondiente. En el Anexo 6 se describe, a detalle, el equipo biométrico lector desarrollado, los componentes electrónicos utilizados, y ciertos aspectos técnicos.

El equipo biométrico lector de iris desarrollado, cuenta con una cámara que emite luz infrarroja (IR) para lograr capturar todas las características biológicas del iris humano en una imagen en blanco y negro. Para proteger la salud de las personas ante la luz infrarroja emitida, y evitar cualquier daño ocular o en la piel, se ha optado por usar el estándar IEC-62471 de seguridad fotobiológica para aplicaciones con luz IR, donde, el desarrollo de las fórmulas establecidas por el estándar, son descritas y calculadas en el Anexo 8.

### 4.4.3. Deep Learning

SRICA, dentro de los diversos procesos y/o servicios que contiene, se encuentran los procesos de procesamiento de imágenes, donde se utiliza algoritmos de aprendizaje profundo (Deep Learning) para la respectiva detección, segmentación, codificación, y reconocimiento del iris de la persona. Para la creación de los modelos de Deep Learning, se ha optado por utilizar herramientas altamente eficientes para el entrenamiento e inferencia, detectando y segmentado las imágenes de iris.

Para la codificación y reconocimiento del iris, se ha utilizado un modelo entrenado con miles de imágenes de iris, el cual fue necesario para aplicar el concepto de One Shot Learning y Redes Siamesas, logrando la codificación (mapa de características) y el reconocimiento correspondiente de la persona. En el Anexo 7 se muestra, a detalle, el apartado Deep Learning del SRICA, donde se indican los modelos entrenados y utilizados, herramientas, procesos y pipelines respectivos.

### 4.4.4. Instalación y despliegue en el Gobierno Regional de Tacna

SRICA, fue instalado en la sede Hipólito Unanue del Gobierno Regional de Tacna, específicamente en la entrada del almacén del área de Tesorería de la misma entidad pública. En el Anexo 9 se describe, a detalle, el proceso de instalación de los diversos compontes electrónicos y equipo biométrico lector de iris, que permitieron controlar el acceso al espacio físico.

Así mismo, para lograr el proceso de instalación y aplicación del proyecto en las instalaciones del Gobierno Regional de Tacna, fue necesario solicitar el respectivo permiso de acceso para cumplir con la investigación, donde, en el Anexo 12, se detalla el proceso de solicitud y aceptación del proyecto respectivo.

## 4.5. Análisis de costo - beneficio

Para el análisis del costo del proyecto “Sistema de Reconocimiento de Iris para Control de Acceso”, SRICA, se han determinado múltiples factores, de los cuales, implica el costo total de desarrollo del proyecto en sus diferentes fases según la metodología RUP, y el costo total de los dispositivos electrónicos utilizados para la respectiva integración de componentes. Así mismo, se está considerando el costo con respecto al uso de servicios y de mantenimiento que son aplicados a la solución tecnología, de forma anual. El área de Tesorería, mediante el Gobierno Regional de Tacna, según la

definición de costos establecida, deberá considerar y/o invertir para el respectivo desarrollo y aplicación del proyecto propuesto.

Para el análisis del beneficio obtenido por la aplicación de la solución tecnológica, se ha optado por realizar y aplicar el estudio de eficiencia de procesos que corresponde al concepto de rediseño de procesos de negocio, considerando la eficiencia como beneficio, debido a que, el área de Tesorería no cuenta con ingresos propios económicos, siendo la misma entidad quien percibe ingresos anualmente. En este estudio se han definido aspectos cuantificables que se manifiestan durante el proceso de control de acceso, realizando la respectiva comparación entre el proceso actual y proceso propuesto. Del mismo modo, mediante el estudio realizado, se pretende obtener la eficiencia y eficacia del proceso de control de acceso con el uso del proyecto, determinando los beneficios y mejoras que justifican la inversión y aplicación de la solución tecnológica.

### 4.5.1. Análisis de costos

Para obtener el esfuerzo y costo al desarrollar el proyecto “Sistema de Reconocimiento de Iris”, siguiendo una metodología de desarrollo o de gestión de proyectos, como lo es RUP, se está utilizando el modelo de estimación de costos “Descomposición Top - Down”, siguiendo un conjunto de tareas definidas por la Estructura de Desglose de Trabajo, el cual puede ser visualizado en el Anexo 5.

Dentro del Anexo 5, se puede contemplar el documento elaborado para planificar la gestión de costos SRICA_012_000 - Plan de Gestión de Costos, donde se indican aspectos a considerar durante la estimación de costos por actividad, duración por actividad, y el presupuesto total de desarrollo del proyecto.

El resumen de costos totales del proyecto puede ser vistos en la Tabla 47, donde se indican diferentes conceptos de costos para el respectivo desarrollo de la solución tecnológica, que comprende apartados de software (siguiendo la metodología de desarrollo RUP), y hardware (componentes y equipos electrónicos).

**Tabla 47**

*Costo total del software y hardware del proyecto*

| | Conceptos | Cantidad | Costo Unitario | Costo Total | % |
|---|---|---|---|---|---|
| Software | Inicio | - | - | 630,00 | 1,86 |

(continúa)

Tabla 47 (continuación)

| | Conceptos | Cantidad | Costo Unitario | Costo Total | % |
|---|---|---|---|---|---|
| Software | Elaboración | - | - | 4185,00 | 12,33 |
| | Construcción | - | - | 28200,00 | 83,11 |
| | Cierre | - | - | 915,00 | 2,70 |
| | | | Sub Total (S./) | 33930,00 | 100 |
| Hardware | Equipo biométrico | 1 | 930,00 | 930,00 | 54,87 |
| | Cámara capturador registrador de iris | 1 | 365,00 | 365,00 | 21,53 |
| | Kit electroimán | 1 | 340,00 | 340,00 | 20,06 |
| | Botón de apertura | 1 | 60,00 | 60,00 | 3,54 |
| | | | Sub Total (S./) | 1695,00 | 100 |
| | | | Total (S./) | 35625,00 | |

Así mismo, en la Tabla 48 se visualiza el resumen de costos para conceptos de contratación de servicios externos (electricidad, servicios en la nube para el despliegue del proyecto), y de mantenimiento (limpieza de componentes y equipos electrónicos).

**Tabla 48**

*Costo total de servicios y de mantenimiento del proyecto*

| | Conceptos | Cantidad | Costo Unitario | Costo Total | % |
|---|---|---|---|---|---|
| Servicio | Microsoft Azure Cloud | 1 año | 3941,61 | 3941,61 | 98,00 |
| | Electricidad | 1 año | 80,42 | 80,42 | 2,00 |
| | Sub Total (S./) | | | 4022,03 | 100 |
| Mantenimiento | Mantenimiento de circuitos y limpieza de polvo (equipo lector, electroimán, botón de apertura) | 1 año | 40,00 x cada 6 meses | 80,00 | 66,67 |

(continúa)

Tabla 48 (continuación)

| | Conceptos | Cantidad | Costo Unitario | Costo Total | % |
|---|---|---|---|---|---|
| Mantenimiento | Limpieza del lente de cámaras capturadoras (cámara del equipo lector, cámara capturador registrador de iris) | 1 año | 20,00 x cada 6 meses | 40,00 | 33,33 |
| | Sub Total (S./) | | | 120,00 | 100 |
| | Total (S./) | | | 4142,03 | |

A continuación, se precisan ciertos aspectos establecidos en la Tabla 47 y Tabla 48:

- Para el desarrollo del proyecto, se está considerando 1 recurso / persona, con un tiempo total de 1 año de desarrollo, incluyendo tanto software y hardware.
- Según el cuadro de costo total del software y hardware del proyecto, se indica el sub monto referente al apartado “Software” que el área de Tesorería, como principal interesado, y que pertenece al Gobierno Regional de Tacna, invertirá para desarrollar, desde cero, el Sistema de Reconocimiento de Iris, contratando 1 recurso / persona durante 1 año, con un sueldo aproximado de S./ 2800,00.
- Según el cuadro de costo total del software y hardware del proyecto, se indica el sub monto referente al apartado “Hardware” que el área de Tesorería, como principal interesado, y que pertenece al Gobierno Regional de Tacna, invertirá para adquirir los componentes electrónicos necesarios para integrar el Sistema de Reconocimiento de Iris, los cuales, tales costos pueden ser visualizados en el Anexo 13.
- Según el cuadro de costo total de servicios y de mantenimiento del proyecto, se indica el sub monto referente al apartado “Servicio”, con concepto “Microsoft Azure Cloud”, que el área de Tesorería, como principal interesado, y que pertenece al Gobierno Regional de Tacna, invertirá, de forma anual, si opta por adquirir la solución cloud de Microsoft Azure para el despliegue del proyecto. Caso contrario de no adquirir la solución cloud, este monto puede

ser no considerado, ya que el proyecto permite ser desplegado en cualquier servidor que la misma entidad pública pueda tener, sin algún equipamiento especial.

- Según el cuadro de costo total de servicios y de mantenimiento del proyecto, se indica el sub monto referente al apartado “Servicio”, con concepto “Electricidad”, que el área de Tesorería, como principal interesado, y que pertenece al Gobierno Regional de Tacna, invertirá, de forma anual, para asumir los costos de electricidad que los componentes electrónicos consumirán al estar conectados a la red eléctrica de la entidad.
- Según el cuadro de costo total de servicios y de mantenimiento del proyecto, se indica el sub monto referente al apartado “Mantenimiento” que el área de Tesorería, como principal interesado, y que pertenece al Gobierno Regional de Tacna, invertirá, de forma anual, para dar mantenimiento al equipo lector biométrico, y demás componentes electrónicos.

### 4.5.2. Análisis de eficiencia como beneficio

Para analizar la eficiencia del Sistema de Reconocimiento de Iris para el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, se utilizará el estudio de eficiencia de procesos correspondiente a la teoría de rediseño de procesos de negocio, considerando la eficiencia resultante como beneficio. Se está optando por el estudio indicado anteriormente debido a que, el área de Tesorería no percibe o genera ingresos propios económicos, siendo el Gobierno Regional de Tacna quien percibe ingresos económicos, de forma anual, por el Gobierno Central del Perú, para la realización y cumplimiento de los planes de ejecución. Así mismo, se está optando por el estudio de eficiencia debido a la limitación de información de gastos económicos del área de Tesorería.

En la Tabla 49 se visualiza la comparación en aspectos cuantificables de seguridad que se presentan durante el proceso de control de acceso, sin intervención de la solución propuesta (proceso actual), y con intervención de la solución propuesta (abstraídas del resultante de la aplicación del proyecto, cuyo análisis se encuentra en el Anexo 11), del cual, se puede verificar la existencia de mejoras entre los valores de cada aspecto cuantificable señalado con respecto al proceso propuesto, y las deficiencias del proceso actual de control de acceso. Dentro de los valores del proceso propuesto, se logra visualizar los diferentes valores en porcentajes, frecuencias, cantidades, y tiempos obtenidos, presentando mejoras notables, como también, la

integración y participación del rol de Seguridad de la entidad durante el proceso de control.

**Tabla 49**

*Cuantificación de aspectos de seguridad durante el proceso de control de acceso*

| Aspectos de Seguridad | Proceso Actual | Proceso Propuesto |
|---|---|---|
| Uso de recursos humanos | 01 – Jefe o encargado de área de Tesorería; 01 – Trabajador | 01 – Jefe o encargado de área de Tesorería; 01 – Personal de Seguridad; 01 – Trabajador |
| Uso de recursos físicos | 01 – Llave y cerradura | 01 – Equipo de registro de accesos; 01 – Equipo controlador de accesos; 01 – Equipo de seguridad de puerta |
| Tiempo de asignación de accesos al trabajador | 5 minutos (espera y entrega de la llave de acceso) | 1 minuto (registro del acceso correspondiente – una vez por trabajador) |
| Participación de seguridad institucional en la asignación de accesos | 0% (sin participación) | 100% (personal de seguridad participa en el registro del acceso correspondiente) |
| Eventualidad de registro de bitácora de asignación de accesos | 0% (sin registros) | 100% (bitácora registrada) |
| Complejidad de seguridad del identificador otorgado | Llave – Nivel bajo (no anti ganzúa, no anti bumping, no copia controlada) | Iris – Nivel alto (patrón y estructura biológica, no reproducible) |
| Unicidad del identificador otorgado | Llave – Nivel de relación “1 – N” (un identificador para todos los trabajadores) | Iris – Nivel de relación “1 – 1” (un identificador para cada trabajador) |
| Complejidad de la estructura de puerta de acceso | Cerradura tradicional – Nivel medio | Equipo de control de puerta (controlador de accesos, seguridad de puerta) – Nivel Alto |
| Frecuencia de uso del identificador otorgado de acceso | 100% de uso para el acceso | 100% de uso para el acceso |

(continúa)

Tabla 49 (continuación)

| Aspectos de Seguridad | Proceso Actual | Proceso Propuesto |
|---|---|---|
| Frecuencia de comprobación del trabajador por parte de seguridad institucional o control en el acceso | 0% (sin comprobación del trabajador por parte de seguridad institucional o control) | 100% (equipo controlador de accesos comprueba la identidad del trabajador) |
| Tiempo de autenticación del identificador del trabajador | 6 segundos (según llave de acceso y cerradura) | 4,13 segundos (promedio) |
| Suplantación de identidad del trabajador | 100% (identificador global para todos los trabajadores, y sin comprobación por parte de seguridad institucional) | 0% (identificador único para cada trabajador, y verificado por el equipo controlador de accesos) |
| Eventualidad de registro de bitácora de autenticación del trabajador | 0% (sin registros) | 100% (bitácora registrada) |
| Otorgación individual de accesos al trabajador | 0% (sin autorización individual de acceso por trabajador) | 100% (con autorización individual de acceso por trabajador) |
| Eventualidad de registro de bitácora de otorgación de accesos al trabajador | 0% (sin registros) | 100% (bitácora registrada) |
| Eventualidad de registro de bitácora de intentos de acceso | 0% (sin registros) | 100% (bitácora registrada) |

Tal como se presentaron las diferencias en aspectos de seguridad para el proceso actual y proceso con el uso de la solución tecnológica, en la Tabla 50 se visualiza el estudio de eficiencia del proceso actual de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, donde se han indicado las actividades correspondientes al proceso de control de acceso que comúnmente es realizado por el área en cuestión, y los tiempos de duración de cada actividad, resultando en un porcentaje de eficiencia del 58,91%.

**Tabla 50**

*Estudio de eficiencia del proceso de control de acceso – sin intervención del proyecto propuesto*

| Estudio de la Eficiencia de Procesos (Proceso Actual) | | | | | | |
|---|---|---|---|---|---|---|
| Proceso | Control de acceso al almacén del área de Tesorería | | | | | |
| Analizado por | Luis Eduardo Mamani Bedregal (Director del proyecto) | | | | | |
| Actividad | Tiempo | | | | | |
| Se selecciona a la persona que accederá al almacén para buscar la información requerida. | 5 s | | | | X | |
| La persona espera la entrega de la llave de acceso por parte del jefe o encargado del área de Tesorería. | 5 min | | | | X | |
| Se entrega la llave de acceso a la persona. | 10 s | | X | | | |
| La persona se dirige al almacén ubicado en la sede Hipólito Unanue. | 15 min | | X | | | |
| La persona se dirige a la puerta de acceso. | 30 s | | X | | | |
| La persona prepara la llave de acceso para proceder con la apertura de la puerta de acceso. | 5 s | | | | X | |
| Se inserta la llave de acceso en la cerradura para abrir la puerta de acceso. | 6 s | | | | X | |
| La persona ingresa al almacén. | 3 s | | X | | | |
| La persona realiza las operaciones correspondientes y recopilación de información dentro del almacén. | 1 h | X | | | | |
| La persona sale del almacén. | 3 s | | X | | | |
| Se cierra la puerta de acceso del almacén. | 2 s | | | | X | |
| Se utiliza la llave de acceso para cerrar el almacén. | 6 s | | | | X | |
| Se comprueba que la puerta de acceso se encuentre correctamente cerrada. | 5 s | | | X | | |

(continúa)

Tabla 50 (continuación)

| Actividad | Tiempo | | | | | |
|---|---|---|---|---|---|---|
| La persona retorna a la sede Central. | 15 min | | X | | | |
| La persona se dirige al área de Tesorería. | 30 s | | X | | | |
| Se entrega la información requerida al personal correspondiente. | 5 s | X | | | | |
| La persona espera al jefe o encargado del área de Tesorería para devolver la llave de acceso. | 5 min | | | | X | |
| Se devuelve la llave de acceso. | 5 s | | X | | | |
| Se guarda la llave de acceso. | 10 s | | | | X | |
| Tiempo de operación (min) | 60,08 | | | | | |
| Tiempo total del proceso (min) | 102,00 | | | | | |
| Eficiencia del proceso (%) | 58,91 | | | | | |

Del mismo modo, en la Tabla 51 se visualiza el estudio de eficiencia del proceso propuesto de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, donde se han indicado las actividades correspondientes al proceso de control de acceso con el uso de la solución tecnológica, y los tiempos de duración de cada actividad, resultando en un porcentaje de eficiencia del 65,76%, logrando una mejora del 6,85%, y la reducción y optimización de actividades en comparación con el proceso actual de control de acceso (el proceso de control de acceso propuesto con el uso de la solución tecnológica, puede ser visualizada en el Anexo 10).

**Tabla 51**

*Estudio de eficiencia del proceso de control de acceso – con intervención del proyecto propuesto*

| Estudio de la Eficiencia de Procesos (Proceso Propuesto) | | | | | | |
|---|---|---|---|---|---|---|
| Proceso | Control de acceso al almacén del área de Tesorería | | | | | |
| Analizado por | Luis Eduardo Mamani Bedregal (Director del proyecto) | | | | | |
| Actividad | Tiempo | | | | | |
| Se selecciona a la persona que accederá al almacén para buscar la información requerida. | 5 s | | | | X | |

(continúa)

Tabla 51 (continuación)

| Actividad | **Tiempo** | | | | | |
|---|---|---|---|---|---|---|
| Se realiza el registro del acceso de la persona que accederá al almacén (una sola vez por persona – tiempo no se contabiliza). | 0 s | | | | X | |
| La persona se dirige al almacén ubicado en la sede Hipólito Unanue. | 15 min | | X | | | |
| La persona se dirige a la puerta de acceso. | 30 s | | X | | | |
| Se realiza la autenticación de la persona para la respectiva apertura de la puerta de acceso. | 4.13 s | | | | X | |
| La persona ingresa al almacén. | 3 s | | X | | | |
| La persona realiza las operaciones correspondientes y recopilación de información dentro del almacén. | 1 h | X | | | | |
| La persona sale del almacén. | 3 s | | X | | | |
| Se cierra la puerta de acceso del almacén y se asegura mediante el equipo de seguridad de la puerta. | 2 s | | | | X | |
| La persona retorna a la sede Central. | 15 min | | X | | | |
| La persona se dirige al área de Tesorería. | 30 s | | X | | | |
| Se entrega la información requerida al personal correspondiente. | 5 s | X | | | | |
| Tiempo de operación (min) | 60,08 | | | | | |
| Tiempo total del proceso (min) | 91,37 | | | | | |
| Eficiencia del proceso (%) | 65,76 | | | | | |

# CAPÍTULO V: DISCUSIÓN

La presente investigación conlleva a un análisis y discusión que se presenta a continuación: Se encuentran diferencias estadísticamente significativas con respecto a los resultados encontrados que evalúan los niveles de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

Según los resultados obtenidos, se ha encontrado que existen semejanzas entre los hallazgos de los investigadores San Martín (2019), Bravo (2019), y Vargas (2016), donde todos ellos manifiestan que, mediante un sistema automatizado e inteligente para el respectivo control de acceso, los niveles de seguridad mejoraron, evitando múltiples problemas de seguridad física, optimización y reducción de tiempos en el proceso de control de acceso, registros de auditoría, y aprobación de las personas intervinientes durante la investigación.

Los objetivos específicos indicados en la investigación fueron de determinar los niveles de seguridad en cuatro fases o etapas que contempla el proceso de control de acceso, para el ingreso al almacén del área de Tesorería del Gobierno Regional de Tacna mediante la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.

Por lo tanto, frente a las hipótesis especificas indicadas en la investigación, que concuerdan con los objetivos específicos señalados, los resultados indican que, el Sistema de Reconocimiento de Iris basado en Deep Learning mejora significativamente el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.

Cabe señalar que, los resultados obtenidos en el capítulo anterior son de mucha importancia, debido al impacto positivo en niveles de seguridad que logran determinar los sistemas automatizados e inteligentes para el control de acceso frente al control de acceso tradicional. Del mismo modo, los resultados dan a conocer que aún sigue existiendo brecha tecnológica en el Perú, un tema bastante preocupante que debe ser disminuido mediante la fomentación de investigación e interés de transformación digital.

# CONCLUSIONES

De la información recopilada mediante el uso del instrumento Ficha de Evaluación, y mediante los resultados de la contrastación de hipótesis, que, con resultado p-valor 0,000, aceptando la hipótesis específica alterna N° 1, el nivel de seguridad en la identificación del personal durante el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, ha mejorado a un 97,3% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning, frente a los 56,0% del proceso de control de acceso actual tradicional.

De la información recopilada mediante el uso del instrumento Ficha de Evaluación, y mediante los resultados de la contrastación de hipótesis, que, con resultado p-valor 0,000, aceptando la hipótesis específica alterna N° 2, el nivel de seguridad en la autenticación del personal durante el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, ha mejorado a un 96,8% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning, frente a los 68,4% del proceso de control de acceso actual tradicional.

De la información recopilada mediante el uso del instrumento Ficha de Evaluación, y mediante los resultados de la contrastación de hipótesis, que, con resultado p-valor 0,000, aceptando la hipótesis específica alterna N° 3, el nivel de seguridad en la autorización del personal durante el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, ha mejorado a un 100% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning, frente a los 46,6% del proceso de control de acceso actual tradicional.

De la información recopilada mediante el uso del instrumento Ficha de Evaluación, y mediante los resultados de la contrastación de hipótesis, que, con resultado p-valor 0,000, aceptando la hipótesis específica alterna N° 4, el nivel de seguridad en la trazabilidad del personal durante el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, ha mejorado a un 100% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning, frente al 20,0% del proceso de control de acceso actual tradicional.

En conclusión, de la información recopilada mediante el uso del instrumento Ficha de Evaluación, y mediante los resultados de la contrastación de hipótesis, que, con

resultado p-valor 0,000, aceptando la hipótesis general alterna, el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, ha mejorado significativamente a un 98,5% mediante el uso del Sistema de Reconocimiento de Iris basado en Deep Learning, frente al 47,7% del proceso de control de acceso actual tradicional.

# RECOMENDACIONES

Se recomienda utilizar una cámara más potente que permita capturar las imágenes de ojos desde una distancia más lejana, para disminuir, aún más, la exposición a la luz IR (según estándar IEC-62471), agregar la posibilidad de reconocimiento de iris cuando la persona utilice lentes, y aplicar el concepto de “tracking” para realizar el seguimiento de ojos, evitando que la persona realice movimientos de cabeza para la respectiva captura de imágenes, para mejorar los resultados obtenidos durante la evaluación y contraste de la hipótesis especifica alterna N° 1.

Se recomienda aplicar técnicas de multihilo para realizar múltiples procesos simultaneaos y reducir, aún más, el tiempo de respuesta. Del mismo modo, mejorar el código para evitar que grandes cantidades de información, referentes a imágenes, sean enviadas a los servicios de procesamiento de imágenes, utilizando técnicas de compresión u otra forma alterna, para mejorar los resultados obtenidos durante la evaluación y contraste de la hipótesis específica alterna N° 2.

Se recomienda que, para otorgar correctamente los permisos al personal autenticado, y que los usuarios confíen en la aplicación, se debe contemplar un correcto modelo de Deep Learning para la extracción de características, y utilizar herramientas que ayuden a mejorar la calidad de datos durante el proceso de extracción de características (filtros y técnicas), para mantener, o mejorar aún más, los resultados obtenidos durante la evaluación y contraste de hipótesis especifica alterna N° 3.

Se recomienda que, para lograr completamente la trazabilidad de SRICA, aparte de los registros, de inicio a fin, de los eventos y acciones del Sistema de Reconocimiento de Iris provenientes del aplicativo web y equipo lector biométrico, incluyendo los registros de accesos denegados o concedidos, se debe contemplar el desarrollo de una funcionalidad que permita obtener información del electroimán cuando éste cierra la puerta de acceso, y obtener información del botón de apertura cuando el personal, desde el interior del espacio físico, lo acciona para abrir la puerta de acceso y salir del lugar, manteniendo, o mejorando aún más, los resultados obtenidos durante la evaluación y contraste de hipótesis especifica alterna N° 4.

Se recomienda seguir las recomendaciones anteriores para mejorar los resultados y evaluaciones de SRICA, para lograr mejores puntajes obtenidos durante la evaluación y contraste de la hipótesis general alterna.

## REFERENCIAS BIBLIOGRÁFICAS


Aggarwal, C. C. (2018). *Neural Networks and Deep Learning* (1st ed.). Springer, Cham. https://doi.org/10.1007/978-3-319-94463-0

Al-Owaid, A., Alarfaj, M., Al-Qahtani, A., & Al-Arfaj, K. (2019). Congenital Microcoria in a Saudi Family. *Ophthalmic Genetics*, *40*(6), 578–580. https://doi.org/10.1080/13816810.2019.1692360

Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., Hasan, M., Van Essen, B. C., Awwal, A. A. S., & Asari, V. K. (2019). A State-of-the-Art Survey on Deep Learning Theory and Architectures. *Electronics*, *8*(3). https://doi.org/10.3390/electronics8030292

Alpaydin, E. (2020). *Introduction to Machine Learning* (4th ed.). The MIT Press.

Alsaadi, I. M. (2015). Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. *International Journal of Scientific & Technology Research*, *4*(12), 285–289. https://www.ijstr.org/final-print/dec2015/Physiological-Biometric-Authentication-Systems-Advantages-Disadvantages-And-Future-Development-A-Review.pdf

Balas, V. E., Roy, S. S., Sharma, D., & Samui, P. (2019). *Handbook of Deep Learning Applications* (1st ed.). Springer, Cham. https://doi.org/10.1007/978-3-030-11479-4

Barrett, M. P. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. In *Proceedings of the Annual ISA Analysis Division Symposium* (Vol. 535). https://doi.org/10.6028/NIST.CSWP.04162018

Bochkovskiy, A., Wang, C.-Y., & Liao, H.-Y. M. (2020). *YOLOv4: Optimal Speed and Accuracy of Object Detection*.

Bowyer, K. W., & Burge, M. J. (2016). Handbook of Iris Recognition. In *Handbook of Iris Recognition* (2nd ed.). Springer, London. https://doi.org/10.1007/978-1-4471-6784-6

Boyd, A., Czajka, A., & Bowyer, K. (2020). *Deep Learning-Based Feature Extraction in Iris Recognition: Use Existing Models, Fine-tune or Train From Scratch?* arXiv. https://doi.org/10.48550/ARXIV.2002.08916

Bravo Pareja, J. J. (2019). *Diseño e Implementación de un Sistema de Control de*

*Acceso a los Campus de la Universidad Tecnológica del Perú - UTP* [Universidad Tecnológica del Perú]. http://repositorio.utp.edu.pe/handle/UTP/2717

Brooks, J. (2019). *COCO Annotator*. https://github.com/jsbroks/coco-annotator

Brown, D. (2010). *Asuntos de la Visión para las Personas con el Síndrome de CHARGE*.

Buitrago, F., & Romero, C. (2018). *Biometría*. https://www.fintechgracion.com/wp-content/uploads/Biometria_Libro.pdf

Caballero Romero, A. (2009). *Innovaciones en las Guías Metodológicas para los Planes y Tesis de Maestría y Doctorado* (2nd ed.). Instituto Metodológico ALEN CARO.

Camargo Cerón, A. M., Rojas López, R. F., & Serrano Camacho, J. C. (2003). Xantogranuloma Juvenil. Presentación de un Caso Clínico y Revisión del Tema. *MedUNAB*, *6*(18), 155–159.

Carrasco Díaz, S. (2005). *Metodología de la Investigación Científica* (1st ed.). Editorial San Marcos.

Dargan, S., Kumar, M., Ayyagari, M. R., & Kumar, G. (2019). A Survey of Deep Learning and Its Applications: A New Paradigm to Machine Learning. *Archives of Computational Methods in Engineering*. https://doi.org/10.1007/s11831-019-09344-w

Daugman, J. (2004). Recognising Persons by Their Iris Patterns. In S. Z. Li, J. Lai, T. Tan, G. Feng, & Y. Wang (Eds.), *Advances in Biometric Person Authentication* (pp. 5–25). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30548-4_4

Daugman, J. (2007). New Methods in Iris Recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *37*(5), 1167–1175. https://doi.org/10.1109/TSMCB.2007.903540

Ferreruela, R. (2007). La Visión y el Ojo. *Apunts: Educación Física y Deportes*, 8–14.

Gálvez Quiroz, F. M. (2000). Oftalmología Pediátrica. In *Cirugía: IV Oftalmología* (1st ed., pp. 187–201). Universidad Nacional Mayor de San Marcos.

García González, M. (2011). Enfermedades Sistémicas con Manifestaciones Oculares: Detección Precoz en Atención Primaria. *Canarias Pediátrica*, *35*(2), 135–137.

Garfias Tito, A. (2018). *Implementación de un Sistema Biométrico por Reconocimiento de Iris para el Registro y Control de Asistencia de los Internos en los Talleres del Establecimiento Penitenciario Ancón II* [Universidad Nacional José María Arguedas].

https://alicia.concytec.gob.pe/vufind/Record/UNAJ_1209e595987ede111e6d1ddd71582941

Geneser, F., Brüel, A., Christensen, E. I., Tranum-Jensen, J., & Qvortrup, K. (2015). *Geneser Histología* (4th ed.). Editorial Médica Paramericana.

Gladstone, R. M. (1969). Development and Significance of Heterochromia of the Iris. *Archives of Neurology*, *21*(2), 184–191. https://doi.org/10.1001/archneur.1969.00480140084008

Gregory, P. H. (2011). *Advanced Physical Access Control For Dummies* (HID Global). John Wiley & Sons, Inc., Hoboken, New Jersey.

Gregory, P. H., & Simon, M. A. (2008). *Biometrics for Dummies* (1st ed.). Wiley Publishing, Inc., Indianapolis, Indiana.

Gulyaev, P., & Filchenkov, A. (2020). Detection of Shocking Images as One-Class Classification Using Convolutional and Siamese Neural Networks. In L. Iliadis, P. P. Angelov, C. Jayne, & E. Pimenidis (Eds.), *Proceedings of the 21st EANN (Engineering Applications of Neural Networks) 2020 Conference* (Vol. 2, pp. 240–250). Springer International Publishing. https://doi.org/https://doi.org/10.1007/978-3-030-48791-1_18

Halfacree, G. (2019). *The Official Raspberry Pi Beginner's Guide: How to Use your New Computer* (3rd ed.). Raspberry Pi Trading Ltd, Maurice Wilkes Building, St. John's Innovation Park, Cowley Road, Cambridge, CB4 0DS.

Harakannanavar, S. S., Prashanth, C. R., Kanabur, V., Puranikmath, V. I., & Raja, K. B. (2019). An Extensive Study of Issues , Challenges and Achievements in Iris Recognition An Extensive Study of Issues , Challenges and Achievements in Iris Recognition. *Asian Journal of Electrical Sciences*, *8*(1), 25–35.

Hernández-García, R., Barrientos, R. J., Rojas, C., & Mora, M. (2019). Individuals Identification Based on Palm Vein Matching Under a Parallel Environment. *Applied Sciences (Switzerland)*, *9*(14). https://doi.org/10.3390/app9142805

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. Mcgraw Hill.

Hingorani, M., Hanson, I., & Van Heyningen, V. (2012). Aniridia. *European Journal of Human Genetics*, *20*(10), 1011–1017. https://doi.org/10.1038/ejhg.2012.100

Hurwitz, J., & Kirsch, D. (2018). *Machine Learning for Dummies* (IBM Limite). John Wiley & Sons, Inc.

ISO/IEC 25000. (2014). *Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Guide to SQuaRE*.

Jaidi, F. (2017). Advanced Access Control to Information Systems: Requirements, Compliance and Future Directives. In J. Sen (Ed.), *Advances in Security in Computing and Communications* (1st ed., pp. 83–99). InTech Open Publishers, Croatia. https://doi.org/10.5772/intechopen.69329

Keung, Y. H. (2014). Information Security Controls. *Advances in Robotics & Automation*, *3*(2). https://doi.org/10.4172/2168-9695.1000e118

Khanam, R., Haseen, Z., Rahman, N., & Singh, J. (2019). Performance Analysis of Iris Recognition System. In L. C. Jain, V. E. Balas, & P. Johri (Eds.), *Data and Communication Networks* (1st ed., Vol. 847, pp. 159–171). Springer Singapore. https://doi.org/10.1007/978-981-13-2254-9_14

Koong, C.-S., Yang, T.-I., & Tseng, C.-C. (2014). A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. *The Scientific World Journal*, *2014*. https://doi.org/10.1155/2014/781234

Li, S. Z., & Jain, A. K. (2015). *Encyclopedia of Biometrics* (2nd ed.). Springer, Boston, MA. https://doi.org/10.1007/978-1-4899-7488-4

Li, Y. H., Huang, P. J., & Juan, Y. (2019). An Efficient and Robust Iris Segmentation Algorithm Using Deep Learning. *Mobile Information Systems*. https://doi.org/10.1155/2019/4568929

Lozej, J., Stepec, D., Struc, V., & Peer, P. (2019). Influence of Segmentation on Deep Iris Recognition Performance. *2019 7th International Workshop on Biometrics and Forensics, IWBF 2019*, 1–6. https://doi.org/10.1109/IWBF.2019.8739225

Mahfouz, A., Mahmoud, T. M., & Eldin, A. S. (2017). A Survey on Behavioral Biometric Authentication on Smartphones. *Journal of Information Security and Applications*, *37*, 28–37. https://doi.org/10.1016/j.jisa.2017.10.002

Martín-Begué, N., Noval Martín, S., Barrio Barrio, J., & Galdós Iztueta, M. (2019). Protocolos en Neuro-Oftalmología Pediátrica. *Revista Acta Estrabológica*, *XLVIII*(2), 165–180.

Martínez Estrada, V., García Salazar, V., & Navarrete Franco, G. (2002). Xantogranuloma Juvenil. Reporte de un Caso. *Revista Del Centro Dermatológico Pascua*, *11*(1), 22–26.

Matilla Rodero, M. (2003). *Caracterización Patobiológica del Melanoma Uveal*

[Universidad de Málaga]. https://riuma.uma.es/xmlui/bitstream/handle/10630/2601/16700685.pdf

Montaña Duque, D. F. (2017). *Sistema de Identificación mediante Huella Digital para el Control de Accesos a la Universidad Libre Sede Bosque Popular simulado en un entorno web* [Universidad Libre Sede Bosque Popular]. https://repository.unilibre.edu.co/bitstream/handle/10901/10557/Proyecto de grado Daniel Felipe Montaña Duque.pdf?sequence=1&isAllowed=y

Moreno Londoño, M. V., Takane Imay, M., González González, M. C., Koga Nakamura, W., Estrada Reyes, C. E., & Islas de la Vega, G. (2014). Nódulos de Lisch y Ultrabiomicroscopia. *Revista Mexicana de Oftalmologia*, *88*(4), 189–193. https://doi.org/10.1016/j.mexoft.2014.05.004

O' Mahony, N., Campbell, S., Carvalho, A., Krpalkova, L., Velasco Hernandez, G., Harapanahalli, S., Riordan, D., & Walsh, J. (2019). One-Shot Learning for Custom Identification Tasks; A Review. *Procedia Manufacturing*, *38*(2019), 186–193. https://doi.org/10.1016/j.promfg.2020.01.025

Oh, J., Lee, U., & Lee, K. (2019). Usability Evaluation Model for Biometric System Considering Privacy Concern Based on MCDM Model. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/8715264

Oloyede, M. O., & Hancke, G. P. (2016). Unimodal and Multimodal Biometric Sensing Systems: A Review. *IEEE Access*, *4*, 7532–7555. https://doi.org/10.1109/ACCESS.2016.2614720

Oostdijk, M., van Velzen, A., van Dijk, J., & Terpstra, A. (2016). State-of-the-Art in Biometrics for Multi-Factor Authentication in a Federative Context. In *TNC16 Conference*. https://www.surf.nl/files/2019-03/201605-biometrics-english.pdf

Peltier, T. R. (2013). *Information Security Fundamentals* (2nd ed.). Auerbach Publications. https://doi.org/10.1201/b15573

Pérez Lescano, H. V. (2018). *Sistema de Control de Acceso por Reconocimiento de Iris para el ingreso de personal a la empresa electroservicios Querubín de la ciudad de Puyo* [Universidad Técnica de Ambato]. http://repositorio.uta.edu.ec/jspui/bitstream/123456789/28577/1/Tesis_ t1465ec.pdf

Proenca, H., & Neves, J. C. (2019). Segmentation-Less and Non-Holistic Deep-Learning Frameworks for Iris Recognition. *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.

http://openaccess.thecvf.com/content_CVPRW_2019/html/Biometrics/Proenca_Segmentation-Less_and_Non-Holistic_Deep-Learning_Frameworks_for_Iris_Recognition_CVPRW_2019_paper.html

Ramprasad, V., Sripriya, S., George, R., Nancarrow, D., Saxena, S., Hemamalini, A., Kumar, D., Vijaya, L., & Kumaramanicakvel, G. (2005). Genetic Homogeneity for Inherited Congenital Microcoria Loci in an Asian Indian Pedigree. *Molecular Vision*, *11*, 934–940. http://www.molvis.org/molvis/v11/a112/

Ravin, J. G. (2016). Iris Recognition Technology (or, Musings While Going through Airport Security). *American Academy of Ophthalmology*, *123*(10), 2054–2055. https://doi.org/10.1016/j.ophtha.2016.07.021

Ren, M., Wang, C., Wang, Y., Sun, Z., & Tan, T. (2019). Alignment Free and Distortion Robust Iris Recognition. *2019 International Conference on Biometrics (ICB)*, 1–7. https://doi.org/10.1109/icb45273.2019.8987369

Rodríguez Carracedo, G., Pintor, J., & Peral, A. (2007). Aniridia Congénita. *Gaceta Óptica: Órgano Oficial Del Colegio Nacional de Ópticos-Optometristas de España*, *420*, 10–14.

Ross, A., Banerjee, S., Chen, C., Chowdhury, A., Mirjalili, V., Sharma, R., Swearingen, T., & Yadav, S. (2019). Some Research Problems in Biometrics: The Future Beckons. *2019 International Conference on Biometrics (ICB)*, 1–8. https://doi.org/10.1109/icb45273.2019.8987307

Sabhanayagam, T., Prasanna Venkatesan, V., & Senthamaraikannan, K. (2018). A Comprehensive Survey on Various Biometric Systems. *International Journal of Applied Engineering Research*, *13*(5), 2276–2297.

Sakib, S., Ahmed, N., Jawad Kabir, A., & Ahmed, H. (2018). *An Overview of Convolutional Neural Network: Its Architecture and Applications*. *November*. https://doi.org/10.20944/preprints201811.0546.v1

Salas San Juan, O., Brooks Rodríguez, M., & Acosta Elizastigui, T. (2013). Síndromes Neurocutáneos Identificables por el Médico General Integral Mediante Examen Físico. *Revista Cubana de Medicina General Integral*, *29*(3), 325–335.

Samarati, P., & de Vimercati, S. C. (2001). Access Control: Policies, Models, and Mechanisms. In R. Focardi & R. Gorrieri (Eds.), *Foundations of Security Analysis and Design* (pp. 137–196). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45608-2_3

Sampedro Pérez, C., Rodriguez-Vazquez, J., Rodríguez Ramos, A., Carrio, A., & Campoy, P. (2019). Deep Learning-Based System for Automatic Recognition and Diagnosis of Electrical Insulator Strings. *IEEE Access*, *7*, 101283–101308. https://doi.org/10.1109/ACCESS.2019.2931144

San Martín Guillén, E. M. (2019). *Diseño e Implementación de un Sistema de Control de Acceso por Biometría* [Universidad Tecnológica del Perú]. http://repositorio.utp.edu.pe/handle/UTP/2648

Sánchez Carlessi, H., & Reyes Meza, C. (2006). *Metodología y Diseños en la Investigación Científica* (4th ed.). Visión Universitaria, Lima, Perú.

Sánchez Reíllo, R. (2000). El Iris Ocular como parámetro para la Identificación Biométrica. *Ágora Sic*, *21*. http://www.revistasic.com/revista41/pdf_41/SIC_41_agora.PDF

Shrestha, A., & Mahmood, A. (2019). Review of Deep Learning Algorithms and Architectures. *IEEE Access*, *7*, 53040–53065. https://doi.org/10.1109/ACCESS.2019.2912200

Sinha, G. R. (2019). Advances in Biometrics. Modern Methods and Implementation Strategies. In *Advances in Biometrics* (1st ed.). Springer, Cham. https://doi.org/10.1007/978-3-030-30436-2

Speroni Aguirre, F. (2016). *Diccionario de Anatomía e Histología* (1st ed.). Editorial de la Universidad Nacional de la Plata. https://libros.unlp.edu.ar/index.php/unlp/catalog/book/650

Tann, H., Zhao, H., & Reda, S. (2019). A resource-efficient embedded iris recognition system Using Fully Convolutional Networks. *ACM Journal on Emerging Technologies in Computing Systems*, *16*(1). https://doi.org/10.1145/3357796

Toulemont, P. J., Urvoy, M., Coscas, G., Lecallonnec, A., & Cuvilliers, A. F. (1995). Association of Congenital Microcoria with Myopia and Glaucoma: A Study of 23 Patients with Congenital Microcoria. *Ophthalmology*, *102*(2), 193–198. https://doi.org/10.1016/S0161-6420(95)31036-6

Traipe, L. (2017). *Fisiología Ocular*. https://www.oftalandes.cl/assets/uploads/2017/07/fisiologia_ocular_-_dr-_traipe.pdf

Tzutalin. (2015). *LabelImg*. Git code. https://github.com/tzutalin/labelImg

Vargas Vimos, X. A. (2016). *Diseño de un Prototipo de Control de Acceso del Personal*

*mediante Reconocimiento Facial en 3D para Empresas Públicas o Privadas* [Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/6034

Whitman, M. E., & Mattord, H. J. (2014). *Management of Information Security* (4th ed.). Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security* (6th ed.). Cengage Learning.

Wu, Y., Kirillov, A., Massa, F., Lo, W.-Y., & Girshick, R. (2019). *Detectron2*. https://github.com/facebookresearch/detectron2

Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. (2018). Convolutional Neural Networks: An Overview and Application in Radiology. *Insights into Imaging*, *9*, 611–629. https://doi.org/10.1007/s13244-018-0639-9

Zhang, A., Lipton, Z. C., Li, M., & Smola, A. J. (2020). *Dive into Deep Learning*. https://d2l.ai/

Zhang, D., Lu, G., & Zhang, L. (2018). *Advanced Biometrics* (1st ed.). Springer, Cham. https://doi.org/10.1007/978-3-319-61545-5

Zheng, S., Rahmat, R. W. O. K., Khalid, F., & Nasharuddin, N. A. (2019). *A Robust Iris Authentication System on GPU-Based Edge Devices using Multi-Modalities Learning Model*. http://arxiv.org/abs/1912.00756

# ANEXOS

# Anexo 1. Matriz de consistencia

| PROBLEMA | OBJETIVOS | HIPÓTESIS | VARIABLES | DIMENSIONES | INDICADORES | METODOLOGÍA |
|---|---|---|---|---|---|---|
| **Problema general**<br><br>¿Cómo es el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020? | **Objetivo general**<br><br>Determinar el nivel de seguridad para el proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020. | **Hipótesis general**<br><br>El Sistema de Reconocimiento de Iris basado en Deep Learning mejora significativamente el nivel de seguridad para el proceso de control de acceso al almacén de área de Tesorería del Gobierno Regional de Tacna – Tacna 2020. | **Variable independiente**<br><br>Sistema de Reconocimiento de Iris | Fiabilidad | - Disponibilidad del sistema<br>- Recuperabilidad del sistema<br>- Tolerancia a fallas | **Tipo de investigación:**<br><br>Aplicada<br><br>**Nivel de investigación:**<br><br>Experimental<br><br>**Población:**<br><br>15 personas<br><br>**Muestra:**<br><br>15 personas<br><br>**Técnica:**<br><br>Ficha de Evaluación<br><br>**Instrumento:**<br><br>Prueba de Comprobación<br><br>**Estadística:**<br><br>Contraste de Hipótesis mediante Prueba T de muestras relacionadas |
| | | | | Usabilidad | - Comprensibilidad del uso del sistema<br>- Flexibilidad del aprendizaje en el uso del sistema<br>- Operatividad del sistema<br>- Estética del sistema<br>- Accesibilidad al sistema | |
| | | | | Seguridad | - Confidencialidad de los datos del sistema<br>- Integridad del sistema<br>- Trazabilidad de acciones del sistema<br>- Autenticación de usuarios en el sistema | |
| | | | | Portabilidad | - Facilidad de la instalación del sistema<br>- Adaptabilidad del sistema en otros ambientes<br>- Capacidad del sistema en sufrir cambios | |
| **Problemas específicos**<br><br>a. ¿Cómo es el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?<br><br>b. ¿Cómo es el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un | **Objetivos específicos**<br><br>a. Determinar el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.<br><br>b. Determinar el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning. | **Hipótesis específicas**<br><br>a. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la identificación del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.<br><br>b. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en la autenticación del personal identificado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.<br><br>c. El Sistema de Reconocimiento de Iris basado en Deep Learning | **Variable dependiente**<br><br>Control de Acceso | Identificación | - Nivel de complejidad en la estructuración del identificador<br>- % de frecuencia del uso del identificador<br>- % de aceptabilidad del uso del identificador | |
| | | | | Autenticación | - Tiempo de demora en el proceso de autenticación<br>- % de acierto en la autenticación<br>- % de aceptación falsa | |
| | | | | Autorización | - % de acierto en la otorgación de permisos para el acceso al área requerida<br>- Nivel de confiabilidad en la otorgación de permisos<br>- % de accesos erróneos otorgados | |
| | | | | Trazabilidad | - Bitácora de acciones/eventos en los procesos<br>- Bitácora de intentos de ingreso por personal no autorizado<br>- Bitácora de accesos garantizados al personal | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Sistema de Reconocimiento de Iris basado en Deep Learning?<br><br>c. ¿Cómo es el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning?<br><br>d. ¿Cómo es el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning? | c. Determinar el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning.<br><br>d. Determinar el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning. | mejora el nivel de seguridad en la autorización del acceso del personal autenticado durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.<br><br>d. El Sistema de Reconocimiento de Iris basado en Deep Learning mejora el nivel de seguridad en el registro de trazabilidad de accesos del personal durante el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna. | **Variable interviniente**<br><br>Deep Learning | | - Nivel de complejidad de la arquitectura de redes neuronales<br>- Tiempo de pre-procesamiento de imágenes en la arquitectura de redes neuronales<br>- Tiempo de post-procesamiento de imágenes en la arquitectura de redes neuronales<br>- Tiempo de predicción de una clase<br>- Porcentaje de precisión de la clase a predecir | |

## Anexo 2. Instrumento de recolección de información

**FACULTAD DE INGENIERÍA**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

***"Ficha de Evaluación"***

**Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna – Tacna 2020**

*Por favor, marque el número de la respuesta que le parezca más apropiada.*

## CONTROL DE ACCESO

### ➢ Identificación

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| **1.** El identificador proporcionado presenta una estructura compleja. | 1 | 2 | 3 | 4 | 5 |
| **2.** El personal utiliza el identificador para autenticarse. | 1 | 2 | 3 | 4 | 5 |
| **3.** El personal se siente cómodo y conforme al usar el identificador. | 1 | 2 | 3 | 4 | 5 |

***N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre**

***Enunciados Directos: 1,2,3**

### ➢ Autenticación

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| **4.** El tiempo que ocupa el proceso de autenticación del personal es rápido. | 1 | 2 | 3 | 4 | 5 |
| **5.** El personal es autenticado correctamente. | 1 | 2 | 3 | 4 | 5 |
| **6.** Existen falsos positivos en la autenticación del personal. | 5 | 4 | 3 | 2 | 1 |

***N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre**

***Enunciados Directos: 4,5 *Enunciados Indirectos: 6**

### ➢ Autorización

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| **7.** Los permisos del personal son otorgados correctamente. | 1 | 2 | 3 | 4 | 5 |
| **8.** El personal confía en la otorgación correcta de los permisos. | 1 | 2 | 3 | 4 | 5 |
| **9.** Existen accesos erróneos otorgados al personal. | 5 | 4 | 3 | 2 | 1 |

***N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre**

***Enunciados Directos: 7,8 *Enunciados Indirectos: 9**

### ➢ Trazabilidad

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| **10.** Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | 1 | 2 | 3 | 4 | 5 |
| **11.** Los registros de intentos de ingreso por personal no autorizado son registrados. | 1 | 2 | 3 | 4 | 5 |
| **12.** Los registros de accesos garantizados al personal son registrados. | 1 | 2 | 3 | 4 | 5 |

***N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre**

***Enunciados Directos: 10,11,12**

| DICCIONARIO DE CONCEPTOS | |
|---|---|
| Identificador | Todo recurso que tiene, conoce, o es parte de la persona para obtener el respectivo acceso al área.<br>• Algo que tiene: Tarjeta RFID, credencial, llave, etc.<br>• Algo que sabe: Contraseña, PIN, clave, etc.<br>• Algo que posee: Huella dactilar, iris, rostro, etc. |
| Identificación | Proceso donde la persona utiliza el identificador para presentarse ante el equipo o método de control de acceso (lector RFID, lector de código PIN, lector facial, lector de huella dactilar, etc.). |
| Autenticación | Proceso donde el equipo o método de control de acceso autentica la identidad de la persona según su identificación presentada. |
| Falso Positivo | Proceso donde el personal no identificado (fraudulento) es autenticado por resultado de alguna falla en el equipo o herramienta de control de acceso, suplantando la identidad de otra persona. |
| Autorización | Proceso donde, en base a la autenticación de la persona, se otorgan los accesos respectivos. |
| Trazabilidad | Proceso donde se registra la bitácora de todas las acciones dadas durante el control de acceso (registro de accesos denegados, concedidos, etc. Tales registros pueden ser visualizados en reportes, logs, historiales). |

- *¿Alguna vez ha escuchado sobre métodos de reconocimiento donde se utilice el iris humano para el control de acceso?*

  No…… 1 Sí……. 2

- *El Sistema de Reconocimiento de Iris es de utilidad y mejora el nivel de seguridad para el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna.*

  No…… 1 Sí……. 2

---

*¡Gracias por responder!*

*El autor del presente instrumento agradece su participación y colaboración.*

*……... de 2022*

# Anexo 3. Instrumento de recolección de información validado por expertos

*Experto 1*

| **Título del Proyecto** | **Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna - Tacna 2020.** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Objetivo** | **Determinar el nivel de seguridad para el proceso de identificación humana en el control de acceso al área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020.** | | | | | | | | | | | | | | | | | | | |
| **Variable** | **Dimensión** | **Indicador** | **Ítems (Ficha de Evaluación)** | **Opinión de las Respuestas** | | | | | **Criterios de Evaluación** | | | | | | | | | | | **Observación y/o recomendaciones** |
| | | | | **Muy en desacuerdo** | **Algo en desacuerdo** | **Ni acuerdo ni en desacuerdo** | **Algo de acuerdo** | **Muy de acuerdo** | **Relación entre la variable y la dimensión** | | **Relación entre la dimensión y el indicador** | | **Relación entre el indicador y el ítem** | | **Relación entre el ítem y la opción de respuesta** | | **La redacción es clara, precisa y comprensible** | | | |
| | | | | | | | | | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | | |
| **Variable Dependiente:** Identificación Humana para el Control de Acceso | Identificación | Nivel de complejidad en la estructuración del identificador | El identificador proporcionado presenta una estructura compleja. | | | | | | X | | X | | X | | X | | X | | Ninguno | |
| | | % de frecuencia del uso del identificador | El personal utiliza el identificador para autenticarse. | | | | | | X | | X | | X | | X | | X | | | |
| | | % de aceptabilidad del uso del identificador | El personal se siente cómodo y conforme al usar el identificador. | | | | | | X | | X | | X | | X | | X | | | |
| | Autenticación | Tiempo de demora en el proceso de autenticación | El tiempo que ocupa el proceso de autenticación del personal es rápido. | | | | | | X | | X | | X | | X | | X | | Ninguno | |
| | | % de acierto en la autenticación | El personal es autenticado correctamente. | | | | | | X | | X | | X | | X | | X | | | |
| | | % de aceptación falsa | Existen falsos positivos en la autenticación del personal. | | | | | | X | | X | | X | | X | | X | | | |
| | Autorización | % de acierto en la otorgación de permisos para el acceso al área requerida | Los permisos del personal son otorgados correctamente. | | | | | | X | | X | | X | | X | | X | | Ninguno | |
| | | Nivel de confiabilidad en la | El personal confía en la otorgación correcta de los permisos. | | | | | | X | | X | | X | | X | | X | | | |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | otorgación de permisos | | | | | | | | | | | | | | | | | |
| | | % de accesos erróneos otorgados | Existen accesos erróneos otorgados al personal. | | | | | | X | | X | | X | | X | | X | | |
| | Trazabilidad | Bitácora de acciones/eventos en los procesos | Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | | | | | | X | | X | | X | | X | | X | | Los enunciados asociados a registros en cada ítem deben ser más consistentes. |
| | | Bitácora de intentos de ingreso por personal no autorizado | Los registros de intentos de ingreso por personal no autorizado son registrados. | | | | | | X | | X | | X | | X | | X | | |
| | | Bitácora de accesos garantizados al personal | Los registros de accesos garantizados al personal son registrados. | | | | | | X | | X | | X | | X | | X | | |

Ing. Jimmy Cristian Muñoz Miranda
Ingeniería en Informática y Sistemas
CIP: 159469

DOCENTE UNIVERSITARIO
E.P. INGENIERÍA EN INFORMÁTICA Y SISTEMAS
UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN

*Experto 2*

| **Título del Proyecto** | **Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna - Tacna 2020.** | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Objetivo** | **Determinar el nivel de seguridad para el proceso de identificación humana en el control de acceso al área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020.** | | | | | | | | | | | | | | | | | | |
| **Variable** | **Dimensión** | **Indicador** | **Ítems (Ficha de Evaluación)** | **Opinión de las Respuestas** | | | | | **Criterios de Evaluación** | | | | | | | | | | **Observación y/o recomendaciones** |
| | | | | **Muy en desacuerdo** | **Algo en desacuerdo** | **Ni acuerdo ni en desacuerdo** | **Algo de acuerdo** | **Muy de acuerdo** | **Relación entre la variable y la dimensión** | | **Relación entre la dimensión y el indicador** | | **Relación entre el indicador y el ítem** | | **Relación entre el ítem y la opción de respuesta** | | **La redacción es clara, precisa y comprensible** | | |
| | | | | | | | | | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | **SI** | **NO** | |
| **Variable Dependiente:** Identificación Humana para el Control de Acceso | Identificación | Nivel de complejidad en la estructuración del identificador | El identificador proporcionado presenta una estructura compleja. | | | | | | X | | X | | X | | X | | X | | |
| | | % de frecuencia del uso del identificador | El personal utiliza el identificador para autenticarse. | | | | | | X | | X | | X | | X | | X | | |
| | | % de aceptabilidad del uso del identificador | El personal se siente cómodo y conforme al usar el identificador. | | | | | | X | | X | | X | | X | | X | | |
| | Autenticación | Tiempo de demora en el proceso de autenticación | El tiempo que ocupa el proceso de autenticación del personal es rápido. | | | | | | X | | X | | X | | X | | X | | |
| | | % de acierto en la autenticación | El personal es autenticado correctamente. | | | | | | X | | X | | X | | X | | X | | |
| | | % de aceptación falsa | Existen falsos positivos en la autenticación del personal. | | | | | | X | | X | | X | | X | | X | | |
| | Autorización | % de acierto en la otorgación de permisos para el acceso al área requerida | Los permisos del personal son otorgados correctamente. | | | | | | X | | X | | X | | X | | X | | |
| | | Nivel de confiabilidad en la | El personal confía en la otorgación correcta de los permisos. | | | | | | X | | X | | X | | X | | X | | |

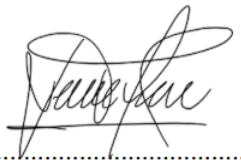
| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | otorgación de permisos | | | | | | | | | | | | | | | | | |
| | | % de accesos erróneos otorgados | Existen accesos erróneos otorgados al personal. | | | | | | X | | X | | X | | X | | X | | |
| | Trazabilidad | Bitácora de acciones/eventos en los procesos | Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | | | | | | X | | X | | X | | X | | X | | |
| | | Bitácora de intentos de ingreso por personal no autorizado | Los registros de intentos de ingreso por personal no autorizado son registrados. | | | | | | X | | X | | X | | X | | X | | |
| | | Bitácora de accesos garantizados al personal | Los registros de accesos garantizados al personal son registrados. | | | | | | X | | X | | X | | X | | X | | |

ing. Josué Gedeón Valdez Ramirez
CIP:169133

*Experto 3*

| Título del Proyecto | Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna - Tacna 2020. | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Objetivo | Determinar el nivel de seguridad para el proceso de identificación humana en el control de acceso al área de Tesorería del Gobierno Regional de Tacna con la implementación de un Sistema de Reconocimiento de Iris basado en Deep Learning – Tacna 2020. | | | | | | | | | | | | | | | | | | |
| Variable | Dimensión | Indicador | Ítems (Ficha de Evaluación) | Opinión de las Respuestas | | | | | Criterios de Evaluación | | | | | | | | | | Observación y/o recomendaciones |
| | | | | Muy en desacuerdo | Algo en desacuerdo | Ni acuerdo ni en desacuerdo | Algo de acuerdo | Muy de acuerdo | Relación entre la variable y la dimensión | | Relación entre la dimensión y el indicador | | Relación entre el indicador y el ítem | | Relación entre el ítem y la opción de respuesta | | La redacción es clara, precisa y comprensible | | |
| | | | | | | | | | SI | NO | SI | NO | SI | NO | SI | NO | SI | NO | |
| **Variable Dependiente:** Identificación Humana para el Control de Acceso | Identificación | Nivel de complejidad en la estructuración del identificador | El identificador proporcionado presenta una estructura compleja. | | | | | | X | | X | | X | | X | | X | | Ninguna |
| | | % de frecuencia del uso del identificador | El personal utiliza el identificador para autenticarse. | | | | | | X | | X | | X | | X | | X | | |
| | | % de aceptabilidad del uso del identificador | El personal se siente cómodo y conforme al usar el identificador. | | | | | | X | | X | | X | | X | | X | | |
| | Autenticación | Tiempo de demora en el proceso de autenticación | El tiempo que ocupa el proceso de autenticación del personal es rápido. | | | | | | X | | X | | X | | X | | X | | Ninguna |
| | | % de acierto en la autenticación | El personal es autenticado correctamente. | | | | | | X | | X | | X | | X | | X | | |
| | | % de aceptación falsa | Existen falsos positivos en la autenticación del personal. | | | | | | X | | X | | X | | X | | X | | |
| | Autorización | % de acierto en la otorgación de permisos para el acceso al área requerida | Los permisos del personal son otorgados correctamente. | | | | | | X | | X | | X | | X | | X | | Ninguna |
| | | Nivel de confiabilidad en la | El personal confía en la otorgación correcta de los permisos. | | | | | | X | | X | | X | | X | | X | | |

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | otorgación de permisos | | | | | | | | X | | X | | X | | X | | X | | |
| | | % de accesos erróneos otorgados | Existen accesos erróneos otorgados al personal. | | | | | | | X | | X | | X | | X | | X | | |
| | Trazabilidad | Bitácora de acciones/eventos en los procesos | Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | | | | | | | X | | X | | X | | X | | X | | Ninguna |
| | | Bitácora de intentos de ingreso por personal no autorizado | Los registros de intentos de ingreso por personal no autorizado son registrados. | | | | | | | X | | X | | X | | X | | X | | |
| | | Bitácora de accesos garantizados al personal | Los registros de accesos garantizados al personal son registrados. | | | | | | | X | | X | | X | | X | | X | | |



Ing. Enrique Waldo Condori Siles

Ingeniero en Informática y Sistemas

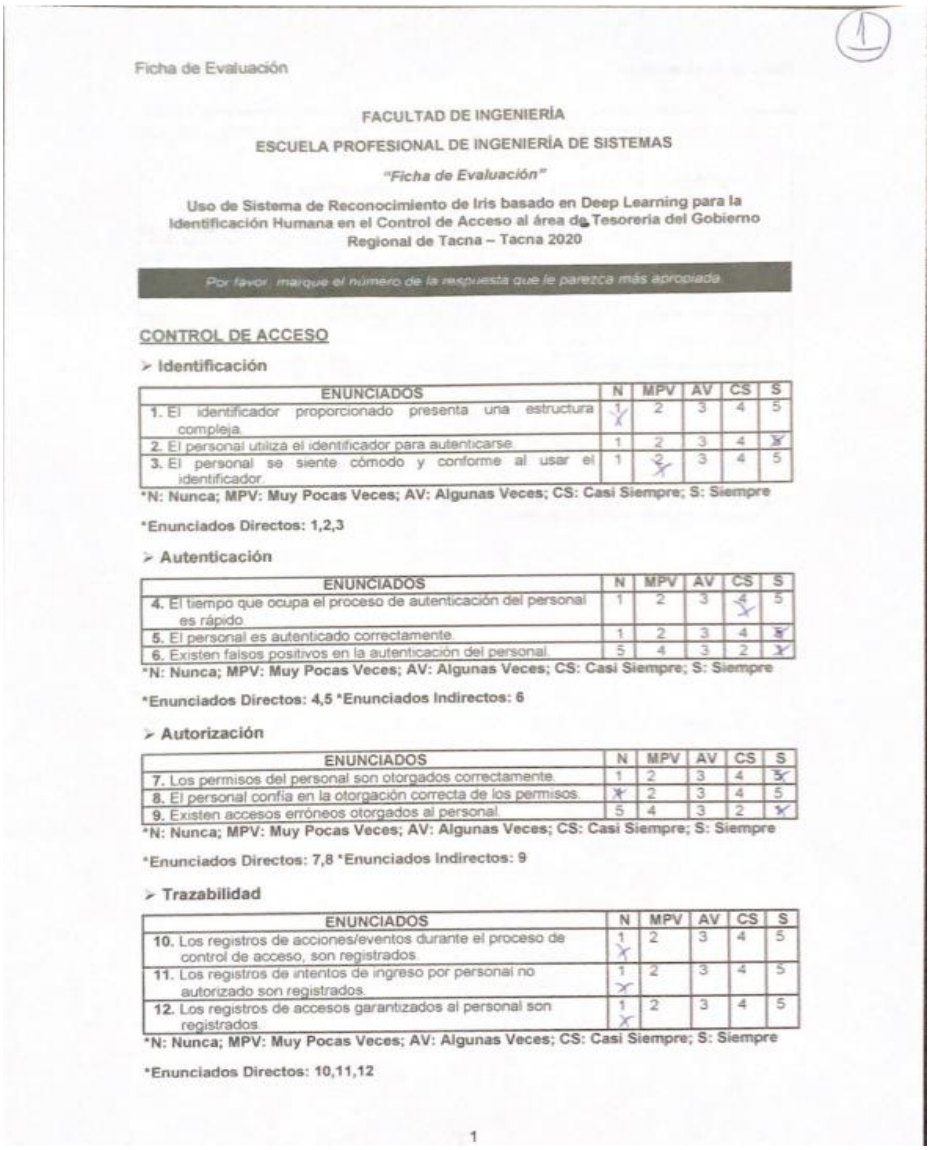
CIP. 229993

## Anexo 4. Aplicación del instrumento de recolección de información

### 1. Descripción

Se ha creado el siguiente repositorio GitHub: **https://github.com/LuisEdMB/SRICA**, directorio **2. Instrumentos**, donde se encuentran los instrumentos aplicados a los trabajadores del área de Tesorería del Gobierno Regional de Tacna.

- **Instrumento_Antes.pdf**, instrumentos “Ficha de Evaluación” ejecutados en el pre test de evaluación de la variable dependiente medible “Control de Acceso”.



Ficha de Evaluación

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

*"Ficha de Evaluación"*

**Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna – Tacna 2020**

*Por favor, marque el número de la respuesta que le parezca más apropiada*

CONTROL DE ACCESO

➢ **Identificación**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 1. El identificador proporcionado presenta una estructura compleja. | 1 | 2 | 3 | 4 | 5 |
| 2. El personal utiliza el identificador para autenticarse. | 1 | 2 | 3 | 4 | 5 |
| 3. El personal se siente cómodo y conforme al usar el identificador. | 1 | 2 | 3 | 4 | 5 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 1,2,3

➢ **Autenticación**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 4. El tiempo que ocupa el proceso de autenticación del personal es rápido. | 1 | 2 | 3 | 4 | 5 |
| 5. El personal es autenticado correctamente. | 1 | 2 | 3 | 4 | 5 |
| 6. Existen falsos positivos en la autenticación del personal. | 5 | 4 | 3 | 2 | 1 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 4,5 *Enunciados Indirectos: 6

➢ **Autorización**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 7. Los permisos del personal son otorgados correctamente. | 1 | 2 | 3 | 4 | 5 |
| 8. El personal confía en la otorgación correcta de los permisos. | 1 | 2 | 3 | 4 | 5 |
| 9. Existen accesos erróneos otorgados al personal. | 5 | 4 | 3 | 2 | 1 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 7,8 *Enunciados Indirectos: 9

➢ **Trazabilidad**

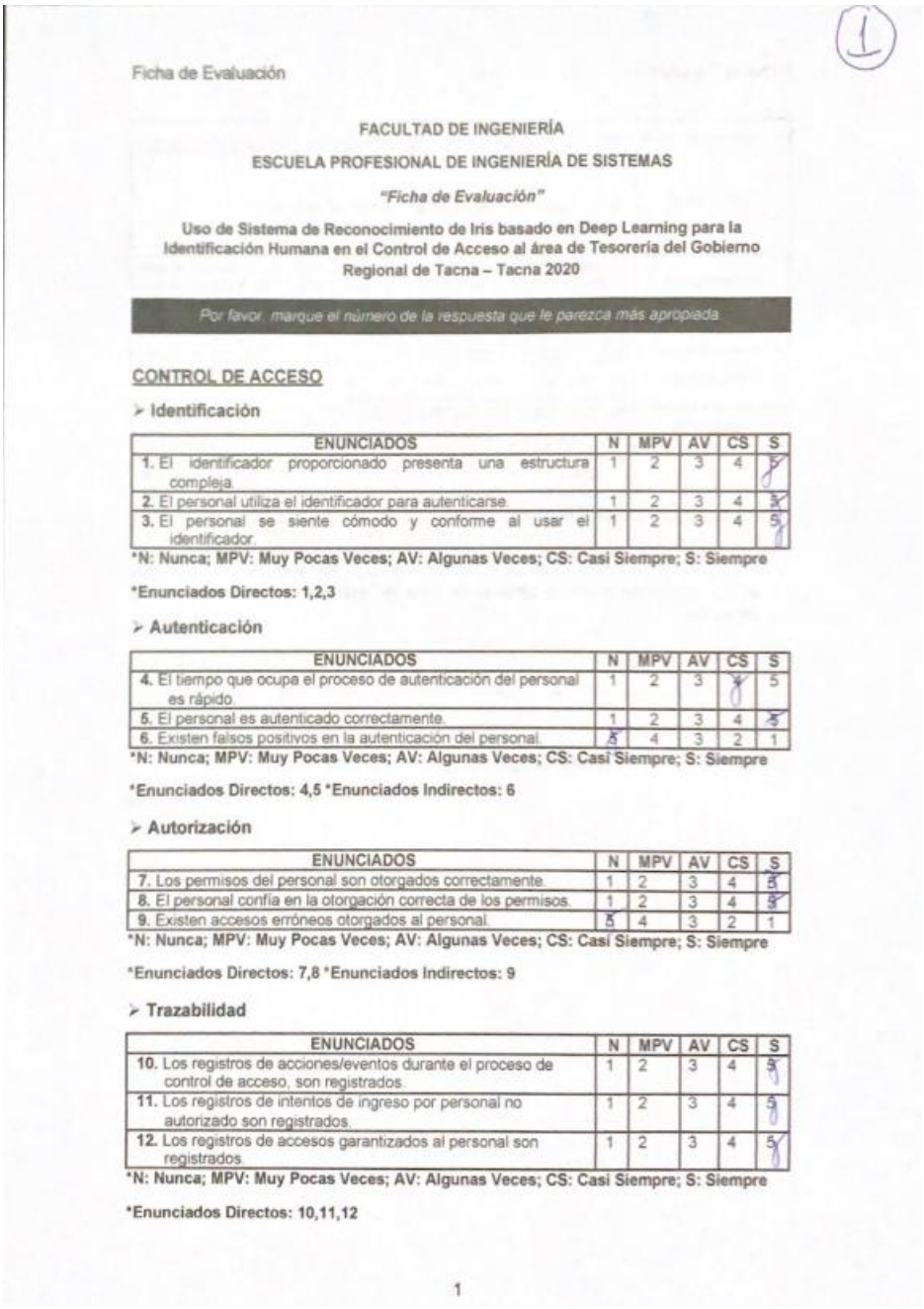
| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 10. Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | 1 | 2 | 3 | 4 | 5 |
| 11. Los registros de intentos de ingreso por personal no autorizado son registrados. | 1 | 2 | 3 | 4 | 5 |
| 12. Los registros de accesos garantizados al personal son registrados. | 1 | 2 | 3 | 4 | 5 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 10,11,12

1

- **Instrumento_Despues.pdf**, instrumentos “Ficha de Evaluación” ejecutados en el post test de evaluación de la variable dependiente medible “Control de Acceso”.



Ficha de Evaluación

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

*"Ficha de Evaluación"*

**Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la Identificación Humana en el Control de Acceso al área de Tesorería del Gobierno Regional de Tacna – Tacna 2020**

*Por favor, marque el número de la respuesta que le parezca más apropiada*

CONTROL DE ACCESO

➢ **Identificación**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 1. El identificador proporcionado presenta una estructura compleja. | 1 | 2 | 3 | 4 | 5 |
| 2. El personal utiliza el identificador para autenticarse. | 1 | 2 | 3 | 4 | 5 |
| 3. El personal se siente cómodo y conforme al usar el identificador. | 1 | 2 | 3 | 4 | 5 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 1,2,3

➢ **Autenticación**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 4. El tiempo que ocupa el proceso de autenticación del personal es rápido. | 1 | 2 | 3 | 4 | 5 |
| 5. El personal es autenticado correctamente. | 1 | 2 | 3 | 4 | 5 |
| 6. Existen falsos positivos en la autenticación del personal. | 5 | 4 | 3 | 2 | 1 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 4,5 *Enunciados Indirectos: 6

➢ **Autorización**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 7. Los permisos del personal son otorgados correctamente. | 1 | 2 | 3 | 4 | 5 |
| 8. El personal confía en la otorgación correcta de los permisos. | 1 | 2 | 3 | 4 | 5 |
| 9. Existen accesos erróneos otorgados al personal. | 5 | 4 | 3 | 2 | 1 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 7,8 *Enunciados Indirectos: 9

➢ **Trazabilidad**

| ENUNCIADOS | N | MPV | AV | CS | S |
|---|---|---|---|---|---|
| 10. Los registros de acciones/eventos durante el proceso de control de acceso, son registrados. | 1 | 2 | 3 | 4 | 5 |
| 11. Los registros de intentos de ingreso por personal no autorizado son registrados. | 1 | 2 | 3 | 4 | 5 |
| 12. Los registros de accesos garantizados al personal son registrados. | 1 | 2 | 3 | 4 | 5 |

*N: Nunca; MPV: Muy Pocas Veces; AV: Algunas Veces; CS: Casi Siempre; S: Siempre

*Enunciados Directos: 10,11,12

1

# Anexo 5. SRICA – Sistema de reconocimiento de iris

## 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, es el sistema desarrollado para lograr el objetivo de la presente investigación. Comprende de un sistema web que permite la gestión de registros que usa el proyecto, y la visualización de reportes. También, contiene múltiples servicios para lograr un buen funcionamiento del proceso, tomando en cuenta el enfoque de microservicios, para tener un sistema escalable. Del mismo modo, se ha construido un equipo biométrico lector de iris que controla el área protegida. Cada componente, software y hardware, están conectados entre sí, permitiendo un sistema robusto de reconocimiento de iris.

Para la realización de la estructura del proyecto, y de los cuales, en los siguientes puntos se mencionará de forma detallada, se ha creado el siguiente repositorio GitHub: **https://github.com/LuisEdMB/SRICA**. Cualquier investigador puede revisar y usar los elementos descritos en el repositorio, solo para fines de investigación.

## 2. Metodología de Gestión de Proyecto

SRICA sigue la metodología RUP para la gestión del proyecto, conteniendo las siguientes fases de desarrollo (cada elemento descrito en cada fase, contiene la nomenclatura de identificación según definida en el documento **SRICA_002_000 – Acta de Constitución del Proyecto**, y la numeración según el documento **SRICA_006_000 – EDT**, ambos pertenecientes a la fase de Inicio):

### 2.1. Inicio

En esta fase se establece el conocimiento, revisión del alcance, objetivos del proyecto, viabilidad, planes de gestión, y demás elementos que dan inicio al desarrollo del proyecto.

A continuación, se detallan los elementos que participan dentro de la fase de Inicio de la metodología RUP aplicada (para más detalles, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio**):

### 2.1.1. 1.1.2 SRICA_002_000 - Acta de Constitución del Proyecto

Este documento describe la finalidad, objetivos, alcance, y limitaciones del proyecto. También se describe la lista de requerimientos funcionales y no funcionales iniciales, metodología de proyecto a aplicar, elementos y fases de configuración, codificación de los elementos de configuración, cronograma, y financiamiento del proyecto.

Para visualizar el documento **1.1.2 SRICA_002_000 - Acta de Constitución del Proyecto**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.2 SRICA_002_000 - Acta de Constitución del Proyecto.docx**.

### 2.1.2. 1.1.3 SRICA_003_000 - Problemática Actual

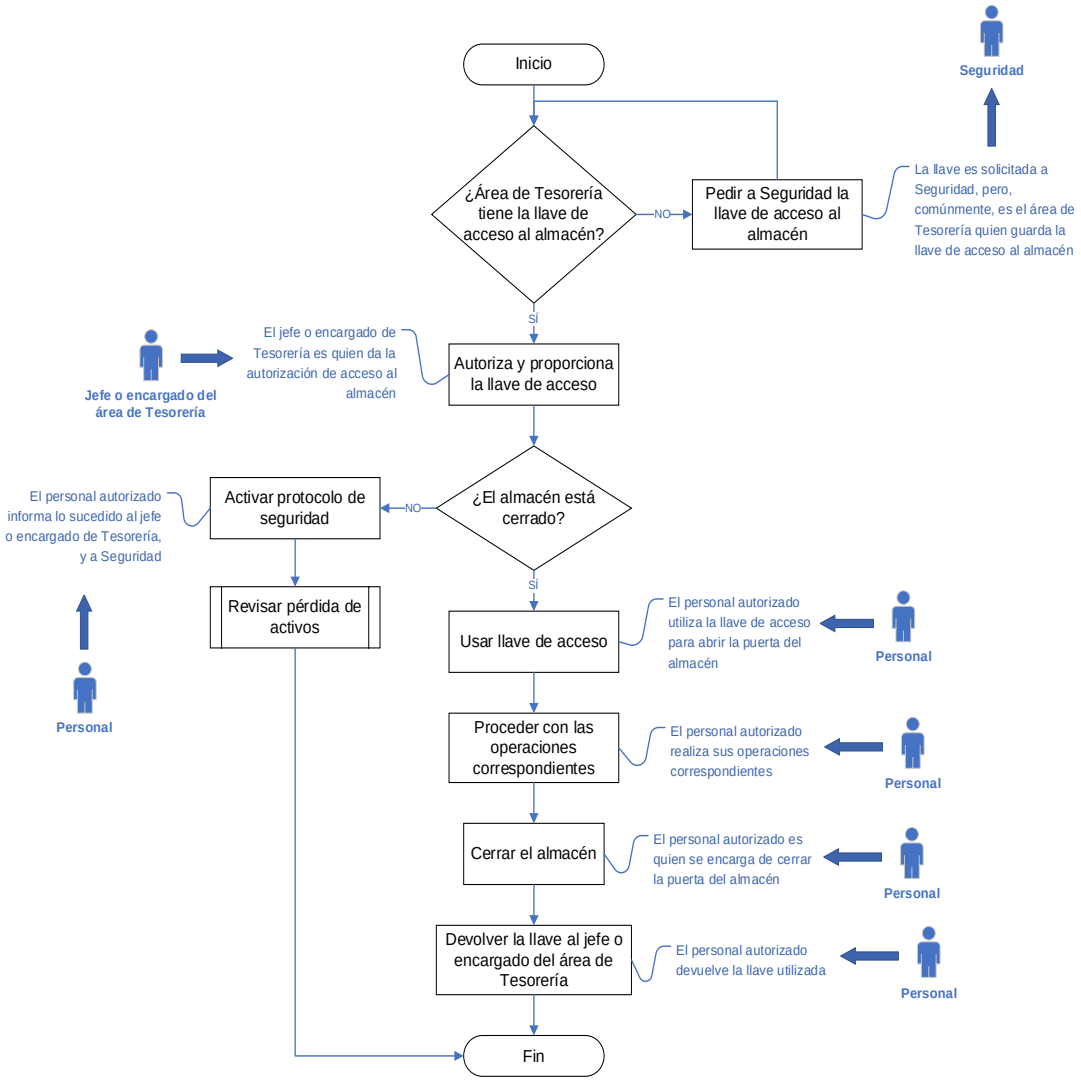
Este documento describe la problemática actual que existe en el almacén del área de Tesorería del Gobierno Regional de Tacna, y se visualiza el diagrama “Árbol de Problemas” que resume lo descrito en la descripción del problema.

Para visualizar el documento **1.1.3 SRICA_003_000 - Problemática Actual**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.3 SRICA_003_000 - Problemática Actual.docx**.

### 2.1.3. 1.1.4 SRICA_004_000 - Proceso Actual

Este documento describe el proceso actual de control de acceso que sigue el área de Tesorería del Gobierno Regional de Tacna para acceder a su almacén, mediante un diagrama de flujo.

*Proceso actual de control de acceso*

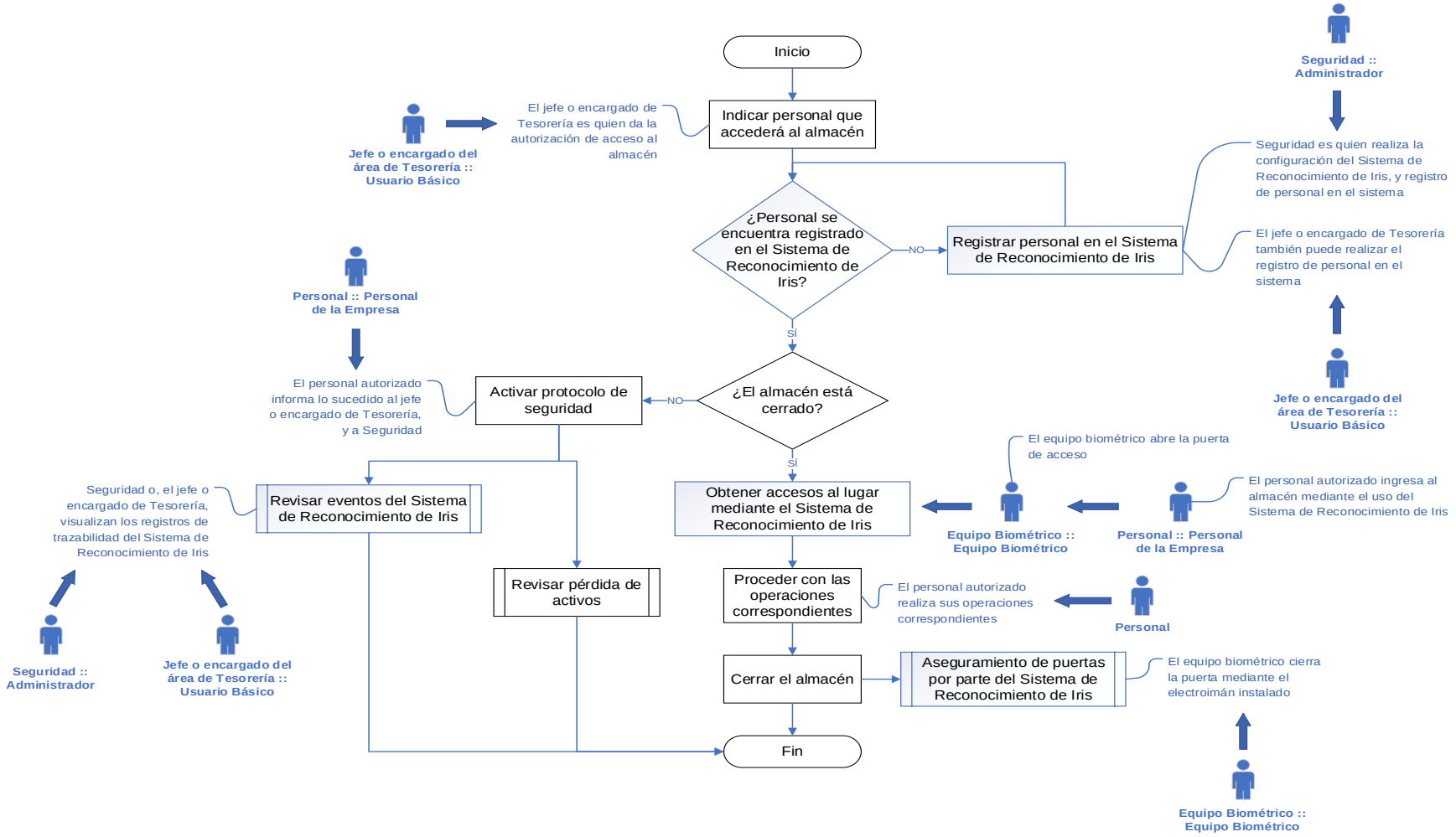



Para visualizar el documento **1.1.4 SRICA_004_000 - Proceso Actual**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.4 SRICA_004_000 - Proceso Actual.docx**.

### 2.1.4. 1.1.5 SRICA_005_000 - Proceso Propuesto

Este documento describe el proceso propuesto de control de acceso que seguirá el área de Tesorería del Gobierno Regional de Tacna para acceder a su almacén, debido al uso del Sistema de Reconocimiento de Iris “SRICA”, mediante un diagrama de flujo.

*Proceso propuesto de control de acceso*



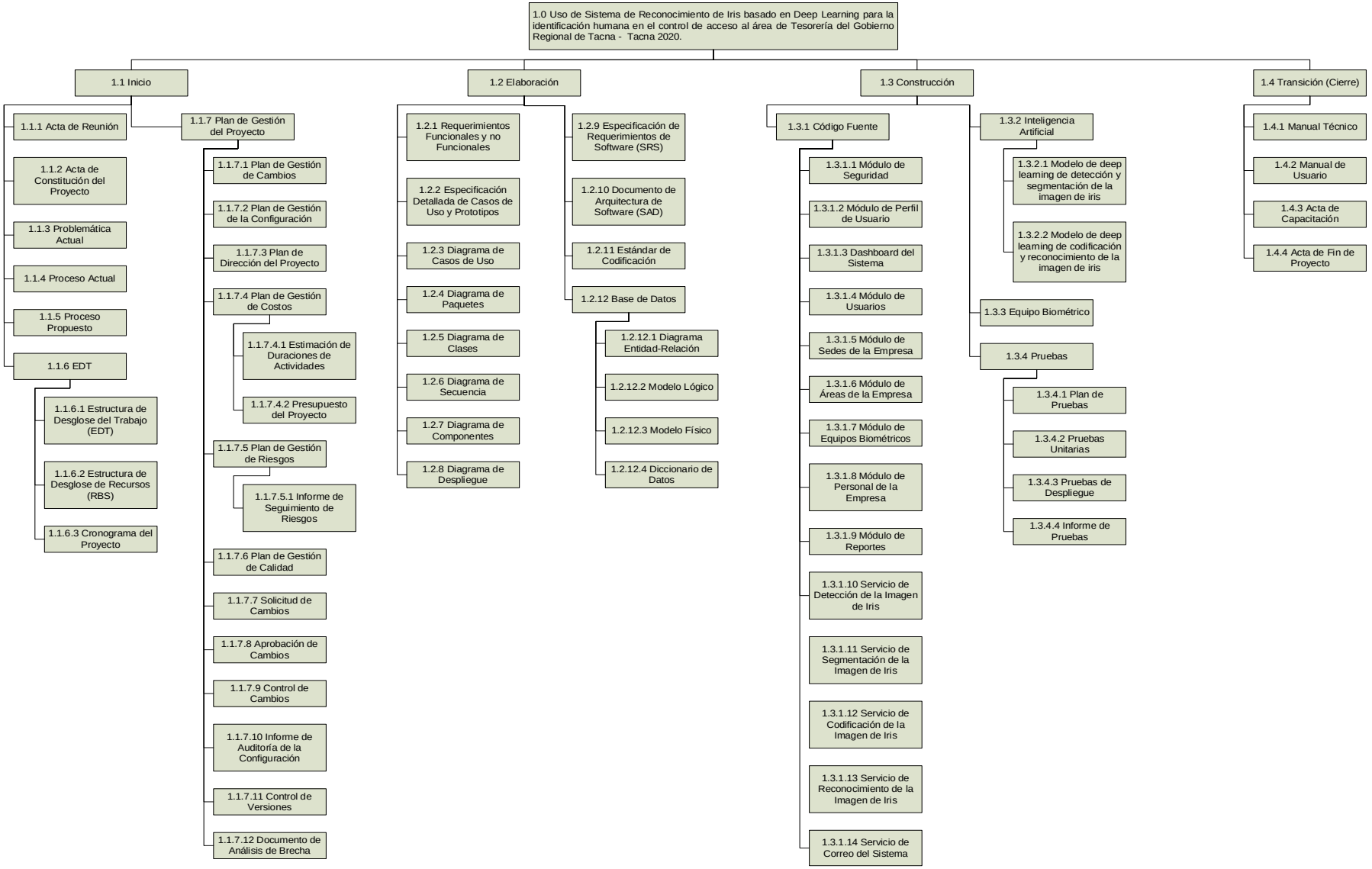
Para visualizar el documento **1.1.5 SRICA_005_000 - Proceso Propuesto**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.5 SRICA_005_000 - Proceso Propuesto.docx**.

### 2.1.5. Estructura de Desglose de Trabajo (EDT)

#### 2.1.5.1. 1.1.6.1 SRICA_006_000 – EDT

Este documento lista todos los paquetes de trabajo que contiene el proyecto, proporciona una descripción por cada elemento, y se visualiza el desglose de trabajo mediante un diagrama.

*Diagrama de estructura de desglose de trabajo*



Para visualizar el documento **1.1.6.1 SRICA_006_000 - EDT**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.6 EDT / 1.1.6.1 SRICA_006_000 - EDT.docx**.

#### 2.1.5.2. 1.1.6.2 SRICA_007_000 – RBS

Este documento lista todos los recursos humanos y equipos que son contemplados dentro del desarrollo del proyecto, proporciona una descripción por cada recurso, y se visualiza el desglose de recursos mediante un diagrama.

Para visualizar el documento **1.1.6.2 SRICA_007_000 - RBS**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.6 EDT / 1.1.6.2 SRICA_007_000 - RBS.docx**.

#### 2.1.5.3. 1.1.6.3 SRICA_008_000 - Cronograma del Proyecto

Este documento contempla el cronograma de desarrollo del proyecto, indicando la cantidad de horas por cada elemento de trabajo, y el rango de fechas que éstos contemplan.

Para visualizar el documento **1.1.6.3 SRICA_008_000 - Cronograma del Proyecto**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.6 EDT / 1.1.6.3 SRICA_008_000 - Cronograma del Proyecto.docx**.

### 2.1.6. Plan de Gestión

#### 2.1.6.1. 1.1.7.1 SRICA_009_000 - Plan de Gestión de Cambios

Este documento contempla la gestión de cambios que se debe seguir para realizar cambios en los elementos de trabajo del proyecto. Describe los roles, tipos de cambios, procedimientos, planes de contingencia, y herramientas de gestión de cambios.

Para visualizar el documento **1.1.7.1 SRICA_009_000 - Plan de Gestión de Cambios**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.1 SRICA_009_000 - Plan de Gestión de Cambios.docx**.

#### 2.1.6.2. 1.1.7.2 SRICA_010_000 - Plan de Gestión de la Configuración

Este documento contempla la gestión de la configuración, donde se detallan los roles, herramientas, elementos de configuración, plan de gestión de cambios, auditorías, y procedimientos de mantenimiento del plan de gestión de la configuración.

Para visualizar el documento **1.1.7.2 SRICA_010_000 - Plan de Gestión de la Configuración**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.2 SRICA_010_000 - Plan de Gestión de la Configuración.docx**.

#### 2.1.6.3. 1.1.7.3 SRICA_011_000 - Plan de Dirección del Proyecto

Este documento describe el ciclo de vida del proyecto, mediante las cuatro fases de la metodología RUP, y los elementos que pertenecen a cada fase. Se detalla el enfoque de trabajo, revisiones de gestión, y los documentos que contemplan el plan de dirección de proyectos.

Para visualizar el documento **1.1.7.3 SRICA_011_000 - Plan de Dirección del Proyecto**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.3 SRICA_011_000 - Plan de Dirección del Proyecto.docx**.

#### 2.1.6.4. 1.1.7.4 SRICA_012_000 - Plan de Gestión de Costos

Este documento contempla el plan de gestión de costos, donde se describen las unidades de medida por cada tipo de recurso, nivel de precisión de costos por recurso, umbrales de control, métodos de medición de valor ganado, documentos pertenecientes al plan de gestión de costos, financiamiento, y fluctuaciones de tipos de cambios.

Para visualizar el documento **1.1.7.4 SRICA_012_000 - Plan de Gestión de Costos**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.4 SRICA_012_000 - Plan de Gestión de Costos.docx**.

##### 2.1.6.4.1. 1.1.7.4.1 SRICA_012_001 - Estimación de Duraciones de Actividades

Este documento lista los elementos de trabajo, según EDT, por cada fase del RUP, indicando el recurso encargado de realizar cada elemento, la cantidad de trabajo por hora / hombre, y la duración total en horas.

Para visualizar el documento **1.1.7.4.1 SRICA_012_001 - Estimación de Duraciones de Actividades**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware/1.1 Inicio/1.1.7 Plan de Gestion/1.1.7.4.1 SRICA_012_001 - Estimación de Duraciones de Actividades.docx**.

#### 2.1.6.4.2. 1.1.7.4.2 SRICA_012_002 - Presupuesto del Proyecto

Este documento lista los elementos de trabajo, según EDT, por cada fase del RUP, indicando las horas de trabajo por cada elemento, el total de costo por hora de trabajo, y el presupuesto total del proyecto.

Para visualizar el documento **1.1.7.4.2 SRICA_012_002 - Presupuesto del Proyecto**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.4.2 SRICA_012_002 - Presupuesto del Proyecto.docx**.

### 2.1.6.5. 1.1.7.5 SRICA_013_000 - Plan de Gestión de Riesgos

Este documento contempla el plan de gestión de riegos, describiendo la metodología de gestión de riesgos a aplicar, roles y responsabilidades, periodicidad, y el listado de riegos iniciales identificados para el proyecto.

Para visualizar el documento **1.1.7.5 SRICA_013_000 - Plan de Gestión de Riesgos**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.5 SRICA_013_000 - Plan de Gestión de Riesgos.docx**.

#### 2.1.6.5.1. 1.1.7.5.1 SRICA_013_001 - Formato de Informe de Seguimiento de Riesgos

Este documento muestra el formato a utilizar para dar seguimiento a los riegos que puedan identificarse durante el proyecto.

Para visualizar el documento **1.1.7.5.1 SRICA_013_001 - Formato de Informe de Seguimiento de Riesgos**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.5.1 SRICA_013_001 - Formato de Informe de Seguimiento de Riesgos.docx**.

#### 2.1.6.6. 1.1.7.6 SRICA_014_000 - Plan de Gestión de Calidad

Este documento contempla el plan de gestión de calidad, describiendo los objetivos de calidad, factores críticos, roles y responsabilidades, políticas de calidad del proyecto, y listado de los elementos de trabajo que estarán en revisión de calidad, según EDT, por cada fase del RUP.

Para visualizar el documento **1.1.7.6 SRICA_014_000 - Plan de Gestión de Calidad**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.6 SRICA_014_000 - Plan de Gestión de Calidad.docx**.

#### 2.1.6.7. 1.1.7.7 SRICA_015_000 - Formato de Solicitud de Cambios

Este documento muestra el formato a utilizar para realizar una solicitud de cambios de algún elemento de configuración. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.7 SRICA_015_000 - Formato de Solicitud de Cambios**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.7 SRICA_015_000 - Formato de Solicitud de Cambios.docx**.

#### 2.1.6.8. 1.1.7.8 SRICA_016_000 - Formato de Aprobación de Cambios

Este documento muestra el formato a utilizar para realizar la aprobación de alguna solicitud de cambios de elementos de configuración. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.8 SRICA_016_000 - Formato de Aprobación de Cambios**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.8 SRICA_016_000 - Formato de Aprobación de Cambios.docx**.

#### 2.1.6.9. 1.1.7.9 SRICA_017_000 - Formato de Control de Cambios

Este documento muestra el formato a utilizar para realizar el monitoreo de los cambios efectuados a elementos afectados. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.9 SRICA_017_000 - Formato de Control de Cambios**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.9 SRICA_017_000 - Formato de Control de Cambios.docx**.

#### 2.1.6.10. 1.1.7.10 SRICA_018_000 - Formato de Informe de Auditoría de la Configuración

Este documento muestra el formato a utilizar para realizar la respectiva evaluación y auditoría de los cambios realizados. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.10 SRICA_018_000 - Formato de Informe de Auditoría de la Configuración**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.10 SRICA_018_000 - Formato de Informe de Auditoría de la Configuración.docx**.

#### 2.1.6.11. 1.1.7.11 SRICA_019_000 - Formato de Control de Versiones

Este documento muestra el formato a utilizar para realizar el registro de las versiones correspondientes de los elementos de configuración afectados. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.11 SRICA_019_000 - Formato de Control de Versiones**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.11 SRICA_019_000 - Formato de Control de Versiones.docx**.

#### 2.1.6.12. 1.1.7.12 SRICA_020_000 - Formato de Documento de Análisis de Brecha

Este documento muestra el formato a utilizar para asegurar y registrar los cambios efectuados, y realizar la actualización de los documentos necesarios. El documento es referenciado en el documento **SRICA_009_000 - Plan de Gestión de Cambios**.

Para visualizar el documento **1.1.7.12 SRICA_020_000 - Formato de Documento de Análisis de Brecha**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.1 Inicio / 1.1.7 Plan de Gestion / 1.1.7.12 SRICA_020_000 - Formato de Documento de Análisis de Brecha.docx**.

## 2.2. Elaboración

En esta fase se establece el listado de requerimientos funcionales y no funcionales, especificación detallada de casos de uso y prototipos, diagrama de casos de uso, diagrama de paquetes, diagrama de clases, diagrama de secuencia, diagrama de componentes, diagrama de despliegue o arquitectura, documento SRS, documento SAD, estándar de codificación, y diagrama de base de datos, referentes al proyecto.

A continuación, se detallan los elementos que participan dentro de la fase de Elaboración de la metodología RUP aplicada (para más detalles, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración**):

### 2.2.1. 1.2.1 SRICA_021_000 - Requerimientos Funcionales y no Funcionales

Este documento contiene el listado y descripción (no a detalle) de los requerimientos funcionales y no funcionales, la asignación de actores o roles intervinientes en cada requerimiento, módulos y prioridad.

*Requerimientos funcionales y no funcionales del sistema*

<table>
<tr><td colspan="6">ACTORES DEL SISTEMA</td></tr>
<tr><td colspan="2">Actor</td><td colspan="4">Descripción</td></tr>
<tr><td colspan="2">Administrador</td><td colspan="4">Usuario con acceso a todo el sistema de reconocimiento de iris.<br>Este actor representa al personal de Seguridad.</td></tr>
<tr><td colspan="2">Usuario básico</td><td colspan="4">Usuario con accesos limitados en el sistema de reconocimiento de iris.<br>Este actor representa al jefe o encargado del área de Tesorería.</td></tr>
<tr><td colspan="2">Personal de la empresa</td><td colspan="4">Personal de la empresa que se identifica ante el equipo biométrico para poder acceder a un área de la empresa.<br>Este actor representa al personal que ha sido autorizado para ingresar al almacén del área de Tesorería.</td></tr>
<tr><td colspan="2">Equipo biométrico</td><td colspan="4">Equipo biométrico que permite el acceso a un área de la empresa.</td></tr>
<tr><td colspan="6">REQUERIMIENTOS FUNCIONALES</td></tr>
<tr><td>Código</td><td>Nombre</td><td>Descripción</td><td>Actor(es)</td><td>Módulo / Proceso / Servicio</td><td>Prioridad</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| RF01 | Iniciar sesión | El usuario administrador y/o usuario básico pueden ingresar al sistema mediante:<br>Usuario<br>Contraseña (se permite mostrar/ocultar la contraseña)<br>* Las acciones de iniciar sesión y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de seguridad | Medio |
| RF02 | Cerrar sesión | El usuario administrador y/o usuario básico pueden salir del sistema.<br>* Las acciones de cerrar sesión y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de seguridad | Medio |
| RF03 | Recuperar contraseña | El usuario administrador puede recuperar su contraseña mediante el uso del correo registrado / modificado en RF08, o el correo modificado en RF06.<br>El usuario administrador, dentro de la interfaz de inicio de sesión (RF01), ingresa su usuario para recuperar su contraseña.<br>Cuando el administrador requiere recuperar su contraseña, se procesa el RF28.<br>* Las acciones de recuperar contraseña y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador | Módulo de seguridad | Medio |
| RF04 | Cambiar contraseña olvidada | El usuario administrador, después de terminar el proceso de RF03 y RF28, puede ingresar una nueva contraseña en los campos:<br>Nueva contraseña (se permite mostrar/ocultar la contraseña; nivel de fortaleza Medio-Alto o Alto)<br>Confirmar nueva contraseña (se permite mostrar/ocultar la contraseña)<br>El sistema redirige al usuario a la interfaz de inicio de sesión (RF01) para que pueda iniciar sesión en el sistema. | Administrador | Módulo de seguridad | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | El usuario solo tiene 2 minutos para que pueda cambiar su contraseña. Si el usuario no realiza alguna acción, el usuario tendrá que realizar otra vez el proceso de RF03.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de cambiar contraseña olvidada y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF05 | Cambiar contraseña y correo electrónico por defecto | Cuando el usuario administrador y/o usuario básico ingresan por primera vez al sistema, o si la contraseña ha sido modificada al valor por defecto en RF08, son obligados a cambiar su contraseña y/o correo electrónico por defecto mediante los campos:<br>Correo electrónico (visible si es necesario cambiar el valor por defecto)<br>Nueva contraseña (se permite mostrar/ocultar la contraseña; nivel de fortaleza Medio-Alto o Alto)<br>Confirmar nueva contraseña (se permite mostrar/ocultar la contraseña)<br>El sistema espera 2 minutos al usuario para que éste pueda cambiar sus datos por defecto. Si el usuario no realiza alguna acción, el usuario tendrá que realizar otra vez el proceso de RF01.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* La acciones de cambiar los datos por defecto y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de seguridad | Bajo |
| RF06 | Gestionar perfil de usuario | El usuario administrador y/o usuario básico pueden gestionar su perfil de usuario, donde se muestran los campos: | Administrador, usuario básico | Módulo de perfil de usuario | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| | | Usuario (solo lectura)<br>Nombres y apellidos (solo lectura)<br>Correo electrónico<br>Contraseña (no se visualiza la contraseña del usuario; si no se desea modificar la contraseña, se deja el campo vacío; se permite mostrar/ocultar la contraseña; nivel de fortaleza Medio-Alto o Alto)<br>Confirmar contraseña (se permite mostrar/ocultar la contraseña)<br>Rol del usuario (solo lectura)<br>Últimas 5 fechas de sesión iniciada en el sistema (solo lectura)<br>Los campos que el usuario puede modificar son: correo electrónico, contraseña. Cuando el usuario modifica su contraseña, es redirigido a RF01.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, modificación y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF07 | Visualizar dashboard del sistema | El usuario administrador y/o usuario básico pueden visualizar el dashboard (pantalla de inicio) del sistema. El dashboard presenta la siguiente información:<br>Cantidad de trabajadores registrados.<br>Cantidad de equipos biométricos registrados por sede (de mayor a menor).<br>Gráfico de barra de accesos concedidos, denegados y errores por sede y área (se selecciona una sede y una o varias áreas).<br>Gráfico circular del top 10 de los trabajadores con más accesos en cualquier sede y área, de los últimos 6 meses. Si el usuario hace clic | Administrador, usuario básico | Dashboard del sistema | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| | | sobre el trabajador, se visualiza el top 10 de sedes – áreas accedidas por el trabajador y la cantidad de accesos en los últimos 6 meses.<br>Gráfico circular del top 10 de las áreas de cualquier sede más accedidas por los trabajadores, de los últimos 6 meses. Si el usuario hace clic sobre el área, se visualiza el top 10 de trabajadores que más accedieron a tal área en los últimos 6 meses.<br>Los registros y listados de la información presentada en el dashboard, todos son mostrados en estado activo.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF08 | Gestionar usuario del sistema | El usuario administrador puede gestionar los usuarios que ingresarán al sistema.<br>Las opciones disponibles son:<br>Registrar un nuevo usuario: El administrador puede registrar un nuevo usuario en base a los siguientes campos:<br>Usuario (representado por el DNI; único)<br>Contraseña (campo oculto)<br>Nombres<br>Apellidos<br>Rol (seleccionar rol: administrador, usuario básico; roles en estado activo)<br>Correo electrónico (campo oculto)<br>La contraseña generada por defecto es: 123.-SRICa. El correo generado por defecto es: srica@cambiarcorreo.com. | Administrador | Módulo de usuarios | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Modificar usuario existente: El administrador puede modificar los datos de un usuario existente. Los campos son:<br>Usuario (representado por el DNI; único)<br>Contraseña (si se desea modificar la contraseña, se genera la contraseña por defecto: 123.-SRICa)<br>Nombres<br>Apellidos<br>Rol (seleccionar rol: administrador, usuario básico; roles en estado activo)<br>Correo electrónico (campo deshabilitado; no modificable)<br>Inactivar usuario(s) existente(s): El administrador puede inactivar uno o varios usuarios existentes.<br>Activar usuario(s) existente(s): El administrador puede activar uno o varios usuarios existentes.<br>Listar usuarios: El administrador puede listar los usuarios registrados en el sistema. El administrador puede filtrar el listado de usuarios mediante los siguientes filtros: usuario, nombres, apellidos, rol (selección múltiple), estado del usuario (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones obtención de datos, registrar, modificar, activar, inactivar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF09 | Gestionar sede de la empresa | El usuario administrador puede gestionar las sedes de la empresa. Las opciones disponibles son:<br>Registrar una nueva sede: El administrador puede registrar una nueva sede de la empresa en base a los siguientes campos: | Administrador | Módulo de sedes de la empresa | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Sede<br>Modificar sede existente: El administrador puede modificar los datos de una sede existente. Los campos modificables son:<br>Sede<br>Inactivar sede(s) existente(s): El administrador puede inactivar una o varias sedes existentes. La inactivación de una sede no permitirá el flujo de acceso del personal asignado a un área de la sede. Así mismo, cualquier relación de información con alguna sede inactiva, serán inactivados.<br>Activar sede(s) existente(s): El administrador puede activar una o varias sedes existentes.<br>Listar sedes: El administrador puede listar las sedes registradas en el sistema. El administrador puede filtrar el listado de sedes mediante los siguientes filtros: sede, estado de la sede (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, registrar, modificar, activar, inactivar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF10 | Gestionar área de la empresa | El usuario administrador puede gestionar las áreas de la empresa.<br>Las opciones disponibles son:<br>Registrar una nueva área: El administrador puede registrar una nueva área de la empresa en base a los siguientes campos:<br>Área<br>Sede (seleccionar sede: sedes registradas en RF09, en estado activo) | Administrador | Módulo de áreas de la empresa | Medio |

| | | | | | |
|---|---|---|---|---|---|
| | | Modificar área existente: El administrador puede modificar los datos de un área existente. Los campos modificables son:<br>Área<br>Sede (seleccionar sede: sedes registradas en RF09, en estado activo)<br>Inactivar área(s) existente(s): El administrador puede inactivar una o varias áreas existentes. La inactivación de un área no permitirá el flujo de acceso del personal asignado al área. Así mismo, cualquier relación de información con algún área inactiva, serán inactivados.<br>Activar área(s) existente(s): El administrador puede activar una o varias áreas existentes.<br>Listar áreas: El administrador puede listar las áreas registradas en el sistema. El administrador puede filtrar el listado de áreas mediante los siguientes filtros: área, sede (en estado activo; selección múltiple; se permite listar registros donde la sede ha sido inactivada), estado del área (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, registrar, modificar, activar, inactivar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF11 | Gestionar nomenclatura para búsqueda de equipos biométricos | El usuario administrador puede gestionar la nomenclatura inicial del nombre de los equipos biométricos para su búsqueda en la red empresarial. La nomenclatura inicial de los equipos biométricos es: SRI.<br>Las opciones disponibles son: | Administrador | Módulo de equipos biométricos | Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | Registrar nueva nomenclatura: El administrador puede registrar una nueva nomenclatura en base a los siguientes campos:<br>Nomenclatura (3 letras en mayúscula; único)<br>Modificar nomenclatura existente: El administrador puede modificar los datos de una nomenclatura existente. Los campos modificables son:<br>Nomenclatura (3 letras en mayúscula; único)<br>Inactivar nomenclatura(s) existente: El administrador puede inactivar una o varias nomenclaturas existentes. Cualquier relación de información con alguna nomenclatura inactiva, serán inactivados.<br>Activar nomenclatura(s) existente: El administrador puede activar una o varias nomenclaturas existentes.<br>Listar nomenclatura: El administrador puede listar las nomenclaturas registradas en el sistema. El administrador puede filtrar el listado de nomenclaturas mediante los siguientes filtros: nomenclatura, estado de la nomenclatura (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, registrar, modificar, activar, inactivar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF12 | Gestionar equipo biométrico | El usuario administrador puede gestionar los equipos biométricos de reconocimiento de iris.<br>Las opciones disponibles son:<br>Registrar nuevo equipo biométrico: El administrador puede registrar un nuevo equipo biométrico presente en la red empresarial mediante una lista con los siguientes campos: nomenclatura (selección | Administrador | Módulo de equipos biométricos | Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | múltiple; estado activo), nombre de equipo, dirección de red. Los datos guardados son: nomenclatura, nombre de equipo, dirección de red (estático), dirección física (MAC). Estos datos son capturados automáticamente del equipo biométrico a registrar. Los equipos biométricos registrados en el sistema no son visualizados en el listado de equipos biométricos presentes en la red empresarial.<br>Modificar equipo biométrico existente: El administrador puede modificar los datos de un equipo biométrico existente. Los campos modificables son:<br>Nomenclatura (seleccionar nomenclatura: nomenclaturas registradas en RF11, en estado activo).<br>Nombre de equipo (único; formado por la nomenclatura seleccionada y demás nombre del equipo biométrico, ejemplo: SRI-Equipo-01)<br>Dirección de red (estático; único)<br>Sede (seleccionar sede: sedes registradas en RF09, en estado activo)<br>Área (en base a la sede seleccionada, se listan las áreas registradas en RF10, en estado activo)<br>Inactivar equipo(s) biométrico(s) existente: El administrador puede inactivar uno o varios equipos biométricos existentes.<br>Activar equipo(s) biométrico(s) existente: El administrador puede activar uno o varios equipos biométricos existentes.<br>Listar equipos biométricos: El administrador puede listar los equipos biométricos registrados en el sistema. El administrador puede filtrar el listado de equipos biométricos mediante los siguientes filtros: nomenclatura (en estado activo; selección múltiple; se permite listar registros donde la nomenclatura ha sido inactivada), nombre de equipo, dirección de red, sede (en estado activo; selección múltiple; | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | se permite listar registros donde la sede ha sido inactivada), área (en estado activo según sede(s) seleccionada(s); selección múltiple; se permite listar registros donde el área ha sido inactivada), estado del equipo biométrico (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, registrar, modificar, activar, inactivar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF13 | Manipular equipo biométrico | El usuario administrador y/o usuario básico pueden manipular los equipos biométricos registrados en el sistema.<br>Dentro de RF12, el usuario administrador y/o usuario básico (el usuario básico solo visualiza el listado de equipos biométricos registrados y la opción de abrir las puertas de acceso) pueden abrir las puertas de acceso desde el sistema (solo los equipos biométricos en estado activo): el sistema se conecta al equipo biométrico para enviar una señal (alarma) (opcional), para que el usuario pueda decidir abrir o no la puerta de acceso.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de abrir puerta de acceso y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de equipos biométricos | Medio |
| RF14 | Gestionar personal de la empresa | El usuario administrador y/o usuario básico pueden gestionar el personal que ingresará a las áreas de la empresa.<br>Las opciones disponibles son: | Administrador, usuario básico | Módulo de personal de la empresa | Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | Registrar nuevo personal: El administrador y/o usuario básico pueden registrar un nuevo personal en base a los siguientes campos:<br>Nombre<br>Apellido<br>DNI (único)<br>Sede (listado de sedes registradas en RF09, en estado activo)<br>Área (en base a las sedes, se listan las áreas para ser seleccionadas: áreas registradas en RF10, en estado activo)<br>Imagen de iris<br>Mediante el proceso de RF21, el administrador y/o usuario básico pueden capturar las imágenes de iris del nuevo personal a registrar. El total de imágenes es de 1 (uno por persona). Así mismo, el sistema guiará al personal durante el proceso de captura de las imágenes de iris.<br>Las imágenes de iris capturadas son procesadas por RF22 y RF23 (respectivamente), para su respectivo almacenamiento.<br>Importar personal a registrar desde Excel: El usuario administrador y/o usuario básico pueden importar un Excel para el registro masivo del personal. El formato obligatorio que debe tener el archivo Excel (de hasta 100mb) es: nombre, apellido, DNI. Los demás campos como: sede(s), área(s), imágenes de iris, serán llenados manualmente en el sistema mediante el proceso de modificación.<br>Modificar personal existente: El administrador y/o usuario básico pueden modificar los datos de un personal existente. Los campos modificables son:<br>Nombre<br>Apellido<br>DNI (único) | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Sede (listado de sedes registradas en RF09, en estado activo)<br>Área (en base a las sedes, se listan las áreas para ser seleccionadas: áreas registradas en RF10, en estado activo)<br>Imagen de iris (opcional)<br>El administrador y/o usuario básico pueden decidir o no capturar nuevas imágenes del iris para el personal existente. El proceso de captura de las imágenes de iris es el mismo descrito en “Registrar nuevo personal” (la nueva imagen reemplazará a la imagen actual guardada).<br>Verificar Reconocimiento de Iris: El administrador y/o usuario básico pueden verificar el iris capturado a la persona, y así validar si la imagen capturada ha sido correctamente procesada.<br>Inactivar personal existente: El administrador y/o usuario básico pueden inactivar uno o varios trabajadores existentes.<br>Activar personal existente: El administrador y/o usuario básico pueden activar uno o varios trabajadores existentes.<br>Listar personal: El administrador y/o usuario básico pueden listar al personal registrado mediante los siguientes filtros: nombre, apellidos, DNI, sede (con estado activo; selección múltiple; se permite listar registros donde la sede ha sido inactivada), área (con estado activo; selección múltiple; se permite listar registros donde el área ha sido inactivada), iris capturado (sí – no; selección múltiple), estado del personal (activo – inactivo).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado. | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | * Las acciones de obtención de datos, registrar, modificar, inactivar, activar y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF15 | Generar reporte del sistema | El usuario administrador y/o usuario básico pueden generar los reportes de equipos biométricos y personal de la empresa. Si el usuario selecciona el reporte de equipos biométricos, puede visualizar los campos/filtros: sede (sedes en estado activo; selección múltiple; se permite listar registros donde la sede ha sido inactivada), área (áreas en estado activo; según selección de la sede; selección múltiple; se permite listar registros donde el área ha sido inactivada), nomenclatura (nomenclaturas en estado activo; selección múltiple; se permite listar registros donde la nomenclatura ha sido inactivada), nombre de equipo, IP, estado de registro (activo – inactivo; selección múltiple). Si el usuario selecciona el reporte de personal de la empresa, puede visualizar los campos/filtros: sede (sedes en estado activo; selección múltiple; se permite listar registros donde la sede ha sido inactivada), área (áreas en estado activo; según selección de la sede; selección múltiple; se permite listar registros donde el área ha sido inactivada), DNI, nombres, apellidos, iris capturado (sí - no; selección múltiple), estado de registro (activo – inactivo; selección múltiple).<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, generación de reportes y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de reportes | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| RF16 | Exportar reporte del sistema | El usuario administrador y/o usuario básico pueden exportar el reporte generado en RF15. La extensión del archivo generado es: .html.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de exportación de reportes y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de reportes | Bajo |
| RF17 | Generar reporte de acciones del sistema | El usuario administrador puede generar el reporte de acciones del sistema (bitácora - trazabilidad). Los campos para el reporte son: usuario que realizó la acción, nombre y apellido del usuario, rol del usuario, módulo de la acción, recurso de la acción, tipo de evento (error, validación, correcto), acción, descripción del resultado de la acción, valor trazado (el valor anterior se compara con el valor actual para comprobar los valores cambiados), fecha de acción.<br>Las acciones pueden ser: obtención de datos, registro de datos, registro masivo de datos, modificación de datos, activación de registros, inactivación de registros, asignación de servidor de configuración, generación de reportes, exportación de reportes, recuperación de contraseña, cambio de contraseña olvidada, cambio de datos por defecto, acceso a equipos biométricos, apertura de puertas de acceso, acceso al sistema, sesión finalizada.<br>El usuario administrador genera el reporte según el rango de fechas de acción indicado (fecha de inicio – fecha fin).<br>El usuario administrador puede filtrar el listado de acciones del sistema (bitácora - trazabilidad) según los siguientes filtros: usuario que realizó la acción, nombre y apellido del usuario, rol del usuario (selección múltiple), módulo de acción (selección múltiple), recurso | Administrador | Módulo de reportes | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| | | de la acción (selección múltiple), tipo de evento (selección múltiple), acción (selección múltiple). El usuario administrador puede buscar las acciones de un usuario sin importar si a éste se le ha cambiado su usuario.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de generación de reportes y/o errores se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF18 | Exportar reporte de acciones del sistema | El usuario administrador puede exportar el reporte generado en RF17. La extensión del archivo generado es: .html.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de exportación de reportes y/o errores se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador | Módulo de reportes | Bajo |
| RF19 | Generar reporte de acciones de los equipos biométricos | El usuario administrador y/o usuario básico pueden generar el reporte de acciones de los equipos biométricos (bitácora – trazabilidad). Los campos para el reporte son: DNI, nombre del trabajador, sede de la empresa, área de la empresa, equipo biométrico, resultado del acceso (concedido, denegado, error, validación), descripción del resultado de acción, fecha de acceso, imagen del trabajador no registrado en el sistema que intentó ingresar al área.<br>El usuario administrador y/o usuario básico generan el reporte según el rango de fechas de acceso indicado (fecha de inicio – fecha fin).<br>El usuario administrador y/o usuario básico pueden filtrar el listado de acciones de los equipos biométricos (bitácora – trazabilidad) según los siguientes filtros: DNI, nombre del trabajador, sede de la empresa | Administrador, usuario básico | Módulo de reportes | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| | | (selección múltiple; listado según la bitácora guardada), área de la empresa (selección múltiple; listado según la bitácora guardada), equipo biométrico, resultado del acceso (selección múltiple). El usuario administrador y/o usuario básico pueden buscar los accesos de un trabajador sin importar si a éste se le ha cambiado su DNI.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de obtención de datos, generación de reportes y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | | | |
| RF20 | Exportar reporte de acciones de los equipos biométricos | El usuario administrador y/o usuario básico pueden exportar el reporte generado en RF19. La extensión del archivo generado es: .html.<br>Si el usuario es inhabilitado durante su estancia en el sistema, será redirigido al inicio de sesión sin poder ingresar al sistema, hasta que su usuario sea habilitado.<br>* Las acciones de exportación de reportes y errores, se guardan en la bitácora del sistema para que puedan ser visualizadas en RF17. | Administrador, usuario básico | Módulo de reportes | Bajo |
| RF21 | Procesar servicio de detección de la imagen de iris | Servicio de detección de las imágenes de iris de los trabajadores mediante modelo de inteligencia artificial (deep learning), usado por RF14 y RF25. | Administrador, usuario básico, equipo biométrico | Servicio de detección de la imagen de iris | Alto |
| RF22 | Procesar servicio de segmentación de la imagen de iris | Servicio de segmentación de las imágenes de iris de los trabajadores mediante modelo de inteligencia artificial (deep learning), usado por RF14 y RF26. | Administrador, usuario básico, equipo biométrico | Servicio de segmentación de la imagen de iris | Alto |
| RF23 | Procesar servicio de codificación de la imagen de iris | Servicio de codificación de las imágenes de iris de los trabajadores mediante el modelo de inteligencia artificial (deep learning), usado por RF14 y RF26 después de procesarse el RF22. | Administrador, usuario básico | Servicio de codificación de la imagen de iris | Alto |

| | | | | | |
|---|---|---|---|---|---|
| RF24 | Procesar servicio de reconocimiento de la imagen de iris | Servicio de reconocimiento de las imágenes de iris de los trabajadores mediante el modelo de inteligencia artificial (deep learning), usado por RF14 y RF26 después de procesarse el RF23. | Equipo biométrico | Servicio de reconocimiento de la imagen de iris | Alto |
| RF25 | Capturar imagen de iris desde el equipo biométrico | El personal de la empresa se identifica ante el equipo biométrico para el acceso a un área determinada. El equipo biométrico, mediante el proceso de RF21, reconoce el ojo del personal, cuando éste está a 5 cm – 8 cm del equipo biométrico. El equipo biométrico captura la imagen del iris del trabajador para ser procesadas en RF26.<br>Durante el proceso, el equipo biométrico emite señales (pitidos) y voces para indicar los procesos de: capturando imagen, procesando, error, acceso denegado, acceso concedido.<br>Por seguridad, se captura una foto del personal (usado por RF26) para el respectivo envío de correo cuando es un personal no registrado intentando ingresar a un área.<br>Las luces del equipo biométrico representan: rojo (error, validación – acceso denegado), en espera de reconocimiento (blanco), verde (éxito), en proceso (naranja).<br>* Los errores y validaciones durante el proceso de captura de la imagen de iris se guardan en la bitácora de equipos biométricos para que puedan ser visualizados en RF19. | Personal de la empresa, equipo biométrico | Equipo biométrico | Alto |
| RF26 | Procesar imagen de iris capturado por el equipo biométrico | El equipo biométrico, después de procesarse el RF25, empieza con el tratamiento de la imagen del iris capturado del trabajador para el acceso a un área determinada. Para ello, se usan los procesos (en orden): RF22, RF23 y RF24.<br>El equipo biométrico es verificado: equipo biométrico activo, sede y área activa.<br>La persona reconocida es verificada para obtener sus accesos mediante: persona activa, sede y área del trabajador igual a la sede | Equipo biométrico | Equipo biométrico | Alto |

| | | | | | |
|---|---|---|---|---|---|
| | | y área del equipo biométrico (donde la sede y área de la persona se encuentren en estado activo).<br>Así mismo, se procesa el servicio de RF27 cuando existen accesos denegados (envío de correos de alertas).<br>Durante el proceso, el equipo biométrico emite señales (pitidos) y voces para indicar los procesos de: capturando imagen, procesando, error, acceso denegado, acceso concedido.<br>Las luces del equipo biométrico representan: rojo (error, validación – acceso denegado), azul (ocupado), en espera de reconocimiento (blanco), verde (éxito), en proceso (naranja).<br>* El resultado de RF26: acceso concedido, acceso denegado, error, validaciones, se guardan en la bitácora de equipos biométricos para que puedan ser visualizados en RF19. | | | |
| RF27 | Procesar servicio de alerta de accesos denegados a las áreas de la empresa | El equipo biométrico, después de procesarse el RF26, y el resultado es acceso denegado, alerta a los usuarios del sistema mediante un correo. Si el acceso denegado es perteneciente a un personal no registrado en el sistema, se adjunta al correo la foto capturada por el equipo biométrico (foto tomada por RF25). | Equipo biométrico | Servicio de correo del sistema | Medio |
| RF28 | Procesar servicio de alerta para recuperación de contraseña de usuarios administradores | Después de procesarse el RF03 por el administrador, se procesa el servicio de alerta para recuperación de contraseña para usuarios administradores. El correo enviado al usuario administrador contiene la URL de redireccionamiento al sistema para realizar el proceso de RF04. | Administrador | Servicio de correo del sistema | Medio |

| REQUERIMIENTOS NO FUNCIONALES | | | |
|---|---|---|---|
| Código | Nombre | Descripción | Prioridad |

| | | | |
|---|---|---|---|
| RNF01 | Tiempo de respuesta | El sistema de reconocimiento de iris debe ser capaz de procesar las operaciones en un menor tiempo. Así mismo, el tiempo del proceso de identificación y autenticación del personal para el acceso a las áreas de la empresa, debe ser de 1~4 segundos. | Alta |
| RNF02 | Seguridad de acceso al sistema | El sistema de reconocimiento de iris debe ser capaz de controlar los accesos al sistema mediante usuarios, acceso y/o roles. | Alta |
| RNF03 | Interfaz | El sistema de reconocimiento de iris debe presentar una interfaz agradable e intuitiva. | Alta |
| RNF04 | Notificaciones | El sistema de reconocimiento de iris debe mostrar alertas cuando los procesos concluyen. | Alta |
| RNF05 | Captura de imágenes de iris | El sistema de reconocimiento de iris debe capturar la imagen de iris de forma rápida y con buena calidad de imagen. | Alta |
| RNF06 | Seguridad en la transferencia de la información | La información que es transferida entre el sistema web y los servicios, y durante el proceso de reconocimiento de iris mediante los equipos biométricos, debe ser cifrado y encriptado para mejorar el nivel de seguridad del sistema de reconocimiento de iris. | Alta |
| RNF07 | Enmascaramiento de información vital | La información del sistema de reconocimiento de iris que es almacenada en la base de datos, y que es considerada vital, debe estar encriptada. | Alta |
| RNF08 | Portabilidad | El sistema de reconocimiento de iris debe ser fácil de desplegar en cualquier ambiente tecnológico. | Alta |
| RNF09 | Operatividad | El sistema de reconocimiento de iris debe ser fácil de manipular. | Alta |
| RNF10 | Aprendizaje | El sistema de reconocimiento de iris debe ser fácil de aprender. | Alta |

Para visualizar el documento **1.2.1 SRICA_021_000 - Requerimientos Funcionales y no Funcionales**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.1 SRICA_021_000 - Requerimientos Funcionales y no Funcionales.docx**.

### 2.2.2. 1.2.2 SRICA_022_000 - Especificación Detallada de Casos de Uso y Prototipos

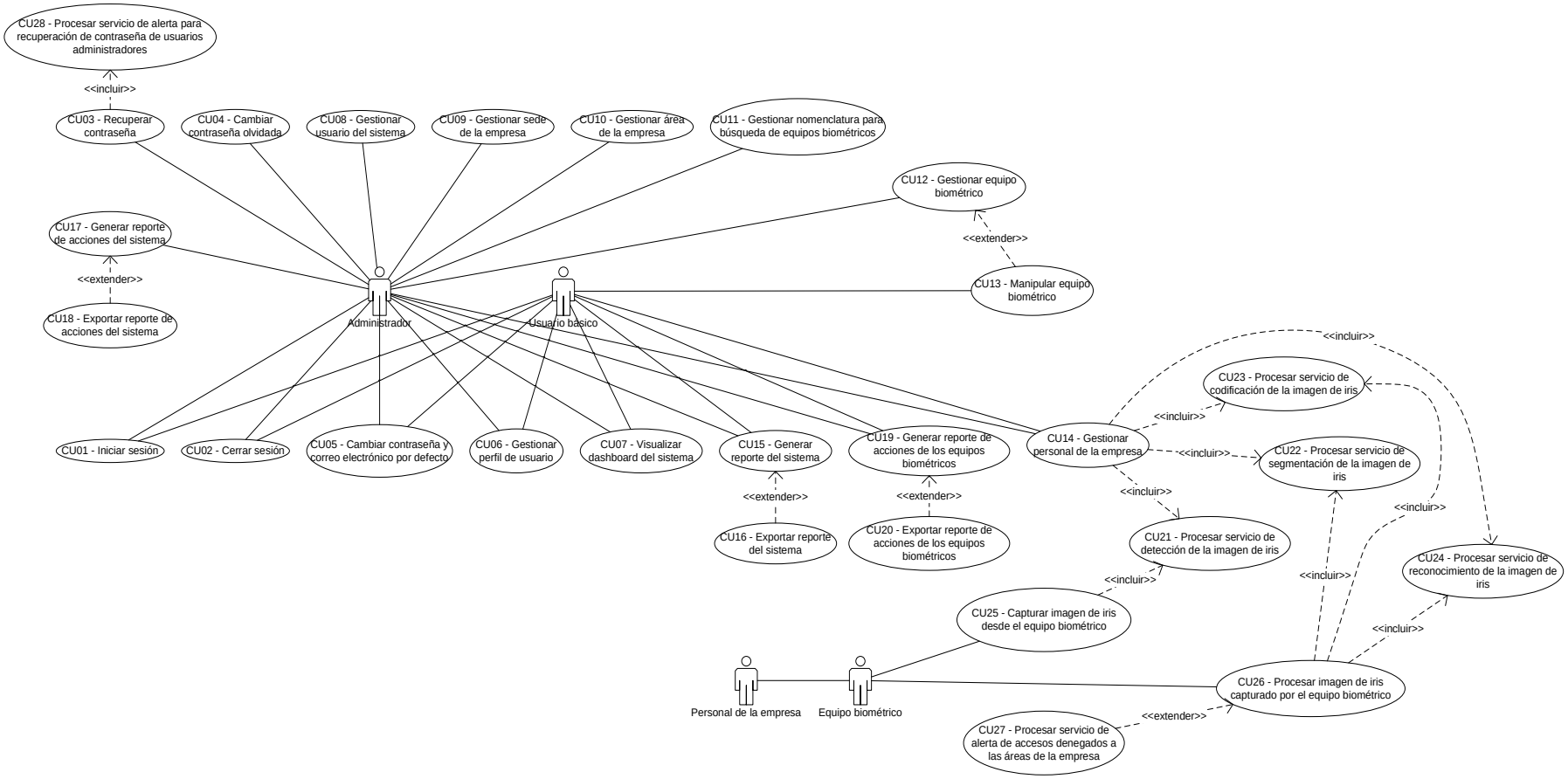
Este documento contiene la especificación detallada de los requerimientos funcionales del proyecto, consideraciones, restricciones, validaciones, reglas de negocio, y prototipos.

Para visualizar el documento **1.2.2 SRICA_022_000 - Especificación Detallada de Casos de Uso y Prototipos**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.2 SRICA_022_000 - Especificación Detallada de Casos de Uso y Prototipos.docx**.

### 2.2.3. 1.2.3 SRICA_023_000 - Diagrama de Casos de Uso

Este documento contiene los diagramas de casos de uso por requerimiento funcional del proyecto, y un diagrama de casos de uso general.

*Diagrama de casos de uso*

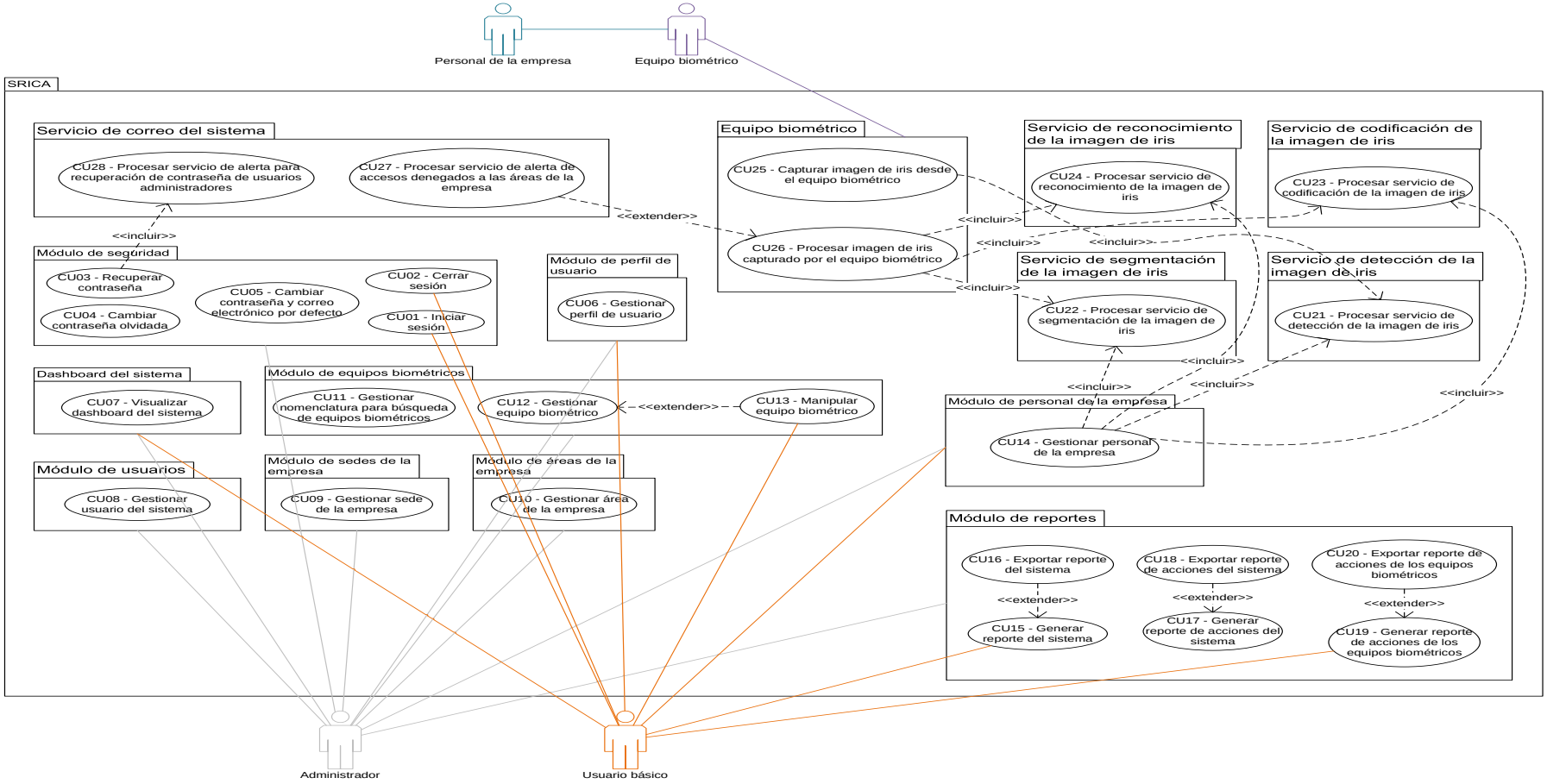



Para visualizar el documento **1.2.3 SRICA_023_000 - Diagrama de Casos de Uso**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.3 SRICA_023_000 - Diagrama de Casos de Uso.docx**.

### 2.2.4. 1.2.4 SRICA_024_000 - Diagrama de Paquetes

Este documento contiene los diagramas de paquetes que envuelven los casos de uso pertenecientes al sistema, y un diagrama de paquetes general.

*Diagrama de paquetes*



Para visualizar el documento **1.2.4 SRICA_024_000 - Diagrama de Paquetes**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.4 SRICA_024_000 - Diagrama de Paquetes.docx**.

### 2.2.5. 1.2.5 SRICA_025_000 - Diagrama de Clases

Este documento contiene los diagramas de clases del sistema.

Para visualizar el documento **1.2.5 SRICA_025_000 - Diagrama de Clases**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.5 SRICA_025_000 - Diagrama de Clases.docx**.

### 2.2.6. 1.2.6 SRICA_026_000 - Diagrama de Secuencia

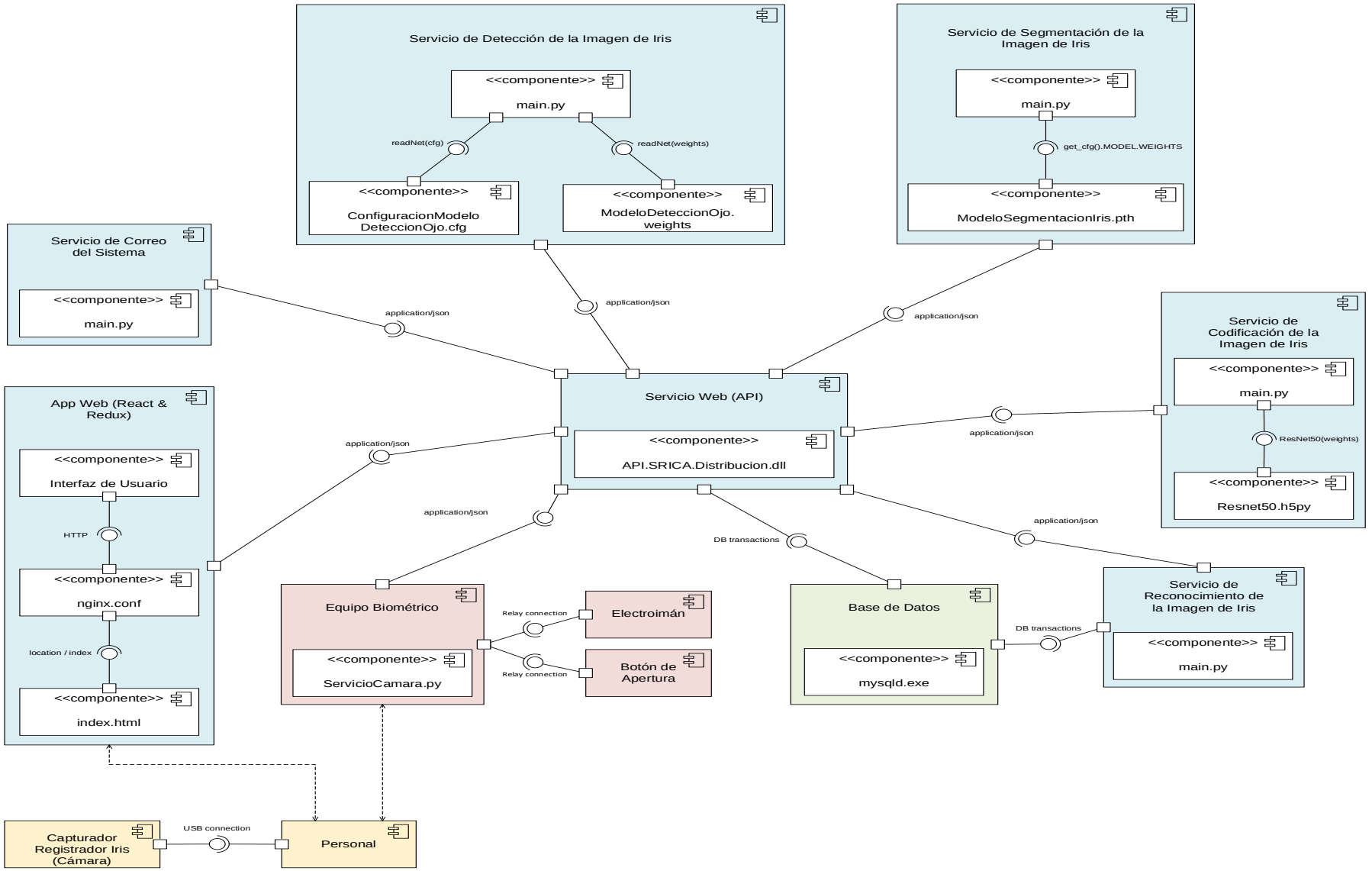
Este documento contiene los diagramas de secuencia de cada caso de uso del sistema.

Para visualizar el documento **1.2.6 SRICA_026_000 - Diagrama de Secuencia**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.6 SRICA_026_000 - Diagrama de Secuencia (Grafico).vsdx**.

### 2.2.7. 1.2.7 SRICA_027_000 - Diagrama de Componentes

Este documento contiene el diagrama de componentes para representar las conexiones y comunicaciones que existe entre cada componente del sistema.

*Diagrama de componentes*

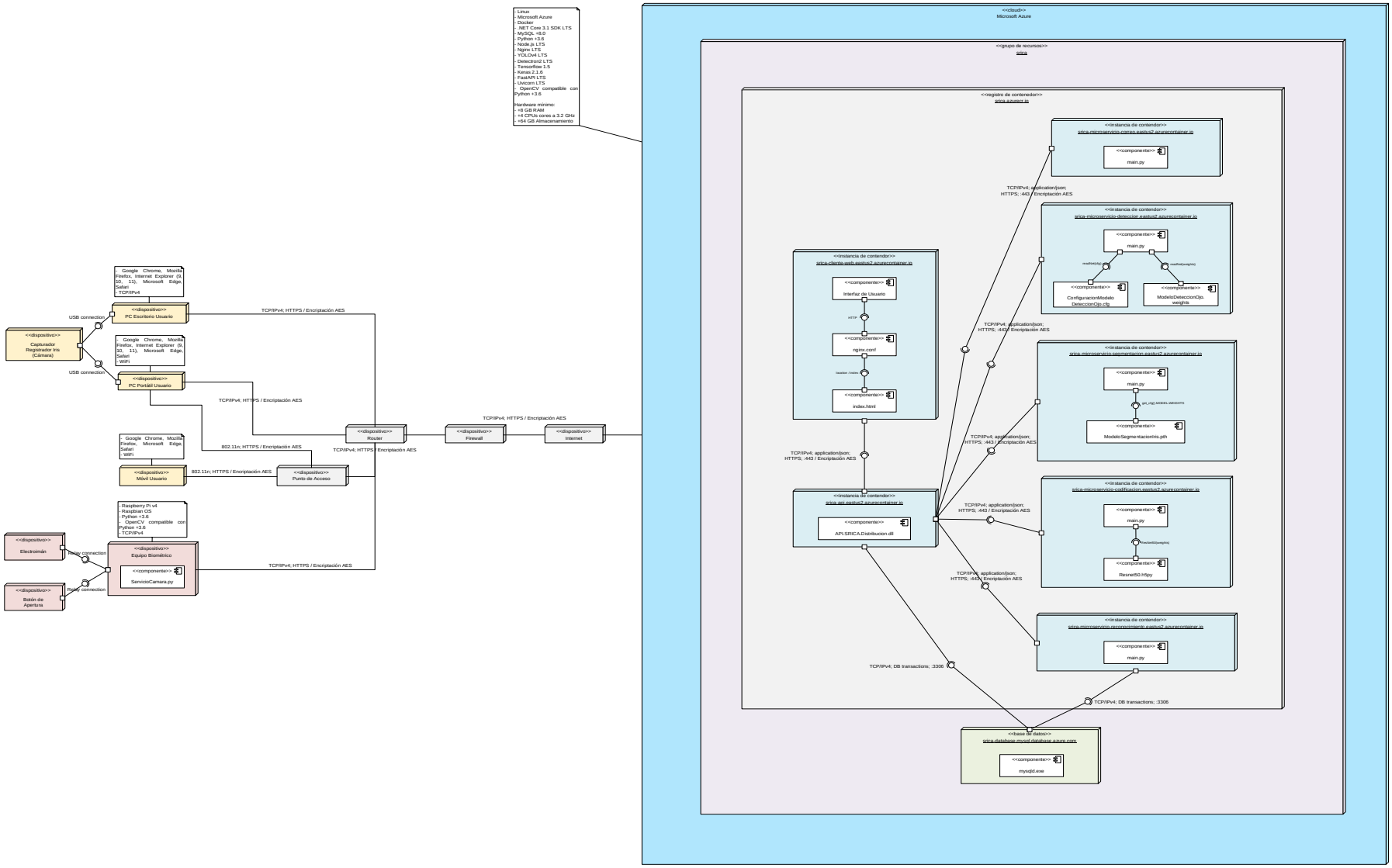


Para visualizar el documento **1.2.7 SRICA_027_000 - Diagrama de Componentes**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.7 SRICA_027_000 - Diagrama de Componentes.docx**.

### 2.2.8. 1.2.8 SRICA_028_000 - Diagrama de Despliegue

Este documento contiene el diagrama de componentes para representar los servidores de despliegue, nodos, tipo de comunicación, protocolos, componentes, dispositivos, y demás, en tiempo de ejecución del sistema. Así mismo, contiene el diagrama de arquitectura del sistema: por etapas según control de acceso, y diagrama general.

*Diagrama de despliegue*



A continuación, se presentan los diagramas de arquitectura de software correspondientes al aplicativo web, y a las cuatro etapas de control de acceso utilizando el Sistema de Reconocimiento de Iris - SRICA: Identificación, Autenticación, Autorización, Trazabilidad.

*Diagrama de arquitectura del sistema web*

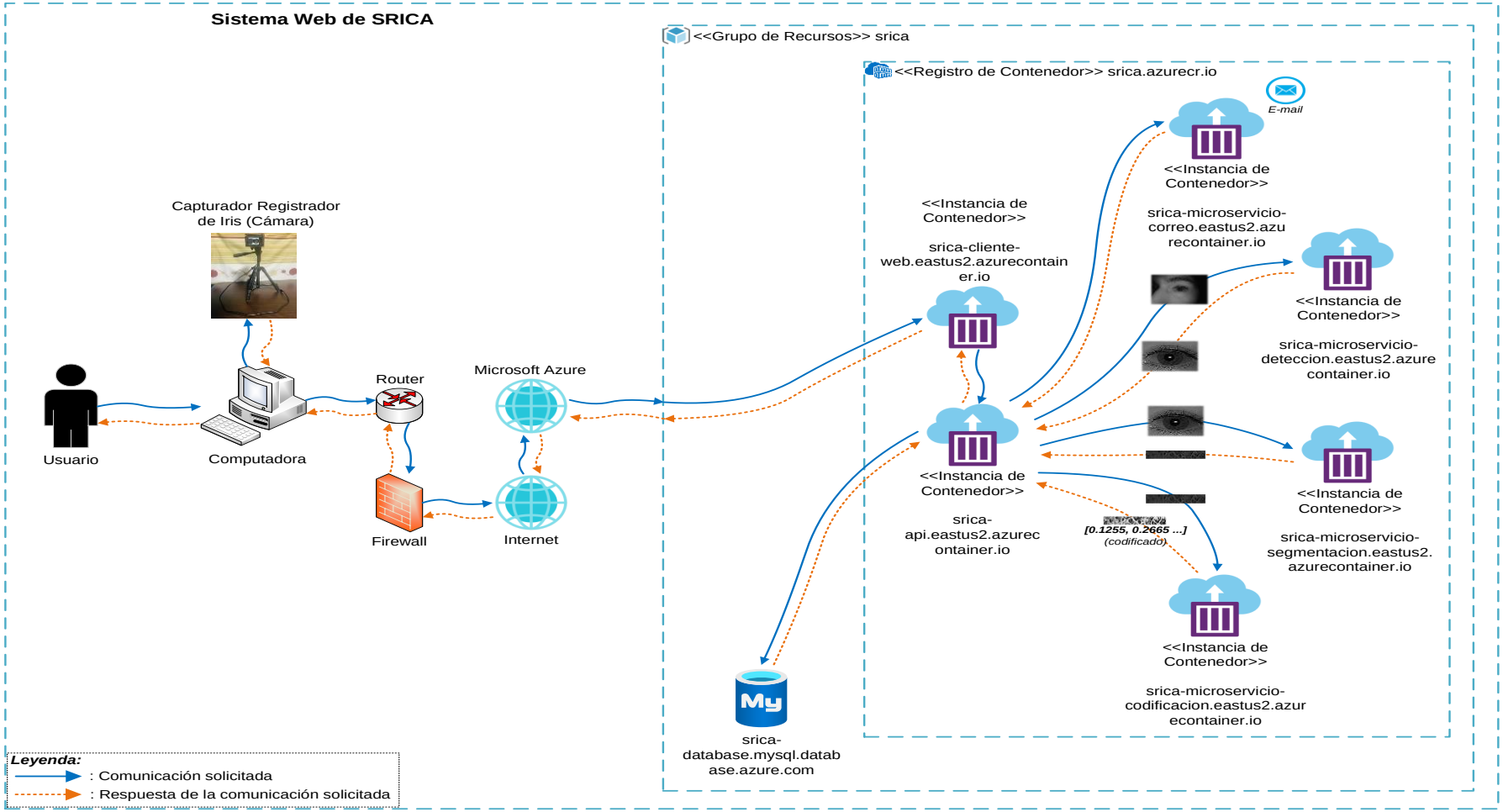


*Diagrama de arquitectura de la etapa "Identificación" durante el control de acceso utilizando el sistema*

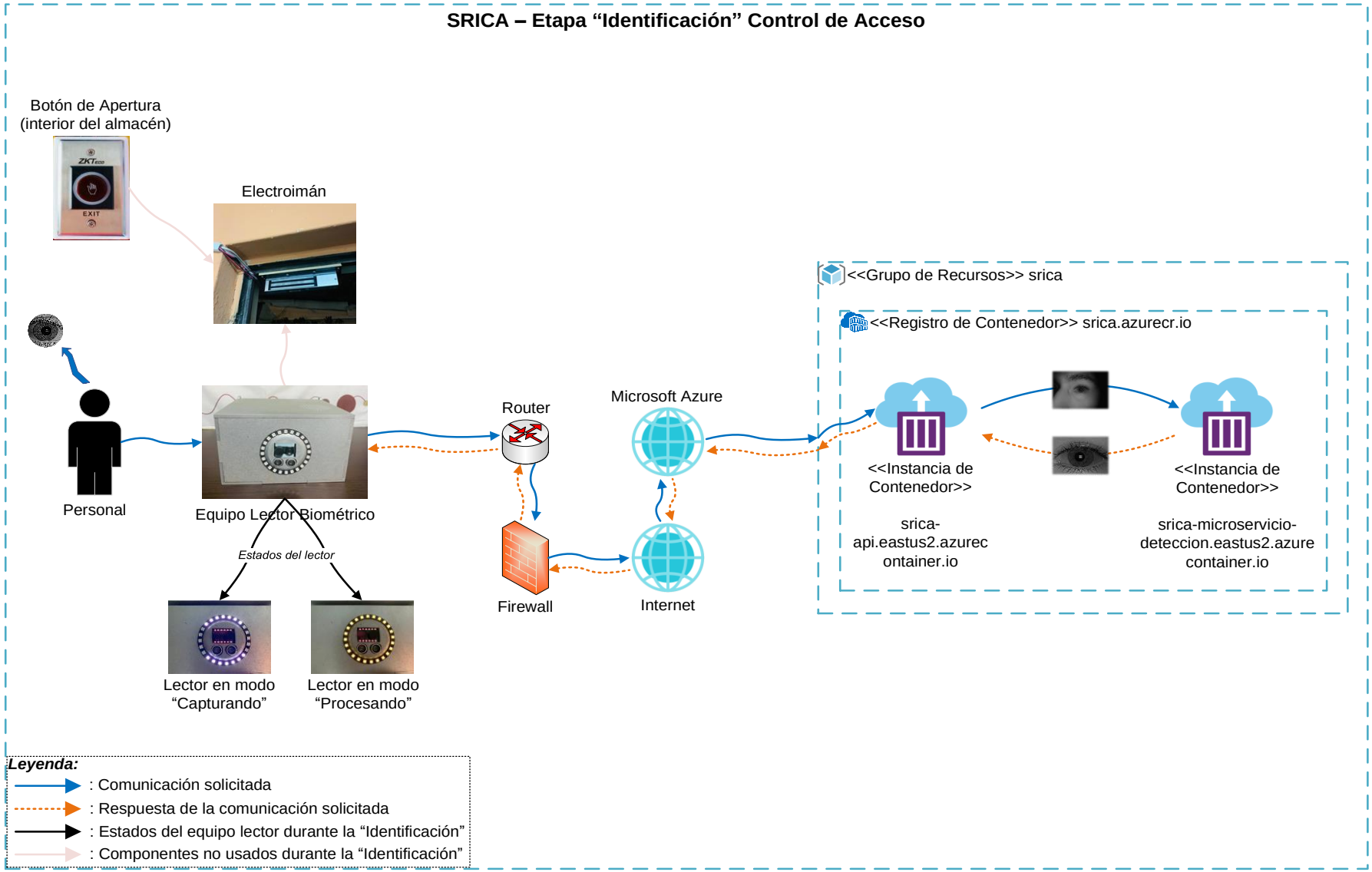


*Diagrama de arquitectura de la etapa "Autenticación" durante el control de acceso utilizando el sistema*

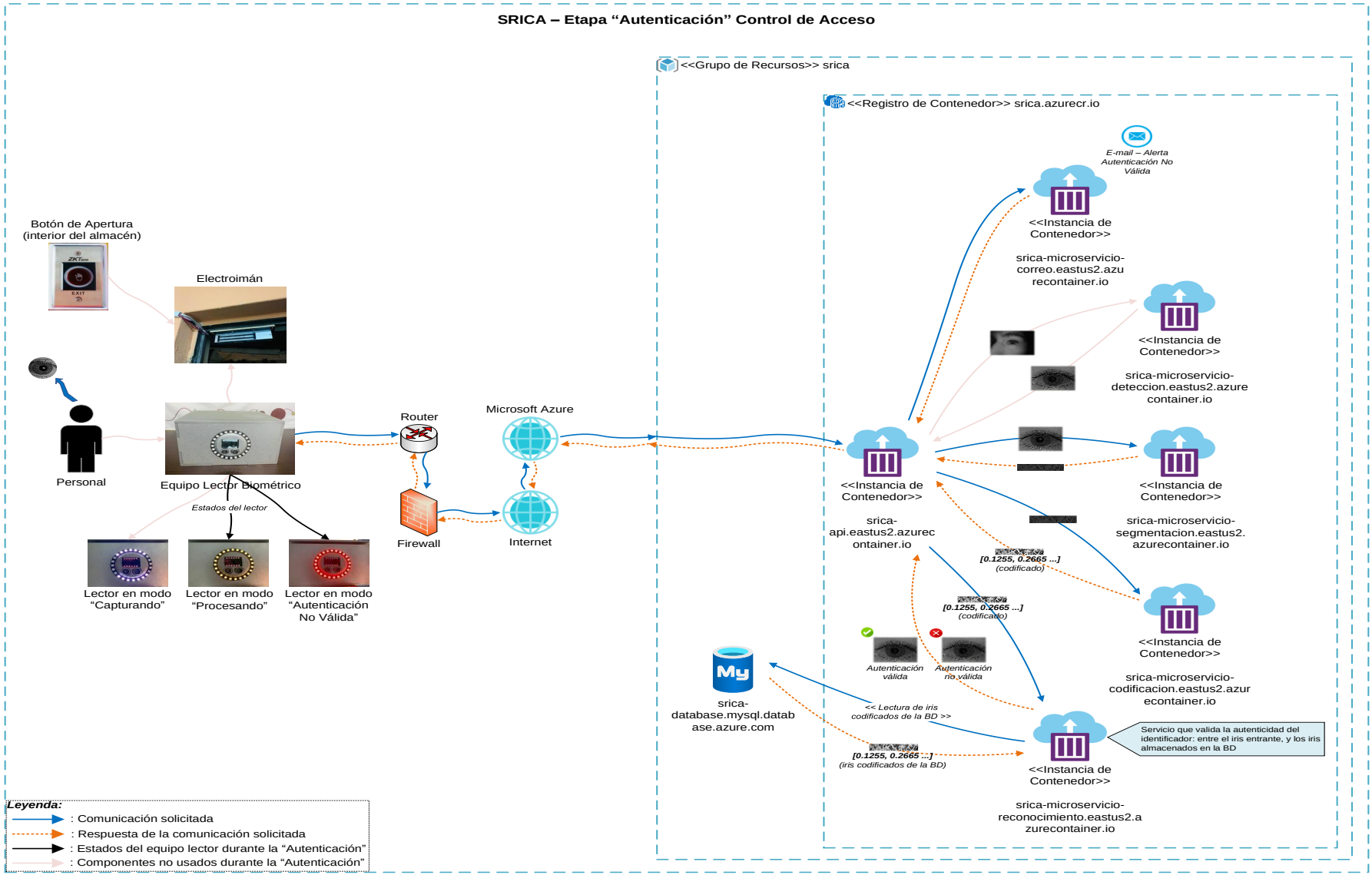


*Diagrama de arquitectura de la etapa "Autorización" durante el control de acceso utilizando el sistema*

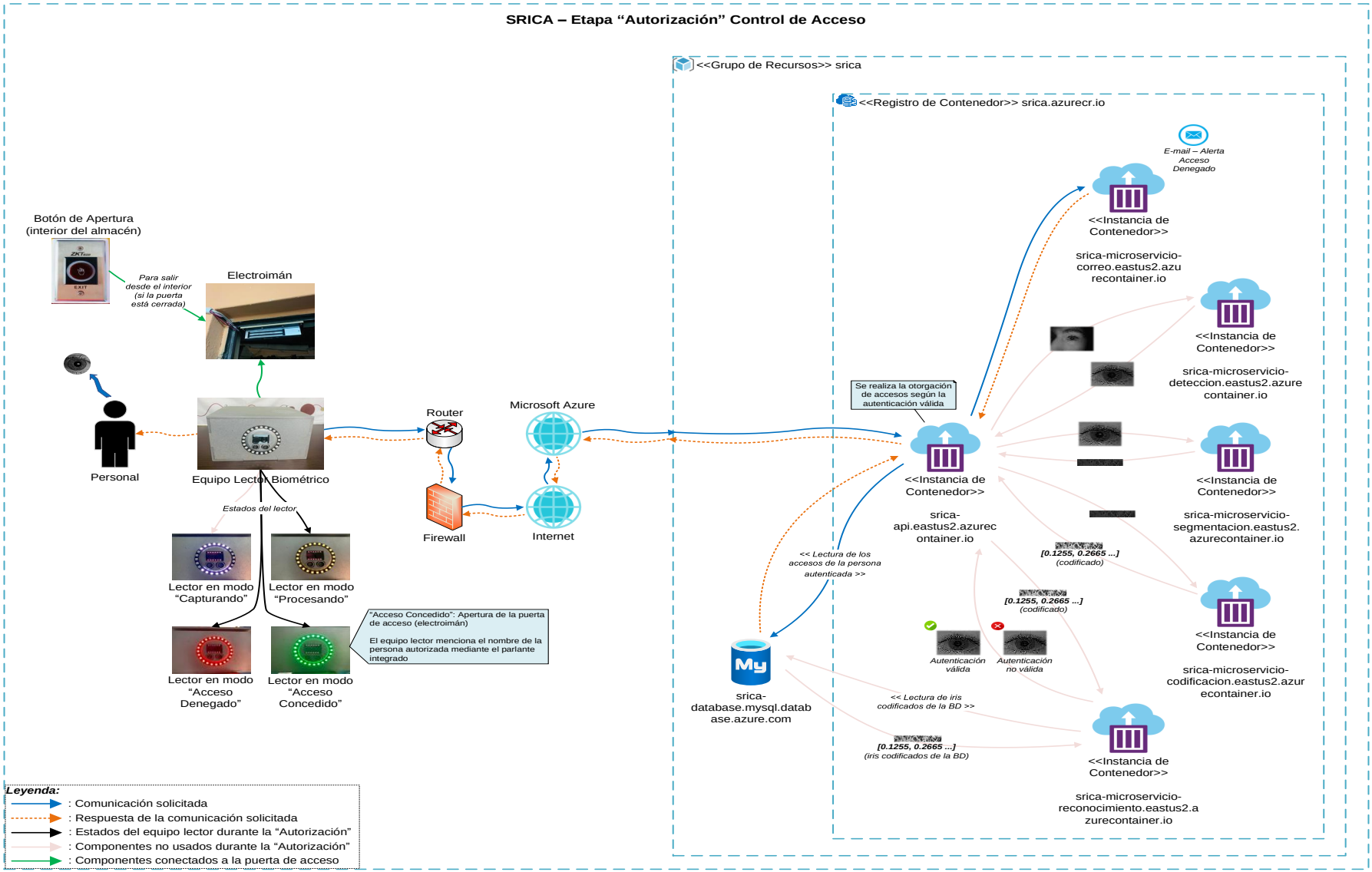


*Diagrama de arquitectura de la etapa “Trazabilidad” durante el control de acceso utilizando el sistema*

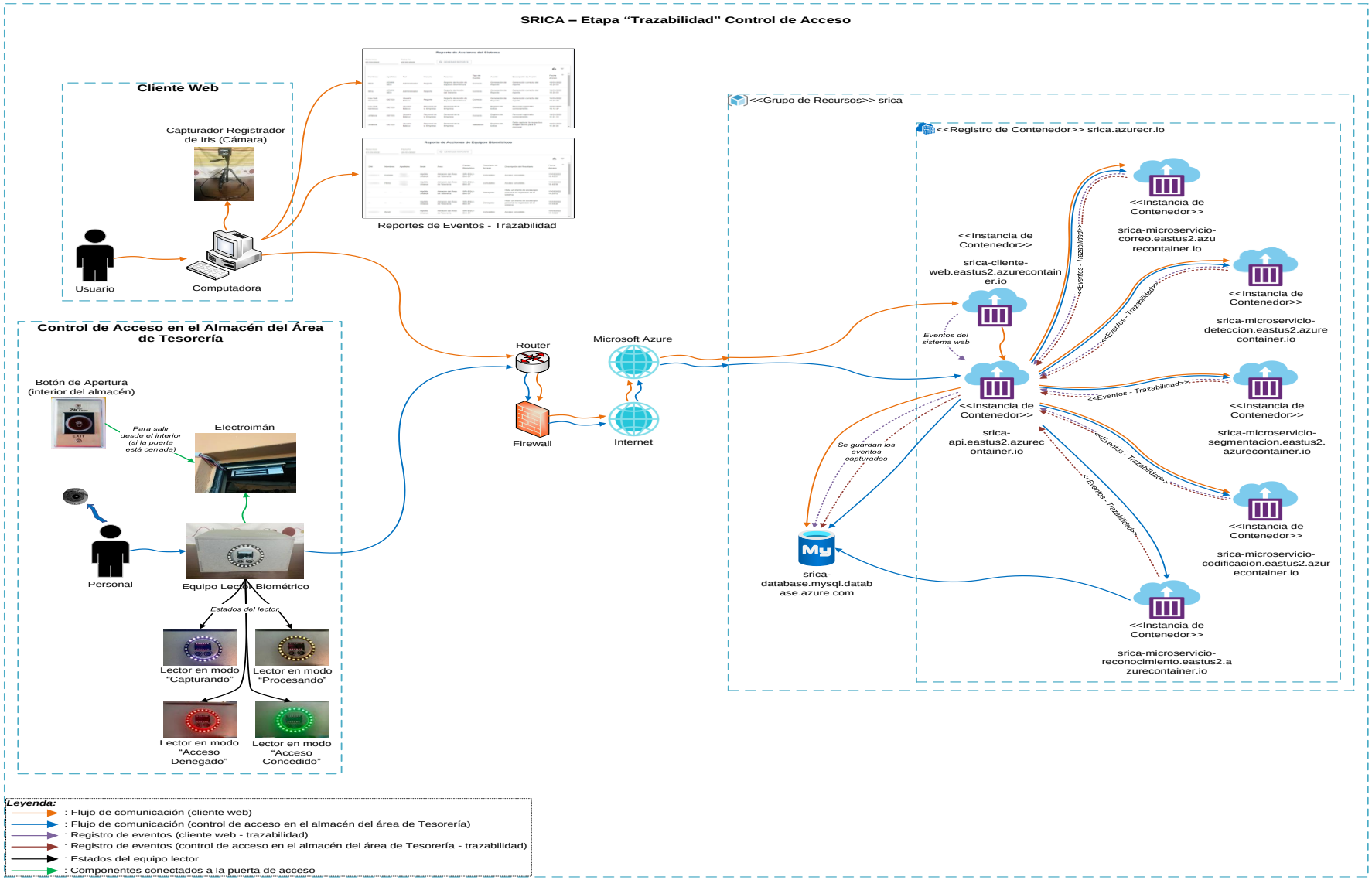
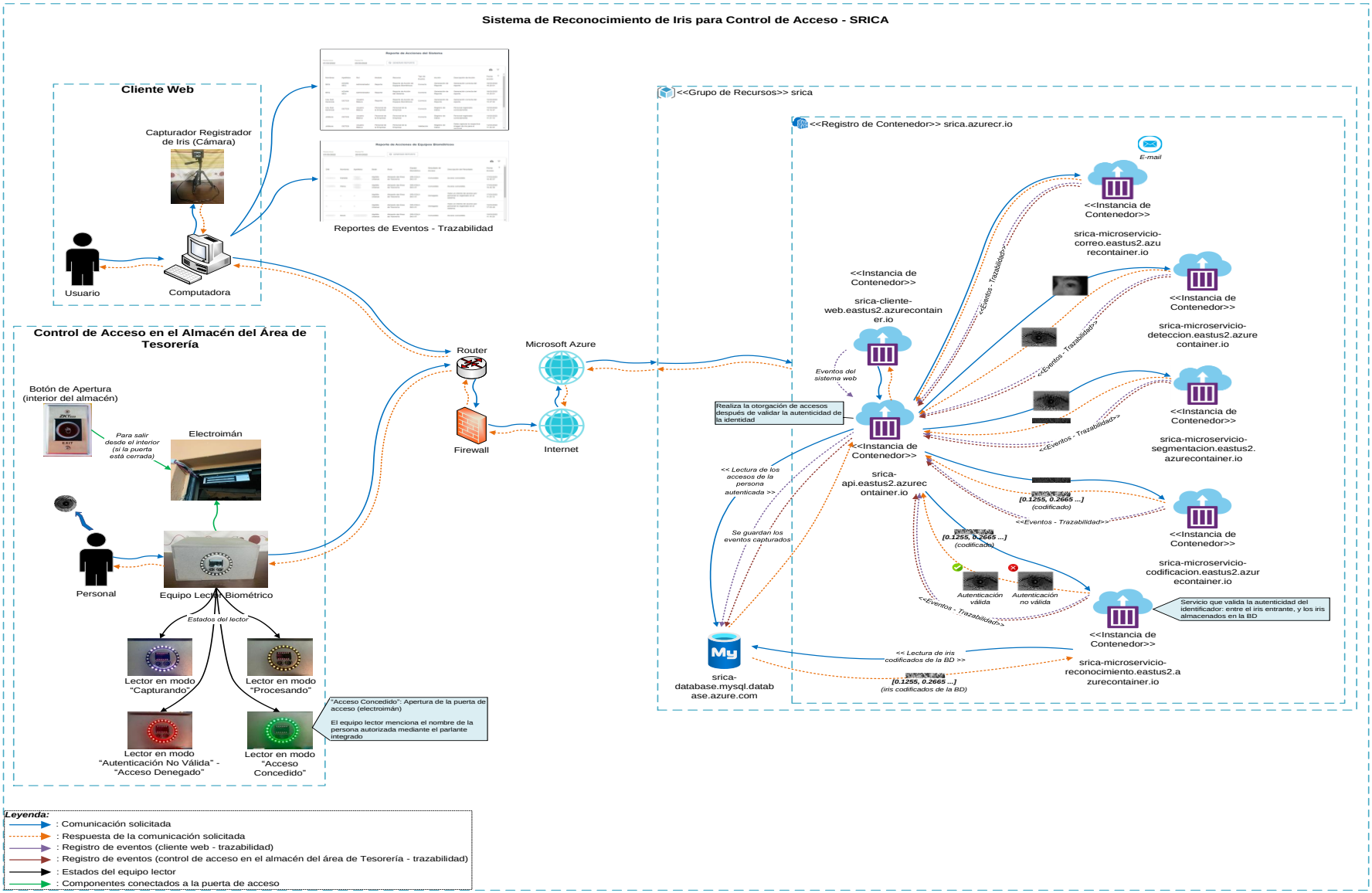


*Diagrama general de arquitectura*



Para visualizar el documento **1.2.8 SRICA_028_000 - Diagrama de Despliegue**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.8 SRICA_028_000 - Diagrama de Despliegue.docx**.

### 2.2.9. 1.2.9 SRICA_029_000 - Especificación de Requerimientos de Software (SRS)

Este documento describe detalladamente los requerimientos del sistema, tanto funcionales y no funcionales, aportando una visión amplia de la funcionalidad del sistema. El documento está construido en base a múltiples referencias: **SRICA_002_000 – Acta de Constitución del Proyecto**, **SRICA_006_000 – EDT**, **SRICA_021_000 – Requerimientos Funcionales y no Funcionales**, **SRICA_022_000 – Especificación Detallada de Casos de Uso y Prototipos**, **SRICA_023_000 – Diagrama de Casos de Uso**.

Para visualizar el documento **1.2.9 SRICA_029_000 - Especificación de Requerimientos de Software (SRS)**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.9 SRICA_029_000 - Especificación de Requerimientos de Software (SRS).docx**.

### 2.2.10. 1.2.10 SRICA_030_000 - Documento de Arquitectura de Software (SAD)

Este documento describe una visión general de la arquitectura del sistema, usando diferentes vistas para apreciar los diferentes aspectos que posee, mediante el uso de Lenguaje Unificado de Modelado (UML) 2.0. Así mismo, se establecen los modelos de datos y estándares de desarrollo (codificación) que se usarán en el desarrollo del sistema. El documento está construido en base a múltiples referencias: **SRICA_029_000 – Especificación de Requerimientos de Software (SRS)**, **SRICA_031_000 – Estándar de Codificación**, **SRICA_024_000 – Diagrama de Paquetes**, **SRICA_025_000 – Diagrama de Clases**, **SRICA_026_000 – Diagrama de Secuencia**, **SRICA_027_000 – Diagrama de Componentes**, **SRICA_028_000 – Diagrama de Despliegue**, **SRICA_032_000 – Diagrama Entidad – Relación**, **SRICA_033_000 – Modelo Lógico**, **SRICA_034_000 – Modelo Físico**, **SRICA_035_000 – Diccionario de Datos**.

Para visualizar el documento **1.2.10 SRICA_030_000 - Documento de Arquitectura de Software (SAD)**, revisar el repositorio GitHub descrito en el punto 1,

directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.10 SRICA_030_000 - Documento de Arquitectura de Software (SAD).docx**.

### 2.2.11. 1.2.11 SRICA_031_000 - Estándar de Codificación

Este documento describe el estándar de codificación de programación a utilizar en el desarrollo del sistema, y el estándar de codificación de base de datos.

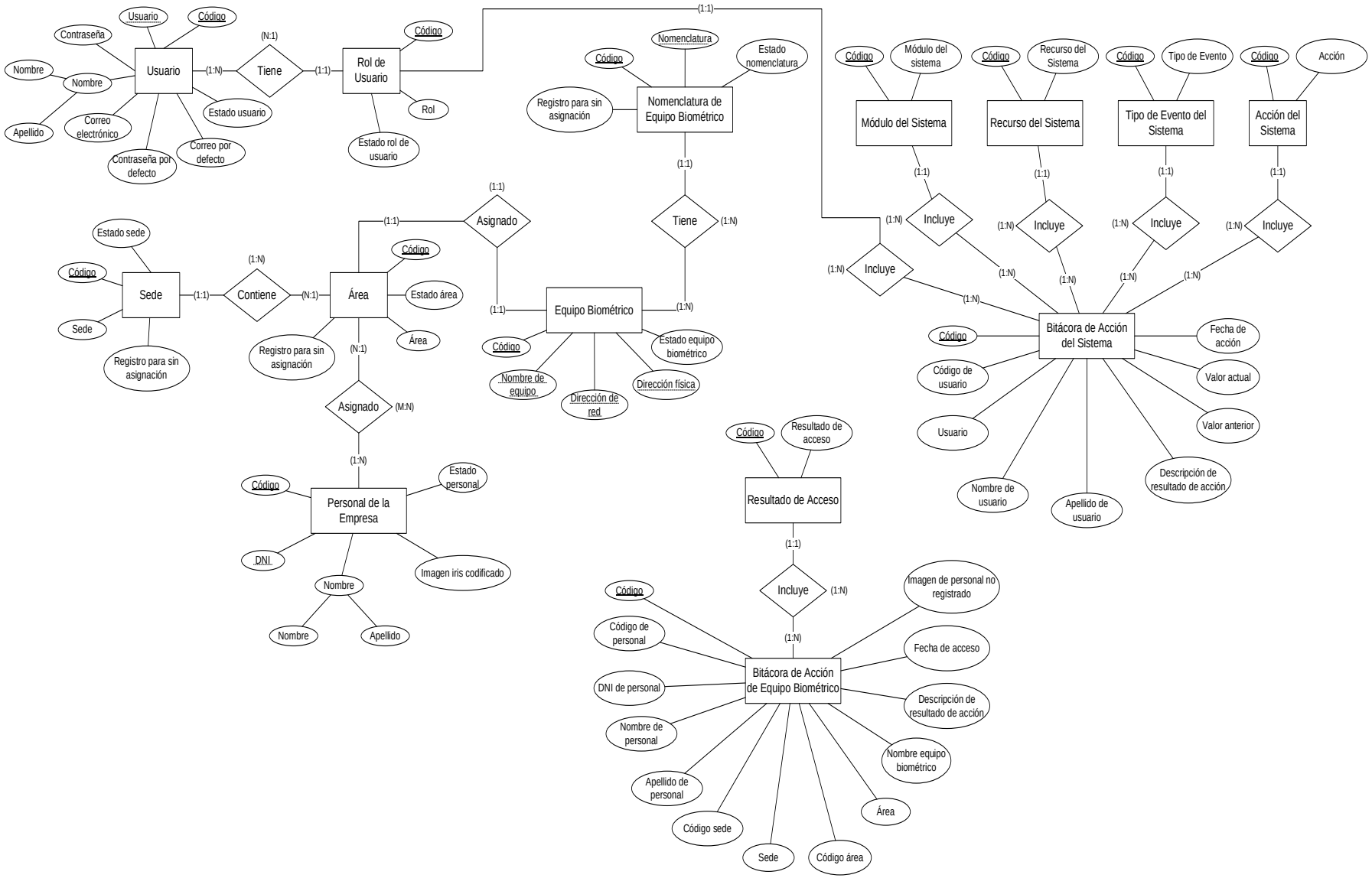
Para visualizar el documento **1.2.11 SRICA_031_000 - Estándar de Codificación**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.11 SRICA_031_000 - Estándar de Codificación.docx**.

### 2.2.12.Base de Datos

#### 2.2.12.1. 1.2.12.1 SRICA_032_000 - Diagrama Entidad – Relación

Este documento muestra el diagrama entidad – relación del sistema, que representarán a las tablas de la base de datos.

*Diagrama entidad - relación*

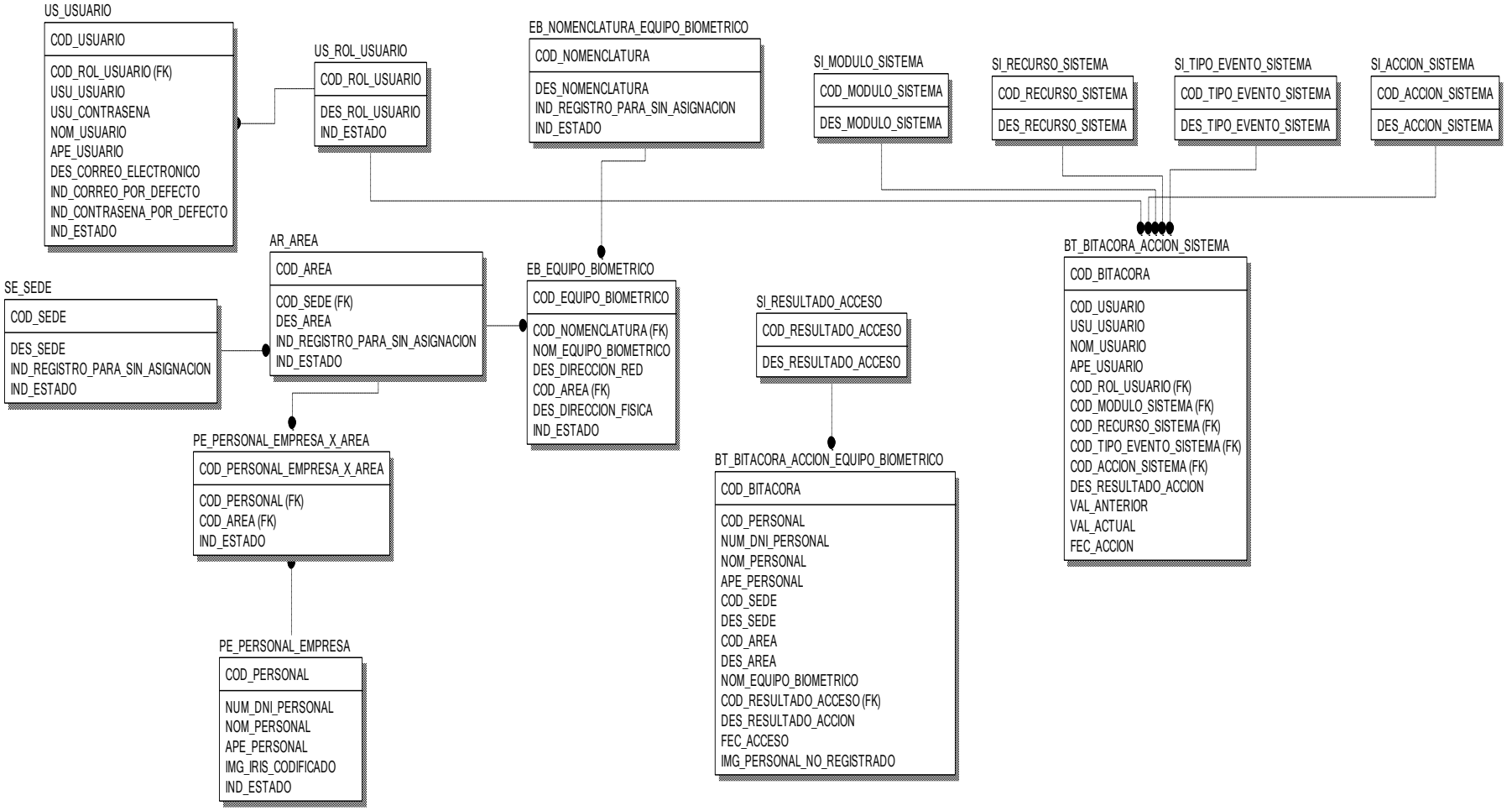


Para visualizar el documento **1.2.12.1 SRICA_032_000 - Diagrama Entidad - Relación**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.12 Base de Datos / 1.2.12.1 SRICA_032_000 - Diagrama Entidad - Relación.docx**.

### 2.2.12.2. 1.2.12.2 SRICA_033_000 - Modelo Lógico

Este documento muestra el diagrama de modelo lógico de base de datos que usará el sistema, especificando las propiedades o campos que tendrá cada futura tabla de base de datos.

*Diagrama de modelo lógico*

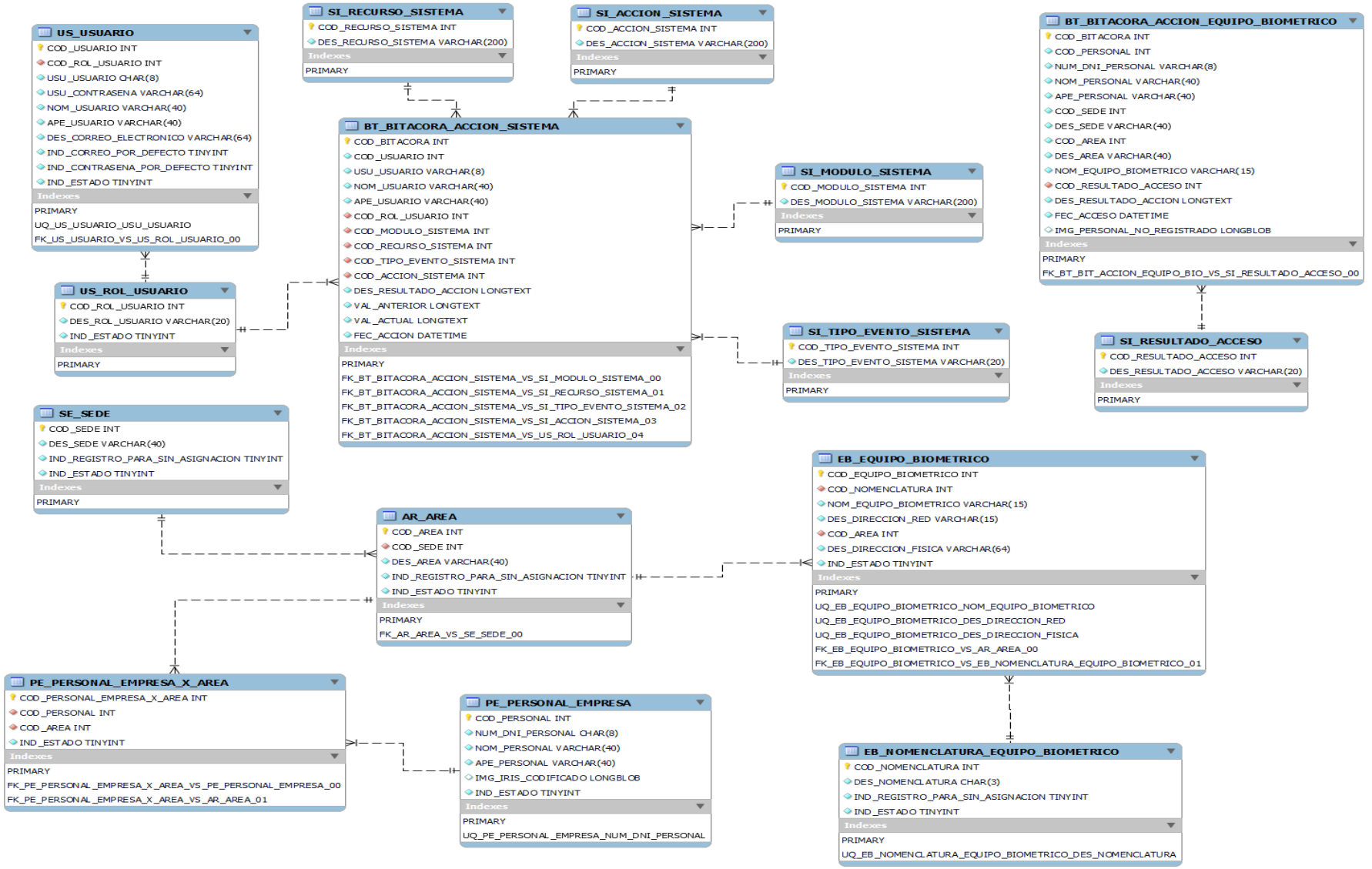


Para visualizar el documento **1.2.12.2 SRICA_033_000 - Modelo Lógico**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.12 Base de Datos / 1.2.12.2 SRICA_033_000 - Modelo Lógico.docx**.

### 2.2.12.3. 1.2.12.3 SRICA_034_000 - Modelo Físico

Este documento muestra el diagrama de modelo físico de base de datos que usará el sistema, especificando las propiedades o campos de las tablas, tipo de dato, llaves primarias, llaves foráneas, y restricciones de base de datos.

*Diagrama de modelo físico*



Para visualizar el documento **1.2.12.3 SRICA_034_000 - Modelo Físico**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.12 Base de Datos / 1.2.12.3 SRICA_034_000 - Modelo Físico.docx**.

#### 2.2.12.4. 1.2.12.4 SRICA_035_000 - Diccionario de Datos

Este documento detalla los esquemas, tablas y propiedades de la base de datos, para tener conocimiento del significado o responsabilidad de cada campo disponible en las tablas de base de datos.

Para visualizar el documento **1.2.12.4 SRICA_035_000 - Diccionario de Datos**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.2 Elaboración / 1.2.12 Base de Datos / 1.2.12.4 SRICA_035_000 - Diccionario de Datos.docx**.

### 2.3. Construcción

En esta fase se establece el código fuente del sistema, modelos de inteligencia artificial que son utilizados por los servicios del sistema, código fuente del equipo biométrico, y los respectivos documentos de ejecución de pruebas, referentes al proyecto.

A continuación, se detallan los elementos que participan dentro de la fase de Construcción de la metodología RUP aplicada (para más detalles, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción**):

#### 2.3.1. 1.3.1 Código Fuente

#### 2.3.1.1. Servicios

Para el desarrollo del proyecto, se han creado 7 servicios que contemplan los siguientes proyectos:

- Frontend, contiene el aplicativo web con funcionalidades CRUD y reportería para el Sistema de Reconocimiento de Iris. Desarrollado con React.js. Para visualizar el código fuente de proyecto “Frontend”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción/1.3.1 Código Fuente / 1.3.1.1 Frontend**.
- Backend, contiene el core y reglas de negocio del Sistema de Reconocimiento de Iris. Además, tiene el rol de comunicarse con los microservicios desarrollados y base de datos. Desarrollado con .Net Core

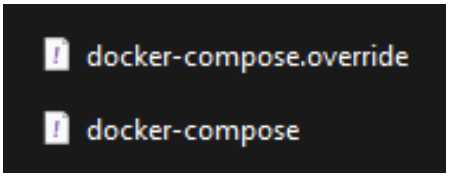
3.1. Para visualizar el código fuente de proyecto “Backend”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.2 Backend**.

- Microservicio de correo, contiene el servicio de correo para el envío de alertas del Sistema de Reconocimiento de Iris. Desarrollado con Python. Para visualizar el código fuente de proyecto “Microservicio de correo”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.3 Microservicio de Correo**.
- Microservicio de detección de iris, contiene el servicio de detección de iris del Sistema de Reconocimiento de Iris. Desarrollado con Python. Para visualizar el código fuente de proyecto “Microservicio de detección de iris”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.4 Microservicio de Detección de Iris**.
- Microservicio de segmentación de iris, contiene el servicio de segmentación de iris del Sistema de Reconocimiento de Iris. Desarrollado con Python. Para visualizar el código fuente de proyecto “Microservicio de segmentación de iris”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.5 Microservicio de Segmentación de Iris**.
- Microservicio de codificación de iris, contiene el servicio de codificación de iris del Sistema de Reconocimiento de Iris. Desarrollado con Python. Para visualizar el código fuente de proyecto “Microservicio de codificación de iris”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.6 Microservicio de Codificación de Iris**.
- Microservicio de reconocimiento de iris, contiene el servicio de reconocimiento de iris del Sistema de Reconocimiento de Iris. Desarrollado con Python. Para visualizar el código fuente de proyecto “Microservicio de reconocimiento de iris”, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.1 Código Fuente / 1.3.1.7 Microservicio de Reconocimiento de Iris**.

### 2.3.1.2. Docker-Compose

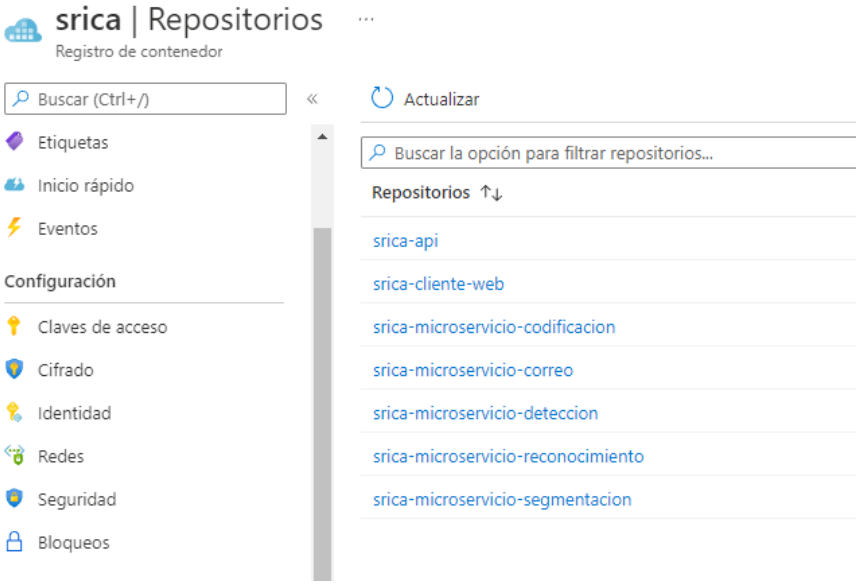
Para el despliegue de los servicios en contenedores, se está utilizando Docker, y se agiliza el despliegue masivo de los servicios mediante docker-compose.

*Archivos docker-compose para el despliegue del sistema*



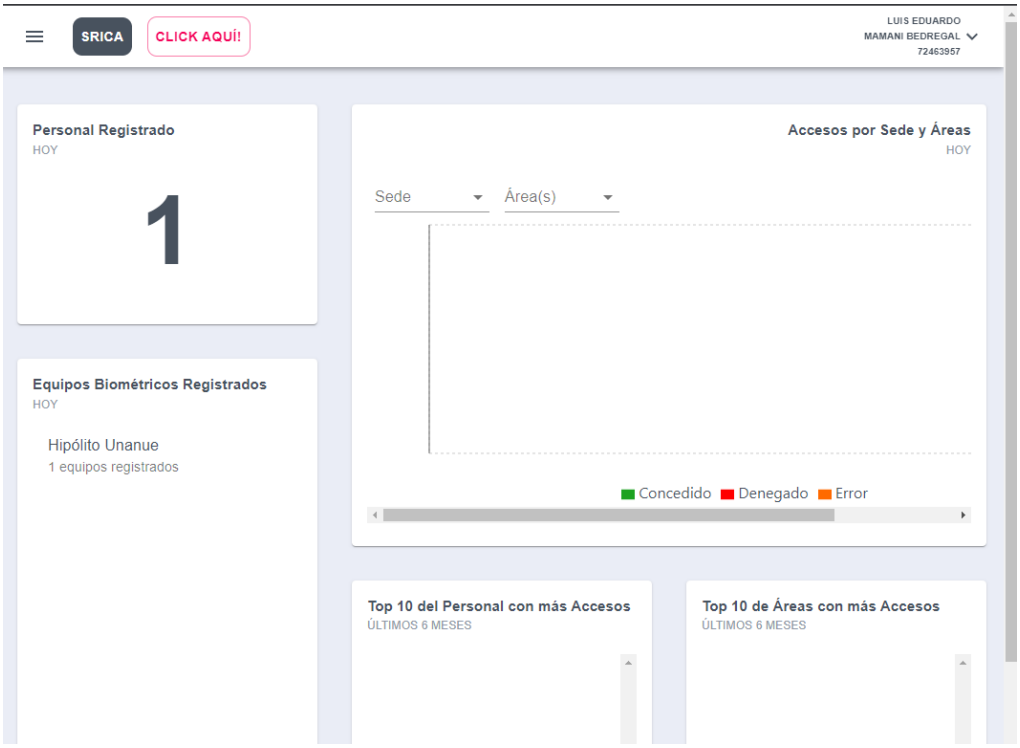

Los servicios son desplegados en el proveedor Cloud Microsoft Azure, y se muestran a continuación:

*Servicios desplegados en Microsoft Azure*




- **srica-cliente-web**, cliente web del sistema para la gestión de registros, y visualización de reportes.

*Interfaz del sistema*




- **srica-api**, backend que contiene la lógica de negocio del sistema. Se comunica con los microservicios.
- **srica-microservicio-correo**, microservicio de correo para el envío de alertas del sistema.
- **srica-microservicio-deteccion**, microservicio de detección del ojo humano.
- **srica-microservicio-segmentacion**, microservicio de segmentación del ojo humano. Segmenta en tres clases: ojo, iris, pupila.
- **srica-microservicio-codificacion**, microservicio de codificación del iris humano. Genera un vector de características del iris.
- **srica-microservicio-reconocimiento**, microservicio de reconocimiento de iris. Compara los vectores de características del personal para reconocer a la persona correcta.

#### 2.3.1.3. Equipo Capturador de Iris para el Registro del Personal en el Sistema

Durante el proceso de registro del personal, es necesario capturar el iris de la persona para que pueda tener acceso al área. Para ello, se ha elaborado un capturador de iris que se conecta al equipo computador del usuario registrador para su respectivo uso.

*Equipo registrador de iris – exterior*

*Equipo registrador de iris – interior*

### 2.3.2. 1.3.2 Inteligencia Artificial

El sistema de Reconocimiento de Iris utiliza varios modelos de Deep Learning que son esenciales para el procesamiento de imágenes de iris de las personas, de los cuales, se listan a continuación:

#### 2.3.2.1. 1.3.2.1 Modelo de Deep Learning de Detección y Segmentación de la Imagen de Iris

Contiene los modelos de Deep Learning para la detección y segmentación de imágenes de iris, respectivamente.

La descripción detallada de los modelos de Deep Learning se encuentran en el Anexo 7.

#### 2.3.2.2. 1.3.2.2 Modelo de Deep Learning de Codificación y Reconocimiento de la Imagen de Iris

Contiene los modelos de Deep Learning para la codificación de imágenes de iris, generando un vector de características, y procesado durante el reconocimiento de iris para cada persona.

La descripción detallada de los modelos de Deep Learning se encuentran en el Anexo 7.

### 2.3.3. 1.3.3 Equipo Biométrico

El equipo biométrico es el dispositivo que captura las imágenes de iris de las personas, conectándose a los servicios de inteligencia artificial para el respectivo procesamiento.

La descripción detallada del dispositivo “Equipo Biométrico” se encuentra en el Anexo 6.

### 2.3.4. 1.3.4 Pruebas

#### 2.3.4.1. 1.3.4.1 SRICA_039_000 - Plan de Pruebas

Este documento contempla el plan de pruebas a ejecutar en el proyecto, indicando pruebas unitarias y pruebas de despliegue, siendo informadas post – ejecución en el documento **SRICA_042_000 - Informe de Pruebas**.

Para visualizar el documento **1.3.4.1 SRICA_039_000 - Plan de Pruebas**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.4 Pruebas / 1.3.4.1 SRICA_039_000 - Plan de Pruebas.docx**.

#### 2.3.4.2. 1.3.4.2 SRICA_040_000 - Pruebas Unitarias

Este documento contiene las pruebas unitarias a ser ejecutadas en el proyecto, siendo informadas post – ejecución en el documento **SRICA_042_000 - Informe de Pruebas**.

Para visualizar el documento **1.3.4.2 SRICA_040_000 - Pruebas Unitarias**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.4 Pruebas / 1.3.4.2 SRICA_040_000 - Pruebas Unitarias.docx**.

#### 2.3.4.3. 1.3.4.3 SRICA_041_000 - Pruebas de Despliegue

Este documento contiene las pruebas de despliegue a ser ejecutadas en el proyecto, siendo informadas post – ejecución en el documento **SRICA_042_000 - Informe de Pruebas**.

Para visualizar el documento **1.3.4.3 SRICA_041_000 - Pruebas de Despliegue**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.4 Pruebas / 1.3.4.3 SRICA_041_000 - Pruebas de Despliegue.docx**.

#### 2.3.4.4. 1.3.4.4 SRICA_042_000 - Informe de Pruebas

Este documento contiene el resultado de la ejecución de las pruebas unitarias y de despliegue, hechas al proyecto.

Para visualizar el documento **1.3.4.4 SRICA_042_000 - Informe de Pruebas**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.4 Pruebas / 1.3.4.4 SRICA_042_000 - Informe de Pruebas.docx**.

### 2.4. Cierre

En esta fase se indica el manual técnico y manual de usuario del sistema.

A continuación, se detallan los elementos que participan dentro de la fase de Cierre de la metodología RUP aplicada (para más detalles, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.4 Cierre**):

### 2.4.1. 1.4.1 SRICA_043_000 - Manual Técnico

En este documento se describen los detalles técnicos a contemplar para el correcto despliegue y funcionamiento del Sistema de Reconocimiento de Iris, el cual, contempla requerimientos técnicos de hardware y de software. El documento está construido en base a múltiples referencias: **SRICA_023_000 - Diagrama de Casos de Uso**, **SRICA_034_000 - Modelo Físico**, **SRICA_035_000 - Diccionario de Datos**, **SRICA_044_000 - Manual de Usuario**.

Para visualizar el documento **1.4.1 SRICA_043_000 - Manual Técnico**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.4 Cierre / 1.4.1 SRICA_043_000 - Manual Técnico.docx**.

### 2.4.2. 1.4.2 SRICA_044_000 - Manual de Usuario

Este documento representa una guía de uso del Sistema de Reconocimiento de Iris, contemplando todas las funcionalidades disponibles en el sistema, y proporcionando el "paso a paso" de un correcto manejo del sistema, tanto del sistema web y equipo biométrico.

Para visualizar el documento **1.4.2 SRICA_044_000 - Manual de Usuario**, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.4 Cierre / 1.4.2 SRICA_044_000 - Manual de Usuario.docx**.

# Anexo 6. SRICA – Equipo biométrico

## 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, cuenta con un equipo biométrico construido por medios propios, que sirve como controlador para permitir el acceso a la puerta del área protegida. Está integrado con múltiples sensores y componentes electrónicos, trabajando conjuntamente para un correcto funcionamiento.

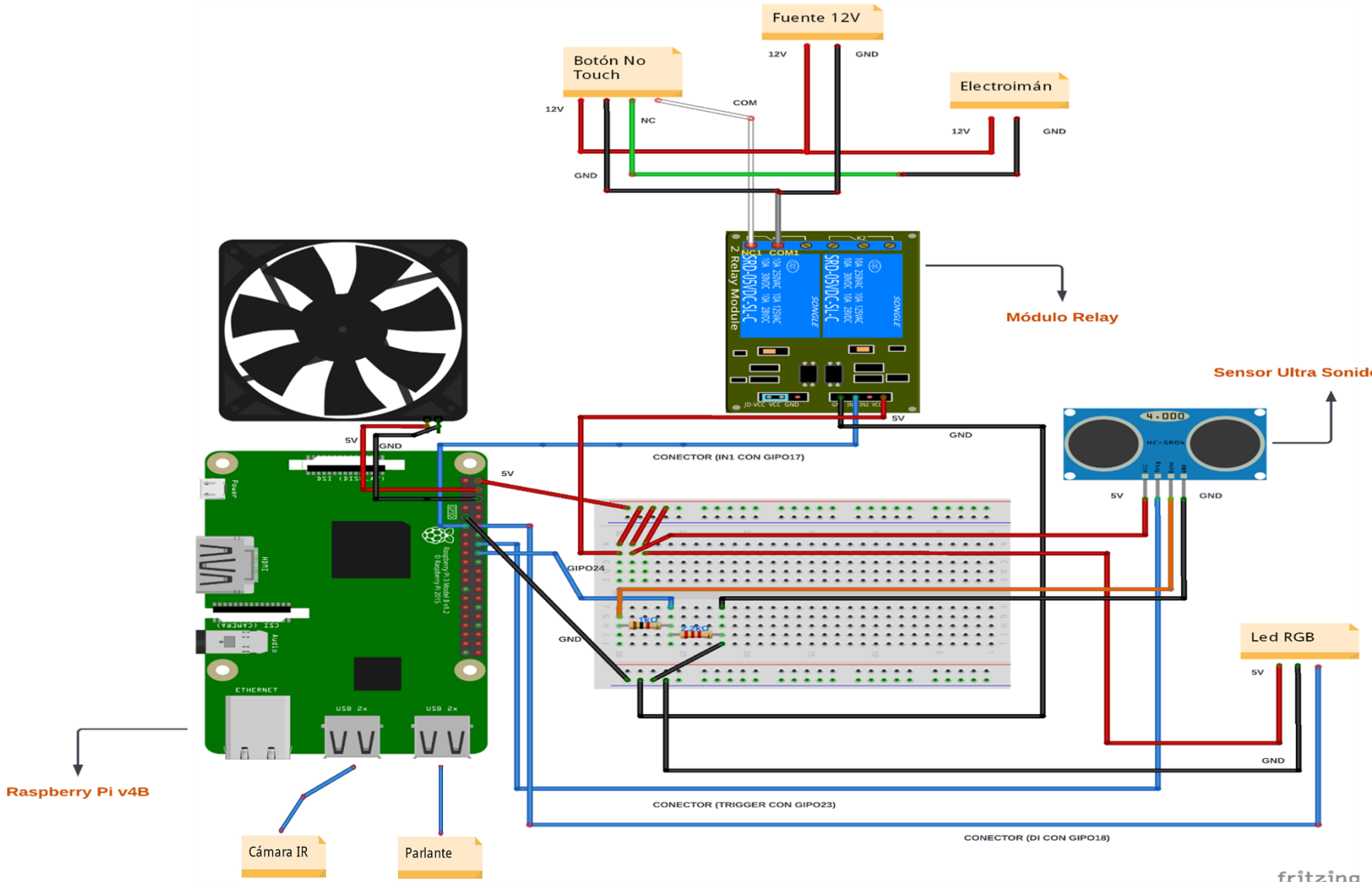
Para la realización del diseño de circuitos y código fuente, de los cuales, en los siguientes puntos se mencionará de forma detallada, se ha creado el siguiente repositorio GitHub: **https://github.com/LuisEdMB/SRICA**. Cualquier investigador puede revisar y usar los elementos descritos en el repositorio, solo para fines de investigación.

## 2. Diseño de Circuitos

El equipo biométrico elaborado, se encarga de capturar el iris de la persona para su respectivo post procesamiento según los servicios que contiene el sistema de reconocimiento. Para ello, el equipo biométrico está integrado con diversos componentes que sirven para lograr el objetivo de control de acceso al área protegida. **El equipo no almacena, en su capacidad de almacenamiento, las imágenes de iris a reconocer. Toda la información es almacenada en los servidores, para evitar que se pierda la información de los iris si es que existe robo del equipo.**

Las conexiones, circuitos, y componentes, son representados en el siguiente diagrama electrónico:

*Diseño electrónico del equipo biométrico*



**3. Descripción de Componentes**

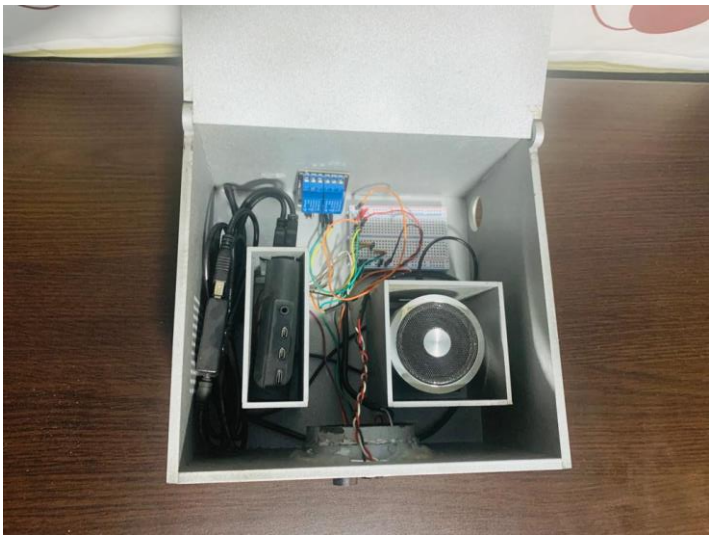
- Fuente 12V de corriente continua que alimenta al **Botón No Touch** y **Electroimán**.
- Electroimán de 272 kg de fuerza, que es colocado en la parte superior de la puerta de acceso. Solo se abre mediante el **Botón No Touch**, o mediante el **Módulo Relay** ejecutado por **Raspberry Pi v4B**.
- Botón No Touch que tiene la funcionalidad de cortar la corriente o circuito del **Electroimán** para interrumpir el flujo electromagnético de éste. Es colocado dentro del área para que el personal pueda salir del ambiente.
- Módulo Relay electrónico que permite controlar dispositivos que usa un mayor voltaje con respecto a **Raspberry Pi v4B**. Esta herramienta sirve para controlar el **Electroimán** que funciona con 12V de energía.
- Sensor Ultra Sonido que detecta la cercanía de la persona al equipo biométrico, para poder comenzar con el proceso de captura y procesamiento de la imagen de iris.
- Led RGB que manifiesta cuatro tipos de colores que indican los procesos de: capturando, procesando, acceso concedido, acceso denegado / error. Este módulo trabaja conjuntamente con el **Sensor Ultra Sonido** para el cambio de sus tipos de colores.
- Resistores para el correcto funcionamiento del **Sensor Ultra Sonido**, el cual es necesario conectar su circuito con dos resistencias: 1kΩ y 2.2kΩ. Caso contrario, el **Sensor Ultra Sonido** puede arrojar valores incorrectos.
- Raspberry Pi v4B que se encarga de coordinar y ejecutar los procesos necesarios para el buen funcionamiento del equipo, y de los demás componentes integrados a éste.
- Parlante conectado al **Raspberry Pi v4B** que se encarga de transmitir sonidos y audios según respuestas recibidas por el procesamiento de la imagen de iris.
- Cámara IR que captura la imagen inicial del iris de la persona para su respectivo procesamiento. Utiliza luz IR para obtener la estructura real del iris (ver Anexo 8, donde se indica el estándar IEC-62471 para productos con luces LED).

## 4. Estructura Física del Equipo Biométrico

Según el diseño electrónico descrito en el punto 2, se ha elaborado una carcasa o caja donde se encuentran los componentes electrónicos interconectados, logrando que el equipo biométrico sea fácilmente transportado a cualquier lugar.

*Estructura física del equipo biométrico - exterior*

*Estructura física del equipo biométrico - interior*



## 5. Código Fuente

Para visualizar el código fuente del equipo biométrico, revisar el repositorio GitHub descrito en el punto 1, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.3 Equipo Biométrico**.

### 5.1. Servicio “daemon” Capturador

**ServicioCamara.service**, es un archivo que permite crear un proceso “daemon”, ejecutando un archivo **ServicioCamara.py** en background dentro de Raspberry Pi v4B, mediante comando de Python, procesando la función principal que inicia el servicio de cámara capturador de la imagen de iris.

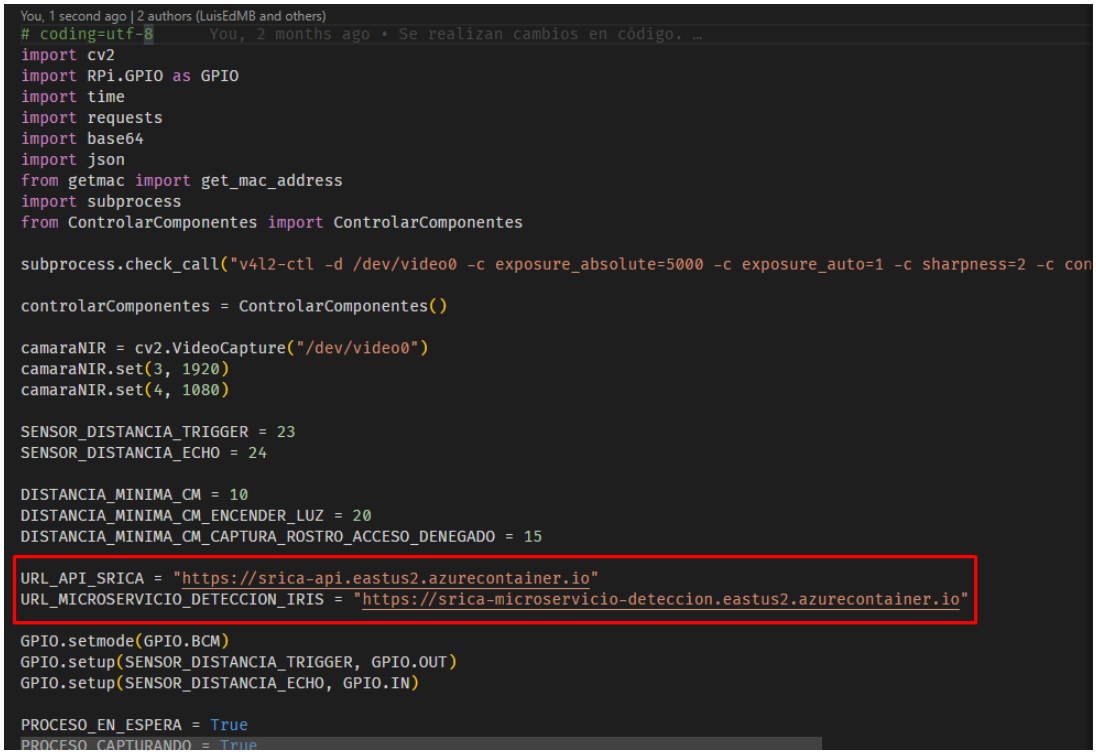
*Servicio “daemon” capturador – equipo biométrico*

```
[Unit]
Description=Servicio de camara en el equipo.
After=network.target

[Service]
User=root
Type=simple
ExecStart=/usr/bin/python3 /home/pi/ServicioCamara.py
StandardInput=tty-force
Restart=always

[Install]
WantedBy=default.target
```

### 5.2. Servicio de Cámara

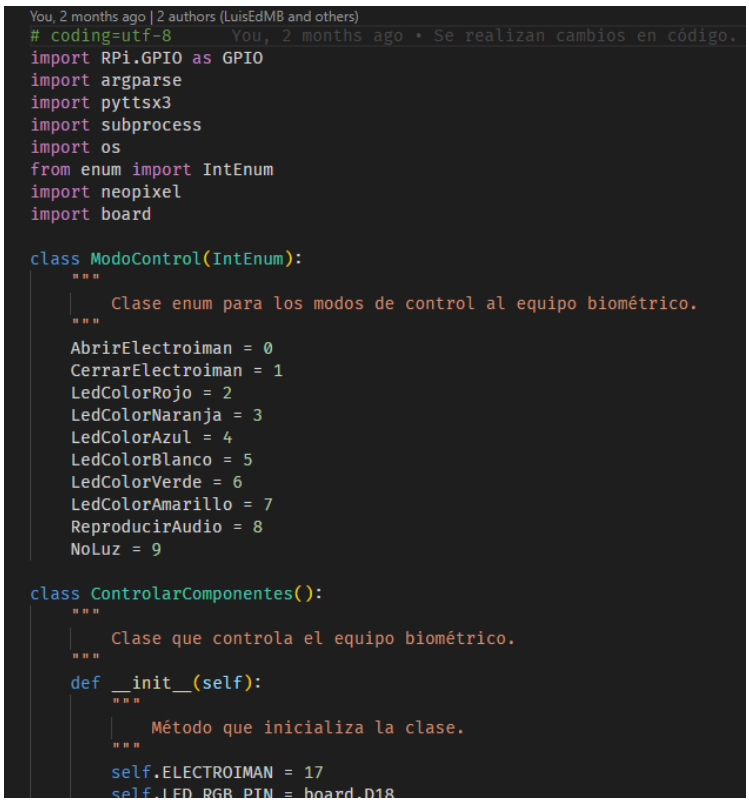
**ServicioCamara.py**, es un archivo que contiene la función principal que inicia el servicio de cámara capturador de la imagen de iris. Es el archivo principal del equipo biométrico que controla los componentes electrónicos, mediante un archivo **ControlarComponentes.py** utilitario. Dentro del mismo archivo principal, se encuentran las conexiones a los servicios del Sistema de Reconocimiento de Iris necesarios para el funcionamiento del equipo biométrico.

*Código principal y configuración – equipo biométrico*



```
You, 1 second ago | 2 authors (LuisEdMB and others)
# coding=utf-8      You, 2 months ago • Se realizan cambios en código. …
import cv2
import RPi.GPIO as GPIO
import time
import requests
import base64
import json
from getmac import get_mac_address
import subprocess
from ControlarComponentes import ControlarComponentes

subprocess.check_call("v4l2-ctl -d /dev/video0 -c exposure_absolute=5000 -c exposure_auto=1 -c sharpness=2 -c con

controlarComponentes = ControlarComponentes()

camaraNIR = cv2.VideoCapture("/dev/video0")
camaraNIR.set(3, 1920)
camaraNIR.set(4, 1080)

SENSOR_DISTANCIA_TRIGGER = 23
SENSOR_DISTANCIA_ECHO = 24

DISTANCIA_MINIMA_CM = 10
DISTANCIA_MINIMA_CM_ENCENDER_LUZ = 20
DISTANCIA_MINIMA_CM_CAPTURA_ROSTRO_ACCESO_DENEGADO = 15

URL_API_SRICA = "https://srica-api.eastus2.azurecontainer.io"
URL_MICROSERVICIO_DETECCION_IRIS = "https://srica-microservicio-deteccion.eastus2.azurecontainer.io"

GPIO.setmode(GPIO.BCM)
GPIO.setup(SENSOR_DISTANCIA_TRIGGER, GPIO.OUT)
GPIO.setup(SENSOR_DISTANCIA_ECHO, GPIO.IN)

PROCESO_EN_ESPERA = True
PROCESO_CAPTURANDO = True
```

*Código controlador de los componentes electrónicos – equipo biométrico*



```
You, 2 months ago | 2 authors (LuisEdMB and others)
# coding=utf-8      You, 2 months ago • Se realizan cambios en código.
import RPi.GPIO as GPIO
import argparse
import pyttsx3
import subprocess
import os
from enum import IntEnum
import neopixel
import board

class ModoControl(IntEnum):
    """
        Clase enum para los modos de control al equipo biométrico.
    """
    AbrirElectroiman = 0
    CerrarElectroiman = 1
    LedColorRojo = 2
    LedColorNaranja = 3
    LedColorAzul = 4
    LedColorBlanco = 5
    LedColorVerde = 6
    LedColorAmarillo = 7
    ReproducirAudio = 8
    NoLuz = 9

class ControlarComponentes():
    """
        Clase que controla el equipo biométrico.
    """
    def __init__(self):
        """
            Método que inicializa la clase.
        """
        self.ELECTROIMAN = 17
        self.LED_RGB_PIN = board.D18
```

# Anexo 7. SRICA – Deep Learning

## 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, cuenta con microservicios encargados de detectar, segmentar, codificar y reconocer la imagen de iris de cada persona. Estos servicios utilizan procesos con aprendizaje profundo (Deep Learning), ya que, este subcampo de Machine Learning, es más eficaz para el procesamiento de imágenes, debido a su gran cantidad de capaz ocultas, capaces de extraer características de una forma más eficiente.

Para el entrenamiento de los modelos de DL, se optó por usar Google Colab (**https://colab.research.google.com**), debido a que, para realizar un entrenamiento más rápido, es necesario el uso de GPU (se puede utilizar CPU, pero tomará más tiempo).

Para encontrar los modelos entrenados y/o utilizados, revisar el siguiente repositorio GitHub: **https://github.com/LuisEdMB/SRICA**, directorio **1. Software y Hardware / 1.3 Construcción / 1.3.2 Inteligencia Artificial**. Cualquier investigador puede revisar y usar los elementos descritos en el repositorio, solo para fines de investigación.

## 2. Modelo de Detección del Ojo Humano

Para el entrenamiento del modelo que detecta la imagen del ojo de la persona, se usó YOLOv4, desarrollado por Bochkovskiy et al. (2020) (los pasos de entrenamiento para objetos específicos, se encuentran indicados en la documentación de la herramienta). Para el procesamiento de entrenamiento de las imágenes de ojos, se consideró 80% de imágenes para el entrenamiento, y 20% de imágenes para las pruebas. Así mismo, todos los pasos realizados para el entrenamiento de detección de ojos, se describen en el siguiente Google Colab: **https://colab.research.google.com/drive/1dFYuIjzrUx_7ojtJjcr2KH-nfdG67oeC?usp=sharing**.

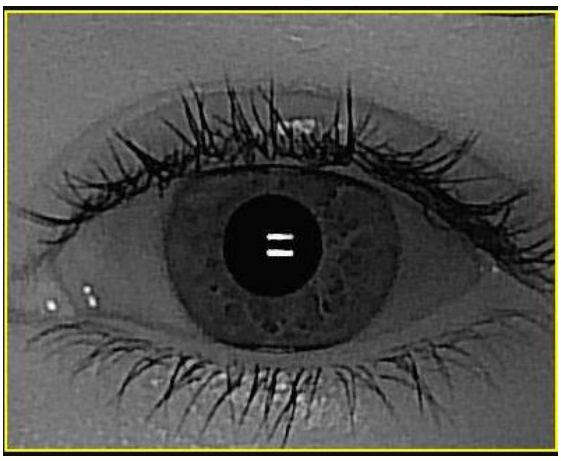
El modelo de detección del ojo humano funciona de la siguiente manera:

- Se envía la imagen con el ojo a detectar.

*Imagen original para la detección del ojo humano*

- El microservicio de detección detecta el ojo en la imagen, y se obtiene solo la imagen recortada con la ubicación del ojo identificado.

*Imagen del ojo humano detectado*



- Después de procesarse la imagen, se ejecuta el microservicio de segmentación del ojo humano.

### 3. Modelo de Segmentación del Ojo Humano

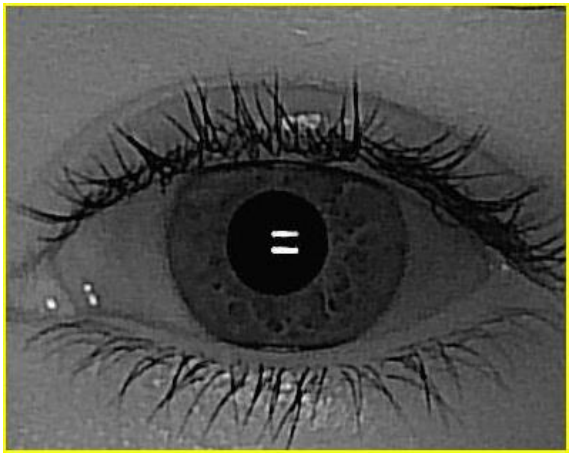
Para el entrenamiento del modelo que segmenta la imagen del ojo en tres clases: ojo, iris, y pupila, de la persona, se usó Detectron2, desarrollado por Wu et al. (2019) (los pasos de entrenamiento para objetos específicos, se encuentran indicados en la documentación de la herramienta). Para el procesamiento de entrenamiento de las

imágenes de ojos, se consideró 80% de imágenes para el entrenamiento, y 20% de imágenes para las pruebas. Así mismo, todos los pasos realizados para el entrenamiento de segmentación de ojos, se describen en el siguiente Google Colab: **https://colab.research.google.com/drive/19xpMzD2w2c6SSoflqv3la-qOkr4l_y8a?usp=sharing**.

El modelo de segmentación del ojo humano funciona de la siguiente manera:

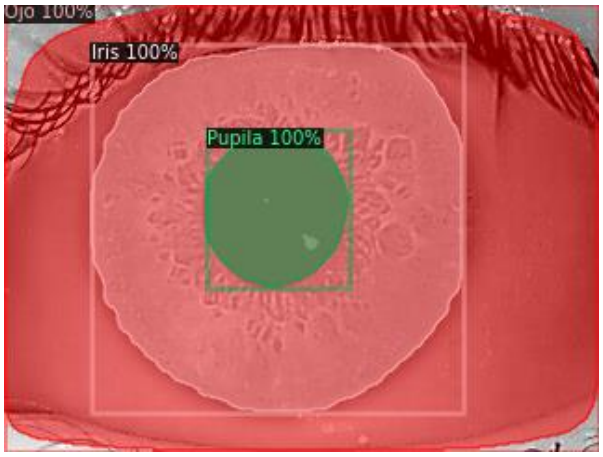
- Después que se obtenga la imagen del ojo identificado mediante el proceso de detección, se envía la imagen al microservicio de segmentación.

*Imagen del ojo humano a segmentar*



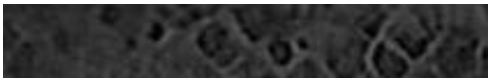
- El servicio de segmentación procesa la imagen, y segmenta la imagen en tres clases: ojo, iris, pupila.

*Imagen del ojo humano segmentado*



- El servicio de segmentación continúa con el procesamiento, y se obtiene la imagen de iris segmentada, y transformada en coordenadas polares, con tamaño 32 x 210.

*Imagen del iris humano segmentado en coordenadas polares*



- Después de procesarse la imagen, se ejecuta el microservicio de codificación y/o reconocimiento del iris humano.

## 4. Modelo de Codificación del Iris Humano

Para el modelo de codificación del iris humano, se optó por usar el modelo entrenado por Boyd et al. (2020), debido a que, el autor realizó un entrenamiento con múltiples imágenes de iris de diferentes tipos, y con demasiadas iteraciones, logrando un modelo robusto (no se realizó un entrenamiento propio debido a que, usando recursos propios, el procesamiento hubiera sido muy costoso, y demoraría mucho tiempo, además de no contar con la gran cantidad de imágenes procesadas por el autor del modelo usado). En base a esto, se procedió a usar uno de sus modelos entrenados: **ResNet50 reentrenado de ImageNet**, utilizando la capa N° **res5c_branch2c**.

El modelo de ResNet50, mediante el microservicio de codificación de iris, funciona de la siguiente manera:

- La imagen segmentada en respuesta del microservicio de segmentación, es enviada al microservicio de codificación.

*Imagen del iris humano a codificar*

- El microservicio de codificación realiza una mejora en la estructura del iris, donde, aplicando efectos blur, mejora el contraste de la imagen, y refuerza la imagen de iris mediante la aplicación de Ecualización de Histogramas.

*Imagen reforzada del iris humano*

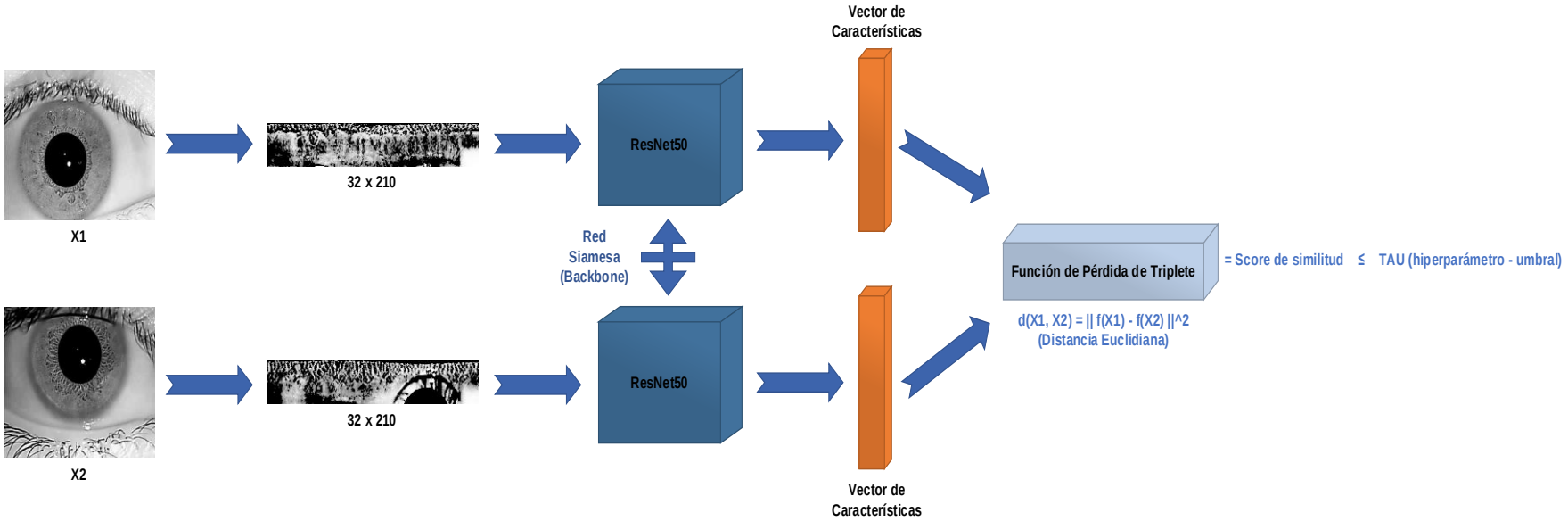
- Después de procesarse la imagen, se ejecuta el microservicio de reconocimiento del iris humano, mediante el concepto de Red Siamesa y One Shot Learning.

## 5. Modelo de Reconocimiento de Iris

Para el procesamiento del reconocimiento de iris, no es necesario el uso de un modelo de aprendizaje profundo, ya que, se usa la codificación del iris almacenada en la base de datos para poder realizar la aplicación de Red Siamesa y One Shot Learning, mediante una función matemática llamada Distancia Euclidiana, y encontrando la distancia mínima entre los vectores según el umbral definido.

Se aplica el enfoque de Red Siamesa para evitar el entrenamiento o reentrenamiento de un modelo, evitar la captura de múltiples imágenes de iris de los trabajadores, y disminuir el uso de recursos (al usar este método, se puede utilizar CPU sin algún inconveniente).

*Pipeline de reconocimiento de iris utilizando Red Siamesa y One Shot Learning*



# Anexo 8. Estándar IEC-62471:2009

## 1. Descripción

El estándar IEC-62471, en sus ediciones 2006 (modificado) y 2009 (vigente), brinda la guía para la evaluación en seguridad biológica de productos que usan lámparas o LED's, especificando el límite de exposición permitido para los productos manufacturados. Este estándar contempla lámparas, cuya longitud de onda están dentro del rango de 200nm a 3000nm (se excluyen los láseres).

Para más detalles, revisar el estándar mencionado.

## 2. Datasheet Led IR

La cámara utilizada para el proceso de captura de las imágenes de iris para cada trabajador, contiene una serie de LED's IR que permiten visualizar, con más claridad, la estructura del iris.

*Cámara utilizada para el proceso de captura de iris*

La hoja de datos (datasheet) de los LED's IR integrados a la cámara, se muestra en el sitio web del fabricante: **https://www.qt-brightek.com/datasheet/QBLP670-IR3.pdf**

## 3. Límites de Exposición

Los LED's IR, al ser de 850nm de longitud de onda, se encuentran dentro del grupo IR-A del estándar. Se está considerando tres tipos de exposición:

### 3.1. Límite de Exposición para la Córnea

La Ecuación 1 es aplicada para calcular exposiciones de luz en la córnea, con tiempo ≤ 1000s:

$$E_{IR} = \sum_{780}^{3000} E_\lambda \,.\, \Delta\lambda \leq 18000.\, t^{-0,75} \qquad W.m^{-2} \qquad (t \leq 1000s) \qquad (1)$$

, donde:

- $t = 1{,}5\ s$ (tiempo máximo de exposición para la captura de la imagen de iris, dado en segundos)
- $d = 0{,}1\ m$ (distancia, dado en metros)
- $I_e = 1{,}2\ m\mathrm{W/sr}$ o $0{,}0012\ \mathrm{W/sr}$
- $E_{IR} = E_e = \frac{I_e}{d^2} = \frac{0{,}0012\ W/sr}{(0{,}1\ m)^2} = 0{,}12\ W/m^2$

, entonces:

- $E_{IR} = 0{,}12\ W/m^2 \ \ x \ \ 12\ LED's\ IR \quad \leq \quad 18000.(1{,}5)^{-0,75}\ W/m^2$
- $E_{IR} = \mathbf{1,44\ W/m^2} \quad \leq \quad 13280{,}18\ W/m^2$

, resultando:

- $\mathbf{1,44\ W/m^2}$ por debajo del límite $13280{,}18\ W/m^2$ establecido por el estándar.

### 3.2. Límite de Exposición para la Piel

La Ecuación 2 es aplicada para calcular exposiciones de luz en la piel, con tiempo ≤ 10s (similar a la Ecuación 1):

$$E_H = \sum_{\lambda=380}^{3000} E_\lambda \,.\, \Delta\lambda \leq 20000.\, t^{-0,75} \qquad W.m^{-2} \qquad (t \leq 10s) \qquad (2)$$

, donde:

- $t = 1{,}5\ s$ (tiempo máximo de exposición para la captura de la imagen de iris, dado en segundos)
- $d = 0{,}1\ m$ (distancia, dado en metros)
- $I_e = 1{,}2\ mW/sr \quad o \quad 0{,}0012\ W/sr$
- $E_{IR} = E_e = \frac{I_e}{d^2} = \frac{0{,}0012\ W/sr}{(0{,}1\ m)^2} = 0{,}12\ W/m^2$

, entonces:

- $E_{IR} = 0{,}12\ W/m^2 \ \ x \ \ 12\ LED's\ IR \ \ \leq \ \ 20000.(1{,}5)^{-0.75}\ W/m^2$
- $E_{IR} = \mathbf{1,44\ W/m^2} \ \ \leq \ \ 14755{,}76\ W/m^2$

, resultando:

- $\mathbf{1,44\ W/m^2}$ por debajo del límite $14755{,}76\ W/m^2$ establecido por el estándar.

### 3.3. Límite de Exposición para la Retina

La Ecuación 3 es aplicada para calcular exposiciones de luz en la retina, con tiempo 10 μs ≤ t ≤ 10s:

$$L_R = \sum_{380}^{1400} L_\lambda \,.\, R(\lambda).\Delta\lambda \leq \frac{50000}{\alpha.t^{0{,}25}} \qquad W.m^{-2}.sr^{-1} \qquad (10\mu s \leq t \leq 10s) \qquad (3)$$

, donde:

- $t \ = \ 1{,}5\ s$ (tiempo máximo de exposición para la captura de la imagen de iris, dado en segundos)
- $\lambda = 850\ nm$
- $R_\lambda = 10^{\left[\frac{700-850}{500}\right]} = 10^{-0{,}3} = 0{,}50$
- $I_e = 1{,}2\ mW/sr$
- $\alpha_{min,eff} = 0{,}0017\ x\ \sqrt{\frac{1{,}5}{0{,}25}} = 0{,}0042 \ \ radianes$
- Dimension = 2,40 mm + 2,40 mm = 4,8 mm
- $L_R = I_e\ x\ \frac{R_\lambda}{\left(\frac{Dimension}{2}\right)^2} = 1{,}2\ mW/sr\ x\ \frac{0{,}50}{5{,}76}\ mm^2 = 0{,}104\ mW/mm^2/sr$

, entonces:

- $L_R = 0{,}104\ mW/mm^2/sr \ \ x \ \ 12\ LED's\ IR \ \ \leq \ \ \frac{50000}{0{,}0042\ x\ 1.5^{0{,}25}}$
- $L_R = \mathbf{1,25\ mW/mm^2/sr} \ \ \leq \ \ 1075{,}72\ x\ 10^4\ mW/mm^2/sr$

, resultando:

- $\mathbf{1,25\ mW/mm^2/sr}$ por debajo del límite $1075{,}72\ x\ 10^4\ mW/mm^2/sr$ establecido por el estándar.

## Anexo 9. Instalación en el Gobierno Regional de Tacna

### 1. Descripción

La investigación se realizó en el Gobierno Regional de Tacna, específicamente en la sede Hipólito Unanue, donde se encuentra el almacén de documentos del área de Tesorería. El ingreso a esta área es por llave de cerrojo según permiso del personal, encargado, o jefe del área. El personal de seguridad solo controla el ingreso a la sede, pero no al ambiente.

### 2. Lugar de Instalación

Como fue mencionado en el punto 1, la investigación fue realizada en la Sede Hipólito Unanue del Gobierno Regional de Tacna, ubicado en Prolongación Hipólito Unanue 1269.

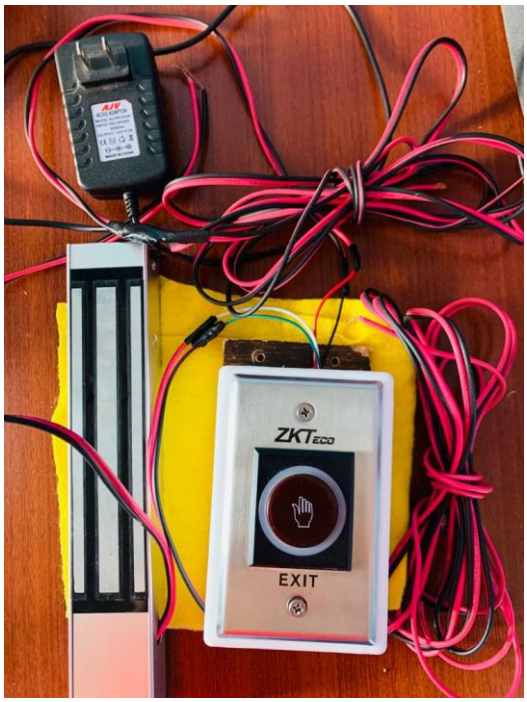
*Sede Hipólito Unanue del Gobierno Regional de Tacna*

### 3. Herramientas de Instalación

Para el proceso de instalación, se han utilizado diversas herramientas que apoyaron para este proceso. Así mismo, se prepararon los componentes electrónicos que se instalaron en el lugar, como el Botón No Touch, Electroimán, y Equipo Biométrico.

*Herramientas utilizadas para el proceso de instalación*

*Componentes electrónicos utilizados para la instalación*



## 4. Proceso de Instalación

Durante el proceso de instalación del equipo biométrico y complementos electrónicos dentro del área, se siguieron diferentes pasos para lograr el objetivo, de los cuales se muestran a continuación:

*Lugar visto desde el interior*

*Documentos del área de Tesorería*

*Medición de la puerta de acceso para colocación del electroimán y botón no touch*

*Colocación de la barra metálica para el electroimán*

*Unificación de cables eléctricos*

*Colocación de canaletas para el cableado*

*Colocación del botón no touch en el interior del área*

*Colocación y cableado del electroimán*

*Electroimán colocado en la puerta de acceso*

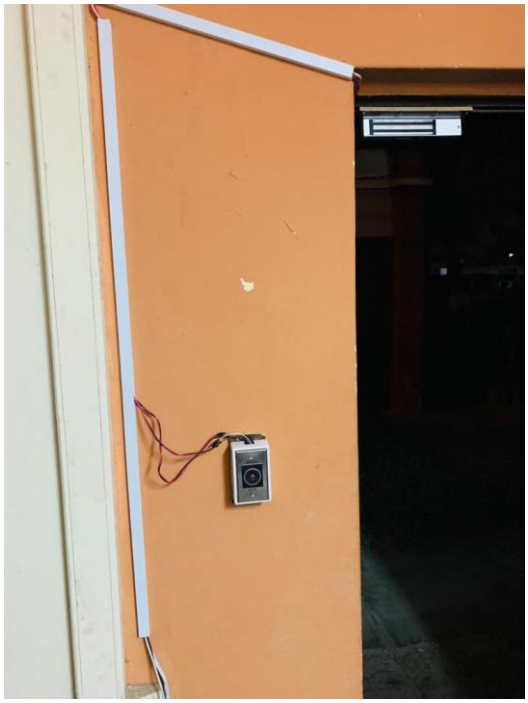
*Ubicación del equipo biométrico al exterior del área*

*Equipo biométrico interconectado al circuito del electroimán y botón no touch*

## 5. Finalización de Instalación

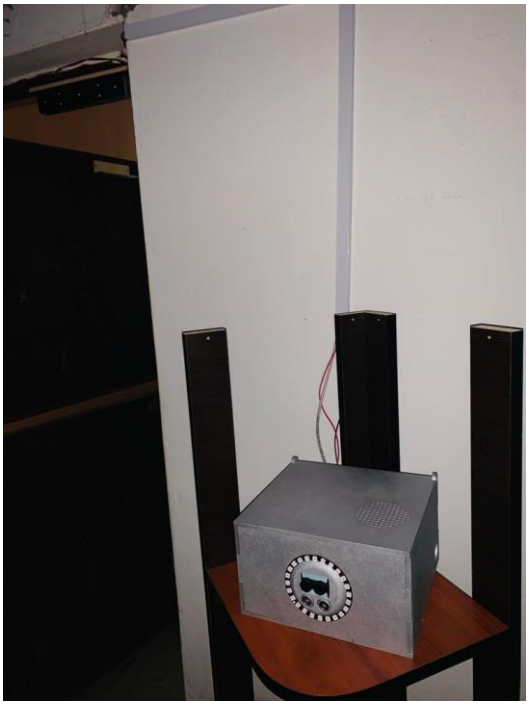
Cumpliendo el objeto de instalación, los componentes electrónicos y equipo biométrico fueron instalados con éxito en el almacén del área de Tesorería de la sede Hipólito Unanue del Gobierno Regional de Tacna, como se muestra a continuación:

*Electroimán y botón no touch instalados*



*Equipo biométrico instalado al exterior del área – vista 1*

*Equipo biométrico instalado al exterior del área – vista 2*



# Anexo 10. Proceso de control de acceso usando el sistema de reconocimiento de iris

## 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, está conformado por diversos componentes que se integran y trabajan de forma conjunta, para proporcionar un sistema de control de acceso que permita, desde el registro del personal que accederá al almacén del área de Tesorería del Gobierno Regional de Tacna, hasta el respectivo acceso al lugar físico protegido, considerando el registro de eventos de la configuraciones y accesos concedidos o denegados. **Los componentes que integran el SRICA, ya han sido expuestos en los anexos anteriores**.

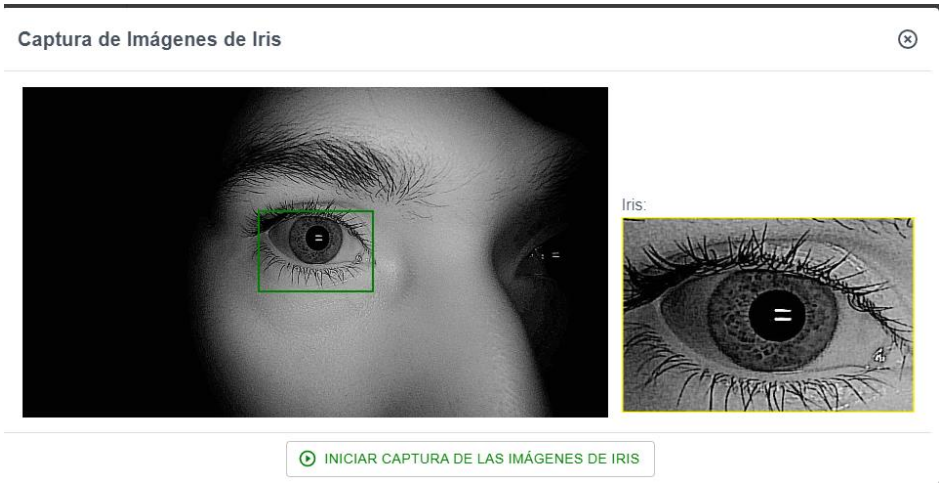
En los siguientes puntos, se detallarán las etapas que SRICA ejecuta y procesa para realizar el control de acceso, de los cuales, comprenden: Identificación, Autenticación, Autorización, Trazabilidad (Responsabilidad).

## 2. Registro del Personal en el Sistema de Reconocimiento de Iris

En primera instancia, el personal que accederá al almacén del área de Tesorería del Gobierno Regional de Tacna, debe ser registrado en el sistema web proporcionado por SRICA, capturando la imagen del iris de la persona (el iris capturado será la llave de acceso al almacén), y algunos datos básicos del personal.

*Registro del personal en el sistema*

*Captura de la imagen de iris del personal en el sistema*



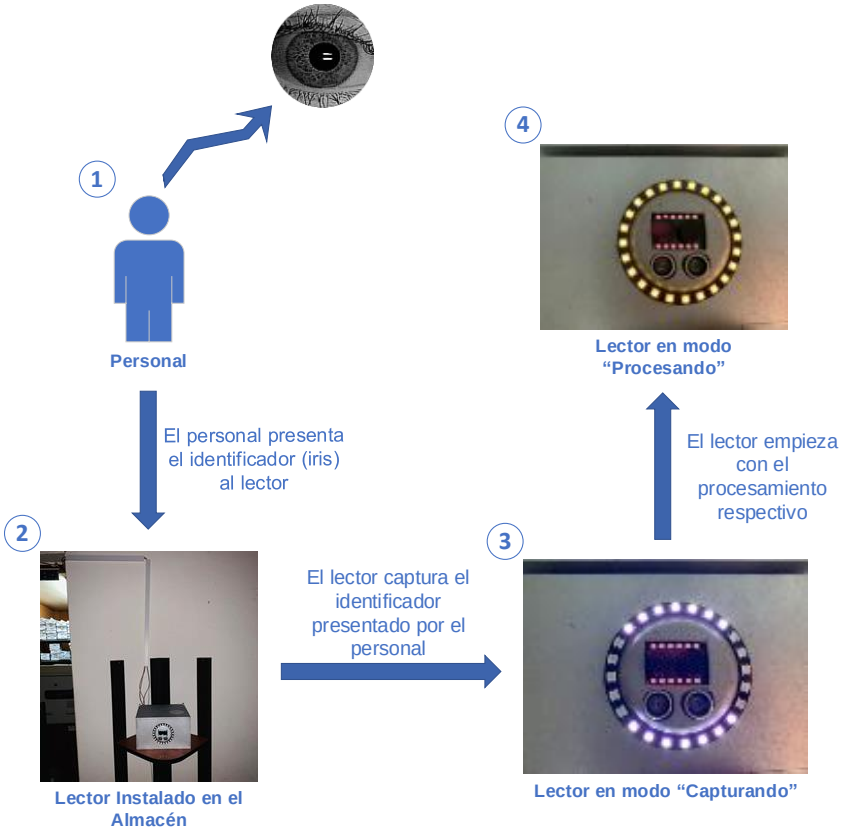

Los datos capturados del personal son almacenados en la base de datos para su posterior uso durante el acceso al almacén del área de Tesorería por el mismo personal registrado. Cabe mencionar que, las actividades de registro del personal son guardadas para su respectiva visualización en los reportes de bitácora (trazabilidad) que proporciona el sistema.

### 3. Etapa “Identificación” en el Sistema de Reconocimiento de Iris

Una vez registrado el personal en el sistema, éste puede ingresar al almacén del área de Tesorería mediante el equipo lector instalado en la puerta de acceso del espacio físico protegido, siendo este lector el encargado de capturar la imagen de iris del personal, para su posterior procesamiento y autorización de acceso.

El personal se presenta ante el lector instalado para proporcionar su identificación, que estaría representada por el iris humano, siendo éste el respectivo identificador individual que cumplirá el rol de llave de acceso.

*Flujo de la etapa "Identificación" durante el control de acceso utilizando el sistema*

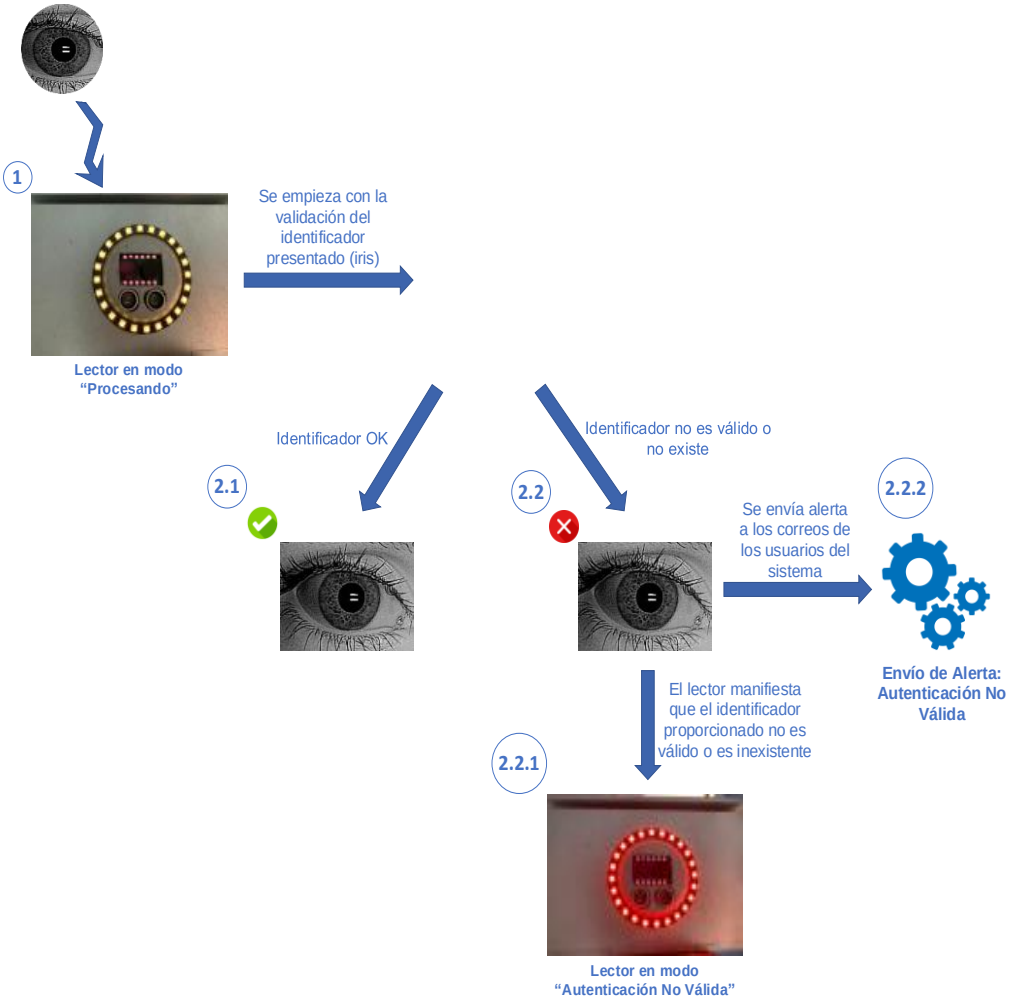



## 4. Etapa "Autenticación" en el Sistema de Reconocimiento de Iris

Según el identificador presentado por el personal, que sería el iris humano, el sistema verificará y comprobará si realmente la persona que se presentó ante el lector, y proporcionó su identificación, es quien dice ser. Para ello, el sistema ejecuta los respectivos procesos para lograr la autenticidad de la persona que intenta acceder al almacén del área de Tesorería.

Siendo los supuestos resultados de la validación del identificador (identificador correcto, identificador no válido, identificador no existe), se procede, o no, con la respectiva otorgación de los permisos de accesos al espacio físico protegido. Para cualquier resultado diferente a una autenticación correcta, se envía un correo de alerta a los correos de los usuarios del sistema.

*Flujo de la etapa "Autenticación" durante el control de acceso utilizando el sistema*

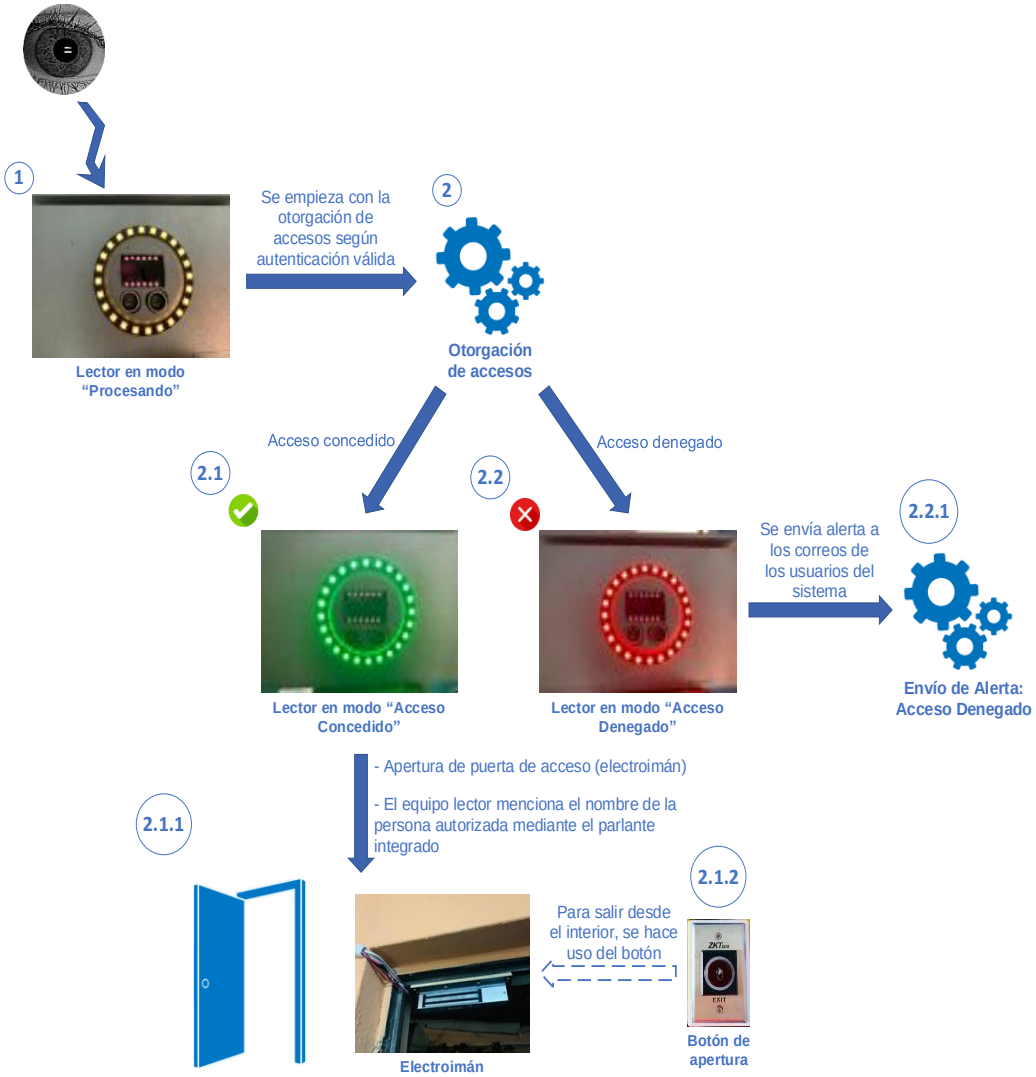



## 5. Etapa "Autorización" en el Sistema de Reconocimiento de Iris

Según la validación y comprobación del identificador presentado por el personal, que sería el iris humano, donde el resultado fue una autenticación correcta, el sistema procederá a autorizar el acceso correspondiente al almacén del área de Tesorería.

Siendo los supuestos resultados de la otorgación de los permisos de accesos (autorizado, no autorizado), el equipo lector, conectado al electroimán instalado en la puerta de acceso, procede, o no, con la apertura de la puerta de acceso del espacio físico protegido. Para cualquier resultado diferente a un acceso concedido, se envía un correo de alerta a los correos de los usuarios del sistema.

*Flujo de la etapa "Autorización" durante el control de acceso utilizando el sistema*




Cabe señalar que, para salir desde el interior del almacén del área de Tesorería cuando la puerta de este espacio físico esté cerrada, se hace uso del botón de apertura, el cual, mediante circuito, está conectado con el electroimán (este evento no es registrado en el sistema).

## 6. Etapa "Trazabilidad" en el Sistema de Reconocimiento de Iris

Durante el proceso de control de acceso al almacén del área de Tesorería, y durante el registro del personal en el sistema, SRICA realiza el registro de eventos de auditoría de las acciones realizadas, siendo mostradas visualmente mediante reportes. Esta acción de registro de eventos del sistema, se realiza para tener conocimiento de las acciones realizadas, como: intentos de accesos no autorizados al almacén, accesos autorizados

al almacén, identificadores válidos o no válidos, modificación de datos o de permisos del personal, configuraciones, acciones del sistema, y errores, registrando la fecha y el actor de la acción.

*Reporte de acciones del sistema*

**Reporte de Acciones del Sistema**

Fecha Inicio 01/03/2022 Fecha Fin 20/03/2022 GENERAR REPORTE

| Nombres | Apellidos | Rol | Modulo | Recurso | Tipo de Evento | Acción | Descripción de Acción | Fecha Acción |
|---|---|---|---|---|---|---|---|---|
| SEG | ADMIN SEG | Administrador | Reporte | Reporte de Acción de Equipos Biométricos | Correcto | Generación de Reporte | Generación correcta del reporte. | 18/03/2022 16:20:01 |
| SEG | ADMIN SEG | Administrador | Reporte | Reporte de Acción del Sistema | Correcto | Generación de Reporte | Generación correcta del reporte. | 18/03/2022 10:20:01 |
| Usu Sub Gerencia | OETES | Usuario Básico | Reporte | Reporte de Acción de Equipos Biométricos | Correcto | Generación de Reporte | Generación correcta del reporte. | 15/03/2022 15:27:22 |
| Usu Sub Gerencia | OETES | Usuario Básico | Personal de la Empresa | Personal de la Empresa | Correcto | Registro de Datos | Personal registrado correctamente. | 15/03/2022 10:12:47 |
| Jefatura | OETES | Usuario Básico | Personal de la Empresa | Personal de la Empresa | Correcto | Registro de Datos | Personal registrado correctamente. | 14/03/2022 11:31:10 |
| Jefatura | OETES | Usuario Básico | Personal de la Empresa | Personal de la Empresa | Validación | Registro de Datos | Debe capturar la respectiva imagen de iris para el personal | 14/03/2022 11:30:35 |

*Reporte de acciones durante el control de acceso utilizando el sistema*

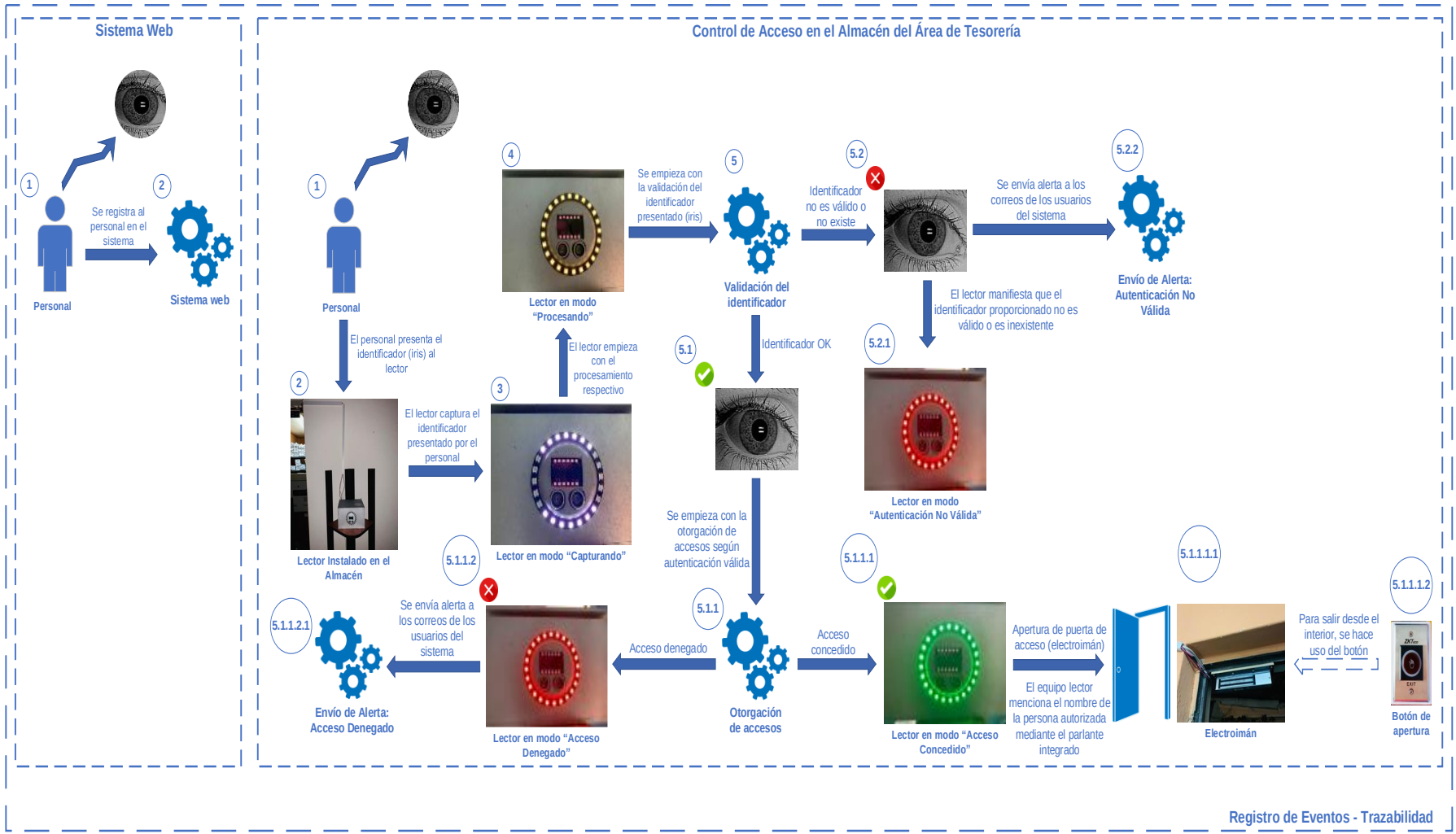
**Reporte de Acciones de Equipos Biométricos**

Fecha Inicio 01/03/2022 Fecha Fin 20/03/2022 GENERAR REPORTE

| DNI | Nombres | Apellidos | Sede | Área | Equipo Biométrico | Resultado de Acceso | Descripción del Resultado | Fecha Acceso |
|---|---|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | Hipólito Unanue | Almacén del Área de Tesorería | SRI-EQUI-BIO-01 | Concedido | Acceso concedido. | 17/03/2022 16:45:57 |
| [redacted] | [redacted] | [redacted] | Hipólito Unanue | Almacén del Área de Tesorería | SRI-EQUI-BIO-01 | Concedido | Acceso concedido. | 17/03/2022 16:42:36 |
| -- | -- | -- | Hipólito Unanue | Almacén del Área de Tesorería | SRI-EQUI-BIO-01 | Denegado | Hubo un intento de acceso por personal no registrado en el sistema. | 17/03/2022 11:25:12 |
| -- | -- | -- | Hipólito Unanue | Almacén del Área de Tesorería | SRI-EQUI-BIO-01 | Denegado | Hubo un intento de acceso por personal no registrado en el sistema. | 15/03/2022 17:03:49 |
| [redacted] | [redacted] | [redacted] | Hipólito Unanue | Almacén del Área de Tesorería | SRI-EQUI-BIO-01 | Concedido | Acceso concedido. | 15/03/2022 11:10:25 |

## 7. Proceso Técnico de Control de Acceso con el Uso del Sistema de Reconocimiento de Iris

*Proceso técnico de control de acceso con el uso del Sistema de Reconocimiento de Iris*



## 8. Proceso Propuesto de Control de Acceso con el Uso del Sistema de Reconocimiento de Iris

*Manual de procedimiento de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Manual de Procedimientos |
| --- |
| *Control de Acceso al Almacén del Área de Tesorería con el Uso del Sistema de Reconocimiento de Iris* |
| Emite: Luis Eduardo Mamani Bedregal (Director del Proyecto) |

**1. Propósito**

Determinar el procedimiento de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con el uso del Sistema de Reconocimiento de Iris.

**2. Alcance**

El presente manual contempla el procedimiento de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna ubicado en la Sede Hipólito Unanue, mediante el uso del Sistema de Reconocimiento de Iris, controlando el acceso de personas al lugar nombrado, cuyo acceso es dado al trabajador correspondiente por indicación del jefe o encargado del área de Tesorería, y gestionado por el área de Seguridad.

**3. Responsabilidades**

**3.1. Jefe del Área de Tesorería**

Indicar a *El Trabajador* que accede al almacén, y solicitar la gestión del acceso correspondiente a *Personal del Área de Seguridad*.

**3.2. Encargado del Área de Tesorería**

Indicar a *El Trabajador* que accede al almacén, y solicitar la gestión del acceso correspondiente a *Personal del Área de Seguridad (reemplaza* a *Jefe del Área de Tesorería* cuando éste no se encuentre presente).

**3.3. Personal del Área de Seguridad**

Gestionar el acceso de *El Trabajador* en el sistema web de control de accesos para que éste pueda acceder al almacén.

**3.4. El Trabajador**

Acceder al almacén según el acceso otorgado.

**4. Procedimiento**

*Sede Principal / Central del Gobierno Regional de Tacna*

| (#) | (Quién) | (Actividad) |
|---|---|---|
| 4.1 | -- | Si se encuentra presente *Jefe del Área de Tesorería*, ir a 4.1.1, caso contrario, ir a 4.2. |
| 4.1.1 | Jefe del Área de Tesorería | Requiere de información y/o documentos. |
| 4.1.2 | | Indica a *El Trabajador* que accederá al almacén para buscar y obtener la información y/o documentos requeridos. |
| 4.1.3 | | Solicita a *Personal del Área de Seguridad* la gestión de *El Trabajador* para el acceso correspondiente (ir a 4.3). |
| 4.2 | -- | Si no se encuentra presente *Jefe del Área de Tesorería*, ir a 4.2.1, caso contrario, ir a 4.1. |
| 4.2.1 | Encargado del Área de Tesorería | Requiere de información y/o documentos. |
| 4.2.2 | | Indica a *El Trabajador* que accederá al almacén para buscar y obtener la información y/o documentos requeridos. |
| 4.2.3 | | Solicita a *Personal del Área de Seguridad* la gestión de *El Trabajador* para el acceso correspondiente (ir a 4.3). |
| 4.3 | Personal del Área de Seguridad | Gestiona el acceso de *El Trabajador* en el sistema web de control de accesos. |
| 4.4 | | Solicita a *El Trabajador* los datos para el acceso: DNI, nombres, iris. |
| 4.5 | El Trabajador | Manifiesta los datos necesarios solicitados por *Personal del Área de Seguridad*. |

| | |
|---|---|
| 4.5.1 | Si tiene el acceso correspondiente, ir a 4.6. |
| 4.5.2 | Si no tiene el acceso correspondiente, ir a 4.3. |

*Sede Hipólito Unanue del Gobierno Regional de Tacna*

| (#) | (Quién) | (Actividad) |
|---|---|---|
| 4.6 | | Accede al almacén con el uso del identificador (iris) ante el controlador instalado en la puerta de acceso. |
| 4.6.1 | | Si el acceso es correcto, ir a 4.7. |
| 4.6.2 | | Si el acceso es denegado, ir a 4.3. |
| 4.7 | | Realiza las operaciones correspondientes dentro del almacén. |
| 4.7.1 | | Si las operaciones han concluido, ir a 4.8. |
| 4.7.2 | | Si las operaciones no han concluido, ir a 4.7. |
| 4.8 | El Trabajador | Sale del almacén con el resultado de las operaciones correspondientes. |
| 4.8.1 | | Si la puerta de acceso se encuentra cerrada, ir a 4.9. |
| 4.8.2 | | Si la puerta de acceso se encuentra abierta, ir a 4.10. |
| 4.9 | | Acciona el botón de apertura para abrir la puerta de acceso y salir de lugar (ir a 4.10). |
| 4.10 | | Cierra la puerta de acceso con el uso del equipo electroimán del marco de la puerta. |
| 4.10.1 | | Si la puerta de acceso se encuentra asegurada, ir a 4.11. |
| 4.10.2 | | Si la puerta de acceso no se encuentra asegurada, ir a 4.10. |

*Sede Principal / Central del Gobierno Regional de Tacna*

| (#) | (Quién) | (Actividad) |
|---|---|---|
| 4.11 | El Trabajador | Entrega la información y/o documentos a *Jefe del Área de Tesorería* o *Encargado del Área de Tesorería*. |

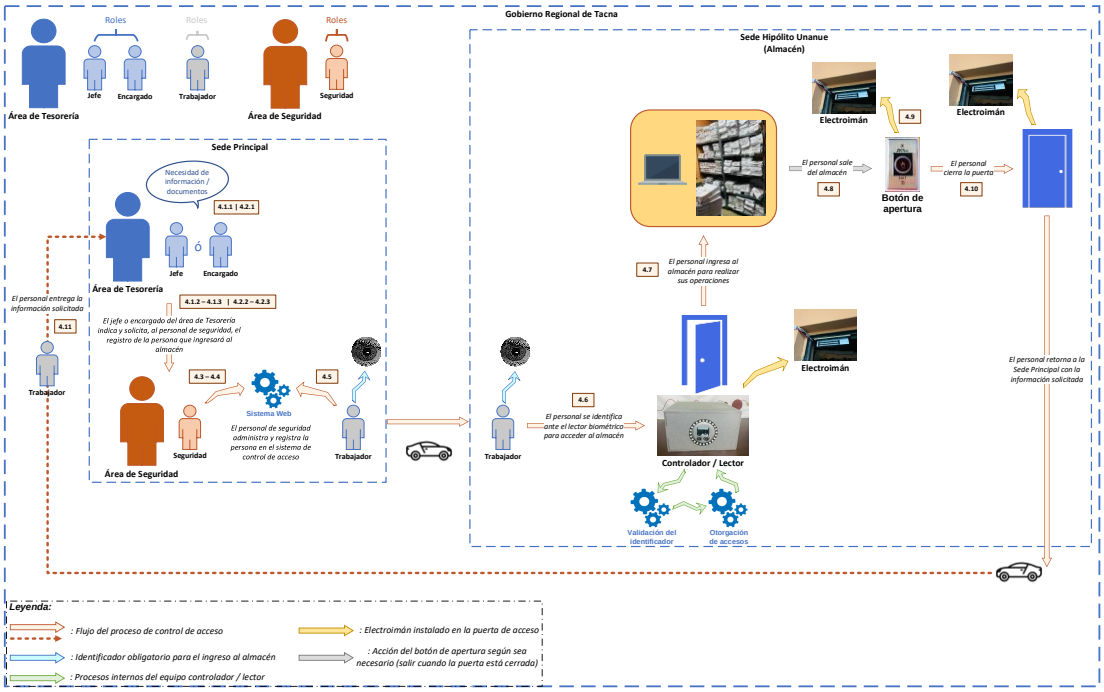
**5. Vocabulario y Siglas**

| Término | Definición |
|---|---|
| Sistema Web de Control de Accesos | Plataforma web que utiliza el *Personal del Área de Seguridad* para gestionar el acceso de *El Trabajador* que ingresa al almacén del área de Tesorería. |

| | |
|---|---|
| Identificador de Acceso | Identificador utilizado por *El Trabajador* para acceder al almacén del área de Tesorería, el cual es representado por el iris humano del mismo. |
| Controlador de Accesos | Equipo instalado en la puerta de acceso del almacén del área de Tesorería que controla el acceso de personas solo autorizadas. |
| Botón de Apertura | Dispositivo instalado en el interior del almacén del área de Tesorería que permite abrir la puerta de acceso si éste se encuentra cerrada, para la respectiva salida de *El Trabajador*. |
| Equipo Electroimán | Dispositivo instalado en el marco de la puerta de acceso del almacén del área de Tesorería que permite asegurar y reforzar la entrada. |

## 6. Anexos

*Proceso propuesto de control de acceso con el uso del Sistema de Reconocimiento de Iris*




## 7. Referencias

Proceso actual de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna (sin código o referencia pública).

# Anexo 11. Análisis de datos generados por el sistema de reconocimiento de iris para control de acceso

## 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, dentro de sus procedimientos internos relacionados a los diversos servicios lógicos que contiene, provee la capacidad de realización de registros de cualquier acción y/o actividad generada durante el proceso de control de acceso, capturando y registrando datos esenciales que, de alguna manera, fueron utilizados para la evaluación del proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna mediante el uso del Sistema de Reconocimiento de Iris propuesto.

En el siguiente apartado, se visualizarán los diversos datos capturados y/o registrados que fueron de utilidad para el análisis y evaluación del proceso de control de acceso mediante la solución propuesta.

## 2. Análisis de Datos del Sistema de Reconocimiento de Iris para Control de Acceso

El personal del área de Tesorería, en total 15 personas, participaron durante la evaluación del proceso de control de acceso utilizando el Sistema de Reconocimiento de Iris, durante tres semanas, donde, se solicitó al área de Tesorería su activa participación para la respectiva recopilación de datos.

Para lograr la evaluación del proceso de control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna con el uso del Sistema de Reconocimiento de Iris, se considera los datos registrados por la funcionalidad de “Trazabilidad” que la presente solución realiza.

### 2.1. Participación del personal durante el proceso de control de acceso

En la siguiente tabla, se visualiza al personal total, y los días de participación, según datos recopilados del Sistema de Reconocimiento de Iris. Cabe señalar que, la participación individual de cada persona, fue de manera intercalada y mínima, durante el día laboral, debido a que el proceso de control de acceso depende de la necesidad de información que el área de Tesorería, u otras áreas, requieran.

*Participación del área de Tesorería durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Día \ Personal | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 | P10 | P11 | P12 | P13 | P14 | P15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D1 | | | | | | | | | | | | X | | | X |
| D2 | | X | | | | | | | | X | | | | | |
| D3 | | | | | | | | | | | | | | | |
| D4 | | | | X | | | X | | | | X | | | | |
| D5 | X | | X | | | | | | | | | | | | |
| D6 | | | | X | | | | | | | X | | | | |
| D7 | | | | | | | | | | | | | | | |
| D8 | | | | | | X | | | | | | | X | | |
| D9 | | | | | X | | | X | | | | X | | | |
| D10 | | | | | | X | | | | X | | | | | |
| D11 | | X | | | | | | | X | | | | | | X |
| D12 | | | | | | | | | | | | | | | |
| D13 | X | | X | | X | | | | | | | | | | |
| D14 | | | | | | | | X | | | | | X | X | |
| D15 | | | | | | | | | | | | | | | |
| Total Días por Personal | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 |

Según la tabla, se visualiza a la totalidad del personal “P” evaluado, y los días “D” de participación, donde se puede apreciar que el personal ha participado, en su totalidad, durante la evaluación del proceso de control de acceso mediante el uso del Sistema de Reconocimiento de Iris propuesto, empleando de 1 ~ 2 días de participación durante los 15 días de evaluación.

**2.2. Tiempo de registro de asignación de accesos**

Según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza a la totalidad del personal “P” evaluado, y los tiempos de registro de asignación de accesos, en el sistema web de control de accesos, para el acceso correspondiente al almacén del área de Tesorería.

*Tiempo promedio de asignación de accesos al personal durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Personal | Tiempo de Asignación de Accesos (segundos) |
|---|---|
| P1 | 58,541 |
| P2 | 61,024 |
| P3 | 61,699 |
| P4 | 55,936 |
| P5 | 59,620 |
| P6 | 58,769 |
| P7 | 63,596 |
| P8 | 55,621 |
| P9 | 62,805 |
| P10 | 58,839 |
| P11 | 64,771 |
| P12 | 59,545 |
| P13 | 60,095 |
| P14 | 62,603 |
| P15 | 62,849 |
| Total promedio | 60,420 |

Según la tabla, se verifica el tiempo que demoró el registro de asignación de accesos al personal en el sistema web de control de accesos para el respectivo acceso al almacén del área de Tesorería, logrando un promedio total de 60,420 segundos.

**2.3. Tiempo de registro de asignación de accesos**

Según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza a la totalidad del personal “P” evaluado, los días “D” donde el personal ha participado en el proceso de control de acceso, y la cantidad de apertura de puerta del

almacén del área de Tesorería, debido al uso obligatorio del identificador. Así mismo, se solicitó al personal la realización de varios accesos para la apertura de la puerta con el fin de recopilar más información.

*Cantidad de apertura de puerta durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Personal | Día(s) | Cantidad de Apertura de Puerta | Subtotal |
|---|---|---|---|
| P1 | D5 | 2 | 3 |
| | D13 | 1 | |
| P2 | D2 | 4 | 7 |
| | D11 | 3 | |
| P3 | D5 | 3 | 5 |
| | D13 | 2 | |
| P4 | D4 | 3 | 6 |
| | D6 | 3 | |
| P5 | D9 | 1 | 4 |
| | D13 | 3 | |
| P6 | D8 | 3 | 6 |
| | D10 | 3 | |
| P7 | D4 | 2 | 2 |
| P8 | D9 | 3 | 5 |
| | D14 | 2 | |
| P9 | D11 | 3 | 3 |
| P10 | D2 | 3 | 6 |
| | D10 | 3 | |
| P11 | D4 | 2 | 4 |
| | D6 | 2 | |
| P12 | D1 | 3 | 5 |
| | D9 | 2 | |
| P13 | D8 | 3 | 5 |
| | D14 | 2 | |
| P14 | D14 | 2 | 2 |
| P15 | D1 | 2 | 5 |
| | D11 | 3 | |
| | | **Total cantidad de apertura de puerta** | 68 |
| | | ***Cantidad según reporte de apertura de puerta – equipo biométrico lector*** | *68* |
| | | ***Frecuencia de uso del identificador*** | *100 %* |

Según la tabla, se verifica el porcentaje de uso del identificador para lograr el acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, siendo del 100%, determinando el uso obligatorio del identificador.

### 2.4. Tiempo de autenticación

Según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza a la totalidad del personal “P” evaluado, los días “D” donde el personal ha participado en el proceso de control de acceso, y los tiempos (en segundos) que el proceso de autenticación ha demorado (validación y comprobación de la identidad de la persona, desde el identificador ya capturado, hasta la respectiva comprobación del identificador).

*Tiempo promedio de autenticación del personal durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Personal | Día(s) | Tiempo Autenticación Registrada (segundos) | Total Tiempo Promedio (segundos) | Total Tiempo Promedio Esperado (segundos) |
|---|---|---|---|---|
| P1 | D5 | 4,539 | 4,446 | 1,000 ~ 4,000 |
| | | 5,095 | | |
| | D13 | 3,703 | | |
| P2 | D2 | 3,743 | 3,852 | |
| | | 3,806 | | |
| | | 4,079 | | |
| | | 3,909 | | |
| | D11 | 3,954 | | |
| | | 3,928 | | |
| | | 3,546 | | |
| P3 | D5 | 3,765 | 3,804 | |
| | | 3,834 | | |
| | | 4,011 | | |
| | D13 | 3,809 | | |
| | | 3,602 | | |
| P4 | D4 | 4,627 | 4,501 | |
| | | 3,894 | | |
| | | 5,018 | | |
| | D6 | 4,448 | | |
| | | 4,144 | | |

| | | | | |
|---|---|---|---|---|
| | | 4,876 | | |
| P5 | D9 | 3,886 | 3,853 | |
| | D13 | 3,664 | | |
| | | 4,166 | | |
| | | 3,695 | | |
| P6 | D8 | 4,005 | 4,670 | |
| | | 4,740 | | |
| | | 4,673 | | |
| | D10 | 5,412 | | |
| | | 5,249 | | |
| | | 3,943 | | |
| P7 | D4 | 3,776 | 3,817 | |
| | | 3,858 | | |
| P8 | D9 | 4,516 | 4,494 | |
| | | 4,140 | | |
| | | 4,842 | | |
| | D14 | 5,082 | | |
| | | 3,891 | | |
| P9 | D11 | 4,046 | 3,749 | |
| | | 3,756 | | |
| | | 3,444 | | |
| P10 | D2 | 5,117 | 4,555 | |
| | | 4,328 | | |
| | | 5,264 | | |
| | D10 | 4,059 | | |
| | | 4,248 | | |
| | | 4,316 | | |
| P11 | D4 | 3,713 | 3,813 | |
| | | 3,910 | | |
| | D6 | 3,788 | | |
| | | 3,839 | | |
| P12 | D1 | 3,862 | 3,837 | |
| | | 3,804 | | |
| | | 4,009 | | |
| | D9 | 3,735 | | |
| | | 3,773 | | |
| P13 | D8 | 3,813 | 4,611 | |
| | | 4,962 | | |
| | | 5,043 | | |

| | | | | |
|---|---|---|---|---|
| | D14 | 3,812 | | |
| | | 5,423 | | |
| P14 | D14 | 3,775 | 3,736 | |
| | | 3,697 | | |
| P15 | D1 | 3,772 | 4,271 | |
| | | 4,587 | | |
| | D11 | 5,218 | | |
| | | 3,658 | | |
| | | 4,119 | | |

Según la tabla, se verifica el tiempo promedio de autenticación que obtuvo cada personal durante su participación en el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, donde, estableciendo un rango de 1,000 ~ 4,000 segundos según requerimiento no funcional, se contempla que algunos procesos demoraron más de lo esperado.

**2.5. % de acierto en la autenticación**

Según modelo de Deep Learning utilizado para el proceso de reconocimiento (autenticación) del iris del personal, donde, aplicando el concepto de One Shot Learning y Redes Siamesas, se contemplan los siguientes datos:

- Siendo la distancia (similitud) de 0,000 ~ 2,999, con porcentaje de acierto entre 100% ~ 85%.
- Siendo la distancia (similitud) de 3,000 ~ 5,999, con porcentaje de acierto entre 85% ~ 75%.
- Siendo la distancia (similitud) de 6,000 ~ 8,999, con porcentaje de acierto entre 75% ~ 65%.
- Siendo la distancia (similitud) de 9,000 ~ 11,999, con porcentaje de acierto entre 65% ~ 55%.
- Siendo la distancia (similitud) de 12,000 ~ 14,999, con porcentaje de acierto entre 55% ~ 45%.
- Siendo la distancia (similitud) de 15,000 ~ 17,999, con porcentaje de acierto entre 45% ~ 35%.
- Siendo la distancia (similitud) de 18,000 ~ 20,999, con porcentaje de acierto entre 35% ~ 25%.

- Siendo la distancia (similitud) de 21,000 ~ 23,999, con porcentaje de acierto entre 25% ~ 15%
- Siendo la distancia (similitud) de 24,000 ~ 26,000, con porcentaje de acierto entre 15% ~ 0%.

; donde el modelo de Deep Learning utilizado, resulta entre un valor de 0,000 a 26,000 de distancia de similitud, indicando el valor 8,000 (es decir, 70%) como umbral.

Por ende, según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza a la totalidad del personal “P” evaluado, los días “D” donde el personal ha participado en el proceso de control de acceso, y los porcentajes de autenticación.

*Porcentaje de autenticación del personal durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| Personal | Día(s) | Puntaje Autenticación (distancia - similitud) | Total Promedio Autenticación (distancia - similitud) | Porcentaje Autenticación | Umbral |
|---|---|---|---|---|---|
| P1 | D5 | 6,667 | 5,686 | 76,20% | *≤ 8,000 distancia o ≥ 70% porcentaje* |
| | | 4,712 | | | |
| | D13 | 5,679 | | | |
| P2 | D2 | 6,695 | 6,206 | 74,40% | |
| | | 7,408 | | | |
| | | 5,229 | | | |
| | | 4,911 | | | |
| | D11 | 6,874 | | | |
| | | 5,062 | | | |
| | | 7,26 | | | |
| P3 | D5 | 5,487 | 4,703 | 79,10% | |
| | | 4,156 | | | |
| | | 5,457 | | | |
| | D13 | 4,103 | | | |
| | | 4,314 | | | |
| P4 | D4 | 6,357 | 6,287 | 74,26% | |
| | | 5,729 | | | |
| | | 7,318 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | D6 | 6,742 | | | |
| | | 6,962 | | | |
| | | 4,613 | | | |
| P5 | D9 | 5,334 | 5,569 | 76,55% | |
| | D13 | 5,132 | | | |
| | | 4,465 | | | |
| | | 7,346 | | | |
| P6 | D8 | 6,047 | 6,026 | 74,98% | |
| | | 4,92 | | | |
| | | 5,214 | | | |
| | D10 | 7,237 | | | |
| | | 5,71 | | | |
| | | 7,027 | | | |
| P7 | D4 | 6,899 | 5,996 | 75,01% | |
| | | 5,092 | | | |
| P8 | D9 | 7,249 | 6,440 | 73,48% | |
| | | 6,898 | | | |
| | | 5,643 | | | |
| | D14 | 6,698 | | | |
| | | 5,713 | | | |
| P9 | D11 | 7,073 | 7,050 | 71,78% | |
| | | 6,747 | | | |
| | | 7,329 | | | |
| P10 | D2 | 6,42 | 6,790 | 72,75% | |
| | | 6,337 | | | |
| | | 7,002 | | | |
| | D10 | 7,266 | | | |
| | | 6,991 | | | |
| | | 6,724 | | | |
| P11 | D4 | 6,442 | 6,763 | 72,76% | |
| | | 6,933 | | | |
| | D6 | 7,36 | | | |
| | | 6,316 | | | |
| P12 | D1 | 7,228 | 6,702 | 72,30% | |
| | | 7,158 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | 5,603 | | | |
| | D9 | 7,381 | | | |
| | | 6,142 | | | |
| P13 | D8 | 6,009 | 6,088 | 74,96% | |
| | | 7,495 | | | |
| | | 6,288 | | | |
| | D14 | 5,464 | | | |
| | | 5,185 | | | |
| P14 | D14 | 5,323 | 5,590 | 76,51% | |
| | | 5,857 | | | |
| P15 | D1 | 6,283 | 5,830 | 75,45% | |
| | | 5,965 | | | |
| | D11 | 5,481 | | | |
| | | 5,067 | | | |
| | | 6,353 | | | |

Según la tabla, se verifica el porcentaje de acierto que obtuvo cada personal durante su participación en el control de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, donde:

- La cantidad de aciertos al 100% de casos evaluados, indica que el personal obtuvo los accesos correspondientes sin ningún inconveniente, donde la totalidad de porcentajes y aciertos cumplieron con el umbral indicado.
- La cantidad de aciertos representa a la misma cantidad indicada en la tabla de cantidad de apertura de puerta de acceso, validando que el personal no recibió accesos erróneos de otra persona (falsos positivos).

### 2.6. Complejidad de seguridad del identificador

Según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza a la totalidad del personal “P” evaluado, los días “D” donde el personal ha participado en el proceso de control de acceso, y la diferencia (distancia - similitud) entre cada identificador del personal.

*Complejidad de seguridad del identificador en el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| | | Personal (distancia – similitud del identificador) | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Personal | Día(s) | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 | P10 | P11 | P12 | P13 | P14 | P15 |
| P1 | D5 | **6,667** | 22,574 | 16,29 | 20,229 | 15,886 | 21,471 | 20,763 | 21,286 | 22,471 | 23,621 | 20,153 | 20,671 | 15,661 | 15,451 | 21,933 |
| | | **4,712** | 18,236 | 19,85 | 19,986 | 20,102 | 17,736 | 20,93 | 15,139 | 15,013 | 21,217 | 23,121 | 20,235 | 15,405 | 16,158 | 21,72 |
| | D13 | **5,679** | 19,394 | 22,573 | 20,985 | 22,682 | 17,415 | 16,411 | 17,649 | 18,714 | 18,334 | 15,795 | 18,871 | 20,151 | 17,633 | 19,399 |
| P2 | D2 | 15,027 | **6,695** | 18,101 | 21,588 | 19,809 | 17,956 | 23,834 | 18,346 | 15,215 | 21,722 | 22,435 | 16,352 | 22,671 | 22,083 | 22,696 |
| | | 20,624 | **7,408** | 19,294 | 17,78 | 20,087 | 20,928 | 19,071 | 17,728 | 19,937 | 21,195 | 15,697 | 15,556 | 20,47 | 21,408 | 17,3 |
| | | 19,687 | **5,229** | 22,748 | 20,25 | 19,729 | 19,84 | 16,837 | 16,191 | 15,486 | 20,129 | 23,58 | 20,358 | 17,106 | 23,37 | 17,813 |
| | | 17,163 | **4,911** | 18,86 | 18,88 | 19,685 | 15,843 | 22,371 | 19,043 | 17,221 | 19,786 | 21,44 | 23,739 | 17,307 | 20,345 | 19,14 |
| | D11 | 16,554 | **6,874** | 17,591 | 18,419 | 22,622 | 21,846 | 21,931 | 23,666 | 20,624 | 19,816 | 20,454 | 20,931 | 23,564 | 23,804 | 16,389 |
| | | 15,958 | **5,062** | 18,661 | 18,833 | 16,027 | 15,814 | 21,831 | 15,688 | 22,934 | 18,818 | 20,045 | 18,294 | 17,533 | 23,238 | 22,382 |
| | | 22,111 | **7,26** | 20,973 | 17,611 | 19,332 | 18,427 | 20,14 | 20,907 | 22,577 | 20,986 | 20,493 | 22,984 | 19,303 | 19,669 | 15,416 |
| P3 | D5 | 20,825 | 16,916 | **5,487** | 20,767 | 16,475 | 15,425 | 18,91 | 17,947 | 18,552 | 15,174 | 16,795 | 21,925 | 22,029 | 16,679 | 23,577 |
| | | 17,184 | 22,206 | **4,156** | 16,701 | 22,578 | 18,001 | 16,204 | 22,563 | 20,543 | 17,013 | 19,96 | 21,86 | 19,452 | 21,481 | 18,743 |
| | | 17,835 | 17,359 | **5,457** | 20,524 | 23,652 | 23,309 | 21,612 | 16,852 | 21,752 | 15,904 | 23,727 | 22,83 | 15,76 | 15,102 | 15,585 |
| | D13 | 16,457 | 21,423 | **4,103** | 17,442 | 16,409 | 16,254 | 21,701 | 15,372 | 18,288 | 19,559 | 20,521 | 20,465 | 23,976 | 18,317 | 22,757 |
| | | 15,203 | 21,289 | **4,314** | 23,34 | 16,78 | 23,445 | 22,484 | 23,495 | 19,558 | 18,016 | 21,683 | 23,557 | 21,426 | 18,622 | 16,687 |
| P4 | D4 | 20,906 | 19,484 | 22,506 | **6,357** | 18,995 | 16,167 | 17,892 | 17,925 | 19,646 | 15,625 | 23,026 | 23,075 | 23,565 | 19,217 | 19,348 |
| | | 22,632 | 15,098 | 16,066 | **5,729** | 23,003 | 16,311 | 21,523 | 20,418 | 19,541 | 16,188 | 21,192 | 16,709 | 17,834 | 18,365 | 18,496 |
| | | 21,02 | 19,965 | 17,748 | **7,318** | 19,681 | 18,434 | 23,771 | 21,943 | 17,417 | 15,492 | 21,882 | 23,332 | 18,702 | 17,577 | 17,272 |
| | D6 | 19,502 | 17,692 | 23,795 | **6,742** | 22,246 | 15,155 | 16,058 | 15,646 | 23,664 | 22,494 | 23,541 | 15,198 | 19,282 | 17,484 | 21,082 |
| | | 19,939 | 19,37 | 23,625 | **6,962** | 20,631 | 19,004 | 20,832 | 19,293 | 22,022 | 23,402 | 17,052 | 17,232 | 18,164 | 17,873 | 19,976 |
| | | 18,897 | 23,705 | 17,122 | **4,613** | 20,781 | 16,288 | 22,001 | 23,015 | 18,224 | 16,666 | 19,41 | 17,394 | 21,937 | 23,519 | 21,583 |
| P5 | D9 | 18,802 | 18,499 | 15,659 | 22,231 | **5,334** | 18,888 | 23,515 | 21,242 | 15,157 | 23,785 | 18,402 | 15,995 | 20,864 | 18,652 | 19,502 |
| | D13 | 16,103 | 19,814 | 23,661 | 21,726 | **5,132** | 23,152 | 17,433 | 20,752 | 17,388 | 20,014 | 19,88 | 22,37 | 23,096 | 17,616 | 16,547 |
| | | 21,001 | 15,521 | 18,126 | 15,414 | **4,465** | 21,792 | 15,28 | 22,061 | 18,327 | 21,776 | 20,317 | 21,277 | 22,23 | 16,893 | 15,547 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 16,748 | 16,435 | 16,102 | 17,793 | **7,346** | 16,231 | 15,882 | 16,634 | 23,369 | 20,403 | 22,298 | 15,626 | 20,426 | 23,439 | 22,186 |
| P6 | D8 | 15,52 | 20,872 | 19,81 | 15,461 | 18,948 | **6,047** | 20,803 | 20,402 | 17,617 | 15,716 | 18,371 | 18,421 | 16,091 | 17,191 | 18,975 |
| | | 20,363 | 16,556 | 17,721 | 16,237 | 15,784 | **4,92** | 17,651 | 15,879 | 16,593 | 15,487 | 19,252 | 20,66 | 20,665 | 16,691 | 15,347 |
| | | 19,19 | 17,067 | 20,222 | 16,87 | 16,482 | **5,214** | 16,88 | 19,548 | 20,989 | 15,85 | 17,94 | 15,085 | 17,291 | 16,378 | 19,617 |
| | D10 | 18,89 | 18,563 | 19,173 | 20,066 | 19,61 | **7,237** | 20,211 | 18,394 | 18,171 | 17,259 | 18,105 | 20,291 | 18,28 | 20,511 | 15,156 |
| | | 19,523 | 20,119 | 15,184 | 18,113 | 16,255 | **5,71** | 19,31 | 17,59 | 18,433 | 17,068 | 17,893 | 19,932 | 20,618 | 18,456 | 18,081 |
| | | 18,722 | 15,446 | 19,614 | 19,362 | 19,094 | **7,027** | 19,508 | 19,122 | 19,458 | 16,306 | 18,329 | 16,268 | 20,083 | 15,214 | 16,827 |
| P7 | D4 | 19,123 | 19,598 | 18,902 | 18,662 | 16,724 | 16,654 | **6,899** | 20,735 | 15,842 | 14,305 | 14,837 | 18,489 | 14,242 | 17,701 | 17,391 |
| | | 19,885 | 17,579 | 17,683 | 18,655 | 20,886 | 17,061 | **5,092** | 15,574 | 19,561 | 15,251 | 20,942 | 14,948 | 14,72 | 19,961 | 19,898 |
| P8 | D9 | 20,076 | 20,319 | 20,983 | 15,02 | 17,901 | 20,524 | 20,491 | **7,249** | 17,813 | 15,822 | 15,149 | 17,289 | 17,476 | 16,154 | 17,985 |
| | | 15,954 | 20,273 | 16,319 | 17,439 | 16,072 | 16,329 | 21,243 | **6,898** | 15,862 | 20,315 | 18,097 | 20,973 | 21,905 | 16,716 | 17,186 |
| | | 21,124 | 18,336 | 15,962 | 16,209 | 20,616 | 19,762 | 17,351 | **5,643** | 16,678 | 17,719 | 21,108 | 15,135 | 19,509 | 21 | 16,235 |
| | D14 | 15,117 | 18,123 | 21,184 | 15,834 | 19,208 | 19,857 | 18,503 | **6,698** | 20,489 | 19,452 | 15,951 | 17,958 | 19,929 | 18,822 | 15,817 |
| | | 21,771 | 15,149 | 15,708 | 18,148 | 17,747 | 19,547 | 18,642 | **5,713** | 19,779 | 19,865 | 19,24 | 17,02 | 21,212 | 17,07 | 19,875 |
| P9 | D11 | 17,193 | 18,002 | 18,854 | 18,586 | 15,558 | 18,099 | 18,298 | 19,45 | **7,073** | 18,227 | 17,291 | 18,531 | 19,273 | 19,415 | 15,841 |
| | | 16,921 | 15,449 | 19,908 | 16,332 | 19,277 | 19,999 | 17,905 | 15,449 | **6,747** | 17,523 | 15,229 | 19,576 | 18,544 | 17,578 | 19,16 |
| | | 15,648 | 19,534 | 18,627 | 15,765 | 19,246 | 16,9 | 18,381 | 15,689 | **7,329** | 16,628 | 15,637 | 19,75 | 18,776 | 19,351 | 18,567 |
| P10 | D2 | 15,038 | 18,656 | 15,246 | 14,792 | 18,193 | 15,972 | 16,255 | 14,858 | 18,867 | **6,42** | 15,442 | 17,223 | 17,53 | 15,815 | 17,921 |
| | | 17,78 | 18,846 | 16,954 | 16,777 | 14,637 | 16,228 | 15,632 | 15,58 | 17,767 | **6,337** | 16,003 | 16,792 | 16,651 | 18,758 | 14,887 |
| | | 17,036 | 14,867 | 15,876 | 15,427 | 16,816 | 18,544 | 15,499 | 16,202 | 16,136 | **7,002** | 16,221 | 17,066 | 16,732 | 16,067 | 15,611 |
| | D10 | 17,28 | 14,662 | 16,273 | 18,219 | 18,037 | 14,528 | 16,532 | 15,328 | 18,877 | **7,266** | 15,909 | 15,14 | 14,785 | 18,236 | 18,925 |
| | | 16,326 | 16,267 | 17,612 | 15,707 | 16,93 | 17,829 | 14,645 | 17,44 | 17,21 | **6,991** | 15,381 | 17,32 | 15,545 | 16,079 | 17,888 |
| | | 14,958 | 17,789 | 17,688 | 18,011 | 14,967 | 15,85 | 18,009 | 17,96 | 18,615 | **6,724** | 18,679 | 16,247 | 17,625 | 17,443 | 16,28 |
| P11 | D4 | 17,01 | 19,26 | 18,432 | 19,412 | 17,084 | 16,089 | 17,828 | 17,147 | 19,111 | 19,893 | **6,442** | 19,795 | 18,858 | 16,611 | 18,785 |
| | | 16,081 | 16,617 | 15,729 | 19,008 | 19,07 | 18,717 | 17,443 | 18,319 | 18,666 | 17,833 | **6,933** | 16,84 | 18,712 | 16,916 | 19,43 |
| | D6 | 18,187 | 18,775 | 19,205 | 17,108 | 16,187 | 16,29 | 18,996 | 18,256 | 19,792 | 18,318 | **7,36** | 16,97 | 16,889 | 19,921 | 18,279 |
| | | 19,221 | 16,539 | 15,758 | 19,215 | 17,975 | 16,292 | 16,251 | 16,79 | 16,175 | 17,882 | **6,316** | 16,16 | 16,34 | 16,252 | 17,357 |
| P12 | D1 | 17,698 | 16,822 | 19,317 | 18,914 | 18,105 | 16,965 | 21,108 | 17,87 | 18,557 | 17,591 | 16,953 | **7,228** | 21,776 | 16,048 | 20,938 |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 21,629 | 18,339 | 21,377 | 16,074 | 20,886 | 20,643 | 18,085 | 16,359 | 19,733 | 19,29 | 18,638 | **7,158** | 17,318 | 21,039 | 21,156 |
| | | 16,691 | 20,26 | 21,2 | 19,408 | 21,941 | 20,609 | 20,227 | 20,646 | 18,694 | 21,952 | 17,255 | **5,603** | 20,274 | 20,617 | 20,667 |
| | D9 | 21,908 | 19,525 | 18,984 | 20,606 | 19,477 | 19,135 | 18,317 | 17,389 | 21,495 | 18,086 | 20,604 | **7,381** | 21,046 | 18,253 | 21,806 |
| | | 19,888 | 17,541 | 17,666 | 16,547 | 21,634 | 19,104 | 20,195 | 16,647 | 16,933 | 19,367 | 20,555 | **6,142** | 19,064 | 17,173 | 18,774 |
| P13 | D8 | 17,914 | 19,578 | 15,351 | 19,691 | 20,183 | 18,992 | 15,21 | 17,58 | 18,28 | 15,992 | 15,481 | 19,247 | **6,009** | 20,515 | 20,308 |
| | | 16,446 | 17,907 | 16,156 | 17,473 | 16,446 | 16,227 | 19,185 | 20,23 | 19,543 | 17,914 | 16,352 | 15,015 | **7,495** | 16,074 | 19,639 |
| | | 17,09 | 15,134 | 15,091 | 15,263 | 17,401 | 18,576 | 17,68 | 15,453 | 18,606 | 20,809 | 17,817 | 19,598 | **6,288** | 15,948 | 18,479 |
| | D14 | 17,668 | 17,13 | 18,625 | 19,086 | 15,162 | 16,224 | 15,612 | 18,889 | 18,249 | 18,958 | 15,151 | 18,761 | **5,464** | 17,439 | 15,776 |
| | | 15,514 | 17,456 | 17,371 | 18,706 | 15,076 | 16,248 | 18,978 | 19,559 | 20,268 | 18,623 | 20,733 | 15,26 | **5,185** | 15,595 | 18,468 |
| P14 | D14 | 20,782 | 20,432 | 18,494 | 19,935 | 17,998 | 20,803 | 20,356 | 20,743 | 16,971 | 20,853 | 20,219 | 17,611 | 21,115 | **5,323** | 17,343 |
| | | 20,869 | 18,876 | 17,037 | 21,052 | 19,401 | 20,462 | 16,7 | 17,303 | 17,64 | 19,743 | 16,514 | 18,598 | 19,761 | **5,857** | 21,198 |
| P15 | D1 | 17,76 | 16,667 | 16,336 | 15,267 | 17,639 | 19,651 | 19,888 | 18,285 | 17,13 | 15,147 | 15,688 | 19,404 | 15,888 | 15,928 | **6,283** |
| | | 15,463 | 15,274 | 18,473 | 18,76 | 16,201 | 17,537 | 16,06 | 15,344 | 18,892 | 17,255 | 16,44 | 15,87 | 17,763 | 16,313 | **5,965** |
| | D11 | 17,537 | 19,798 | 18,832 | 18,211 | 16,82 | 15,708 | 18,924 | 16,246 | 19,578 | 15,363 | 17,739 | 16,881 | 15,512 | 16,389 | **5,481** |
| | | 19,792 | 15,147 | 16,313 | 16,743 | 15,351 | 17,232 | 17,869 | 19,028 | 19,312 | 16,151 | 17,924 | 18,283 | 16,348 | 16,493 | **5,067** |
| | | 16,321 | 18,243 | 15,635 | 17,75 | 15,11 | 19,189 | 17,463 | 19,289 | 15,859 | 16,189 | 19,264 | 18,307 | 18,413 | 16,162 | **6,353** |

Según la tabla, se verifica que el identificador utilizado, iris humano, presenta variabilidad en su composición, y, por ende, seguridad y complejidad para evitar hechos de clonación. Así como fue mencionado en el punto anterior, el modelo de Deep Learning utilizado que emplea el concepto de One Shot Learning y Redes Siamesas, genera una distancia, que, al ser pequeña, corresponde a la misma persona, caso contrario, son personas diferentes.

### 2.7. Bitácora de eventos

Según la trazabilidad del Sistema de Reconocimiento de Iris, en la siguiente tabla se visualiza los días “D” de evaluación, y la cantidad de eventos registrados en cada día para:

- Acceso concedido; cantidad de registros de accesos concedidos a las personas.
- Personal no registrado; cantidad de registros de intentos por personal no registrado.
- Identificador no encontrado; cantidad de registros por la no presencia del identificador en la imagen capturada a procesar.

*Cantidad de registros de eventos durante el proceso de control de acceso con el uso del Sistema de Reconocimiento de Iris*

| | Cantidad | | |
|---|---|---|---|
| Día | Acceso Concedido | Personal no Registrado | Identificador no Encontrado |
| D1 | 5 | 1 | 3 |
| D2 | 7 | 0 | 4 |
| D3 | 0 | 0 | 2 |
| D4 | 7 | 0 | 3 |
| D5 | 5 | 0 | 2 |
| D6 | 5 | 1 | 0 |
| D7 | 0 | 0 | 1 |
| D8 | 6 | 0 | 2 |
| D9 | 6 | 1 | 1 |
| D10 | 6 | 0 | 0 |
| D11 | 9 | 1 | 2 |
| D12 | 0 | 0 | 0 |
| D13 | 6 | 0 | 0 |
| D14 | 6 | 0 | 0 |
| D15 | 0 | 0 | 0 |
| Total | 68 | 4 | 20 |

Según la tabla, se verifica la cantidad de eventos registrados durante el proceso de acceso al almacén del área de Tesorería del Gobierno Regional de Tacna, donde:

- La cantidad de accesos concedidos representa a la misma cantidad indicada en la tabla de cantidad de apertura de puerta de acceso, siendo de 68 accesos concedidos.
- La cantidad de intentos por personal no registrado indica los intentos de acceso de personas no autorizadas, por posibles motivos de acceso o curiosidad de las personas aledañas al lugar, siendo de cuatro intentos de acceso.
- La cantidad de registros por la no presencia del identificador, indica los intentos de posicionamiento del identificador (iris) en el capturador de la puerta de acceso, el cual no ha podido localizar el identificador en la imagen capturada, por posibles motivos de aprendizaje de uso o curiosidad de las personas aledañas al lugar, siendo de 20 registros.

## Anexo 12. Proceso de aceptación del proyecto en el Gobierno Regional de Tacna

### 1. Descripción

SRICA, Sistema de Reconocimiento de Iris para Control de Acceso, es el proyecto elaborado e implementado en el Gobierno Regional de Tacna, específicamente, en el almacén del área de Tesorería ubicado en la Sede Hipólito Unanue, para controlar el acceso de personas a este espacio físico.

Para lograr la implementación del proyecto en la entidad anteriormente mencionada, fue necesario solicitar el permiso correspondiente para el ingreso a las instalaciones, y el permiso de aplicación del proyecto, siendo autorizado satisfactoriamente.

### 2. Solicitud de Permiso de Aplicación del Proyecto

Para la solicitud de permiso de aplicación del proyecto, fue necesario elaborar una carta formal, en el cual se solicitó el apoyo correspondiente para la aplicación del proyecto de control de acceso mediante un Sistema de Reconocimiento de Iris.

*Carta de solicitud para la aplicación del proyecto en el Gobierno Regional de Tacna*

Tacna, 01 de Octubre del 2020

GOBIERNO REGIONAL DE TACNA
ADMINISTRACIÓN DOCUMENTARIA
1078143
05 OCT 2020
RECIBIDO
REGISTRO N° HORA 12:05
FIRMA:

Señor:
Ing. Juan Tonconi Quispe
Gobernador Regional de Tacna

Tacna

ASUNTO:
Solicito apoyo para aplicación de Proyecto de control Biometrico ocular

De mi consideración:

Por la presente me es grato saludarlo deseándole al mismo tiempo continuar con sus logros en beneficio de la región Tacna..
El motivo de la presente es para SOLICITARLE SU APOYO en la APLICACIÓN e INSTALACIÓN DE UN SISTEMA DE CONTROL en la forma siguiente;

1. El suscrito es bachiller egresado en la especialidad de Ingeniería de Sistemas de la Universidad Privada de Tacna por tal motivo con la finalidad de obtener el grado de "ingeniero", es preciso APLICAR un estudio de innovación tecnológica.
2. Esta innovación tecnológica consiste en la instalación de un sistema de seguridad y control de personal denominado "Sistema de reconocimiento de iris para control de acceso a zonas o áreas restringidas".
3. Para la consecución de este proyecto, el suscrito realizará la financiación presupuestal en el 100% que requiere el mismo por lo que SOLICITO el APOYO por parte la entidad representada por su persona destinando el área de acceso restringido en donde se instale este sistema para comprobar su funcionabilidad.
4. Los detalles del proyecto se especifican en el PERFIL que adjunto a la presente.

Señor gobernador, es reconocido su espíritu altruista y apoyo al joven profesional, razón por el cual, no dudo que este PROYECTO será aceptado por su comuna, por lo que me despido de Ud. sin antes dejar mi correo electrónico para las coordinaciones del caso mamanimolinadaniel@gmail.com.

Dios guarde a Ud.

Atentamente

Bach. Luis Eduardo Mamani Bedregal
DNI Nr° 72463957
Celular 943494351

### 3. Reactivación de la Solicitud de Permiso de Aplicación del Proyecto

Debido a que, el desarrollo del proyecto fue elaborado dentro de los tiempos de alerta sanitaria debido al COVID-19, en el cual, el Gobierno Central ha impuesto normativas de bioseguridad, todo proceso administrativo dentro del Gobierno Regional de Tacna se realizó mediante el uso de la Mesa de Partes Virtual de la institución.

Así mismo, debido a que cada año se puede, o no, realizar cambio de jefatura, el cual ocasiona vencimiento de documentos, es que se solicitó, nuevamente, el permiso de aplicación del proyecto dentro de las instalaciones de la entidad Gobierno Regional de Tacna.

*Carta de solicitud y proceso de reactivación para la aplicación del proyecto en el Gobierno Regional de Tacna*

Tacna, Febrero 16 del 2022.

SEÑOR:
Ingº. JUAN TONCONI QUISPE
Presidente del gobierno regional de Tacna

ASUNTO:
Solicito la aplicación del Proyecto denominado "Control Biométrico Ocular"

REFERENCIA: Carta s/n. CUD Nrº 1078143 del 05-10-2020

De mi consideración:

Por el presente me es grato saludarlo y a su vez aprovechar la oportunidad para SOLICITARLE que, por intermedio del Área respectiva, se pueda ejecutar y aplicar el proyecto denominado "CONTROL BIOMETRICO OCULAR", el cual se describe en el perfil que se adjunta en el documento de referencia, al igual que las condiciones del proyecto indicados en las consideraciones del referido documento.

Esta solicitud la reitero en base a las siguientes consideraciones:

1. El suscrito remitió el documento de la referencia el cual fue admitido con fecha 05 de octubre del 2020 con CUD 1078143 y derivado al área respectiva.
2. Con fecha 19 de octubre del 2020 se emite la Carta Nrº 191-2020-ORA-OERRHH/GOB.REG.Tacna en el que se requiere la validación del Proyecto innovador por parte del Decano de la facultad de Ingeniería de la UPT para proceder con la aplicación del proyecto.
3. Con fecha 12 de enero del 2021 se emite la Resolución de decanato Nrº 051-D-2021-FAING/UPT, aprobando y validando el Plan de Tesis.

Es menester precisar que, durante el año 2021, no se pudo continuar con la aplicación del proyecto mencionado por situaciones del COVID-19 y las restricciones impuestas al respecto, razón por el cual, es que solicito una vez más la reactivación de este petitorio para su aplicación y ejecución.

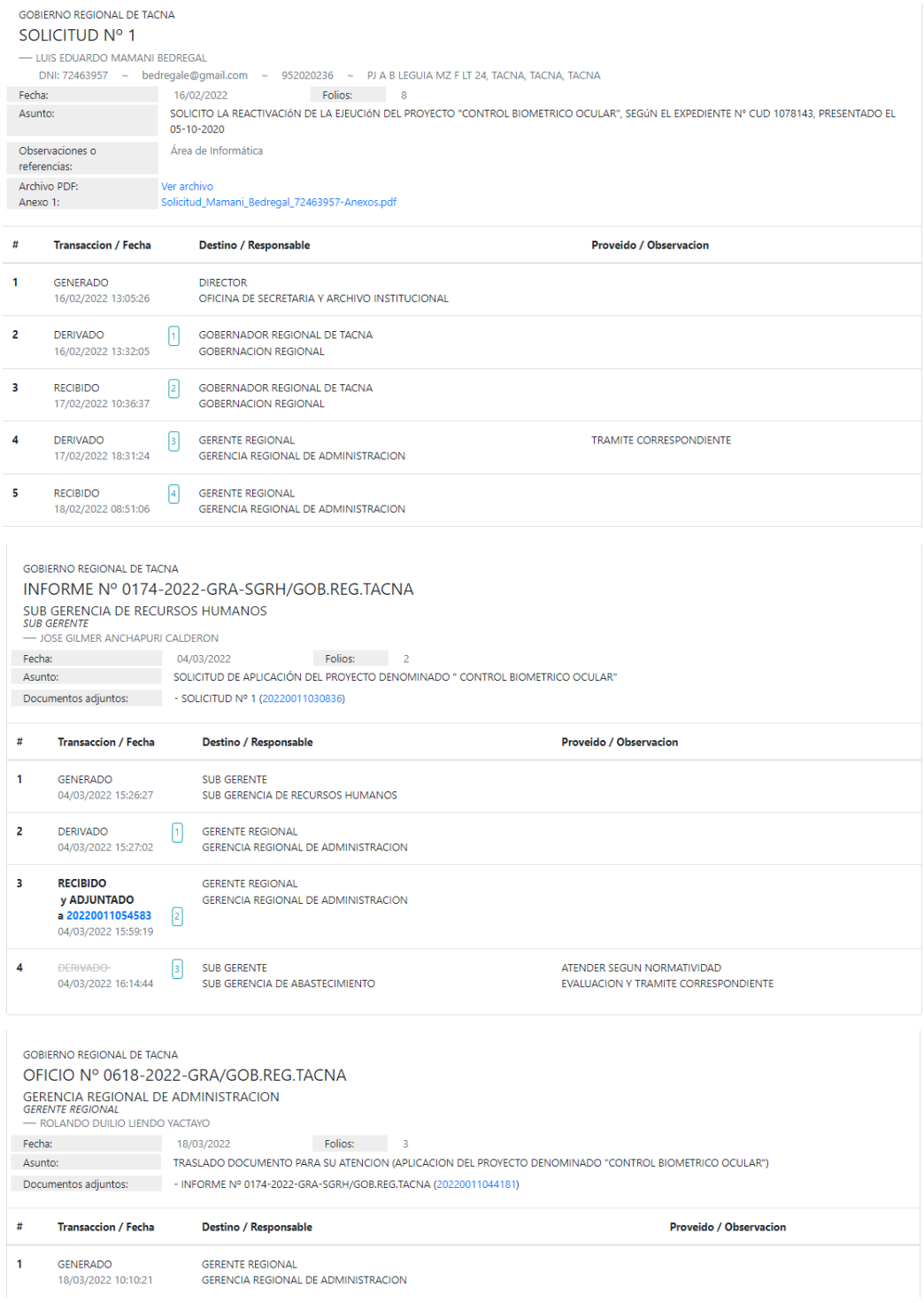
Con la seguridad de que esta solicitud tendrá la atención requerida, invocando una vez más el apoyo, me despido de Ud. reiterándole mi especial consideración.

Adjunto al presente:

- Copia del documento de la referencia
- Perfil del Proyecto
- Carta Nrº 191-2020
- Copia de la Resolución Nrº 051- D-2021-FAING/UPT

Atentamente

Luis Eduardo Mamani Bedregal
Bach. Ingeniería de Sistemas
DNI Nro 72463957



GOBIERNO REGIONAL DE TACNA

SOLICITUD Nº 1

— LUIS EDUARDO MAMANI BEDREGAL

DNI: 72463957 ~ bedregale@gmail.com ~ 952020236 ~ PJ A B LEGUIA MZ F LT 24, TACNA, TACNA, TACNA

| | |
|---|---|
| Fecha: | 16/02/2022 Folios: 8 |
| Asunto: | SOLICITO LA REACTIVACIÓN DE LA EJEUCIÓN DEL PROYECTO "CONTROL BIOMETRICO OCULAR", SEGÚN EL EXPEDIENTE N° CUD 1078143, PRESENTADO EL 05-10-2020 |
| Observaciones o referencias: | Área de Informática |
| Archivo PDF: | Ver archivo |
| Anexo 1: | Solicitud_Mamani_Bedregal_72463957-Anexos.pdf |

| # | Transaccion / Fecha | | Destino / Responsable | Proveido / Observacion |
|---|---|---|---|---|
| 1 | GENERADO 16/02/2022 13:05:26 | | DIRECTOR OFICINA DE SECRETARIA Y ARCHIVO INSTITUCIONAL | |
| 2 | DERIVADO 16/02/2022 13:32:05 | 1 | GOBERNADOR REGIONAL DE TACNA GOBERNACION REGIONAL | |
| 3 | RECIBIDO 17/02/2022 10:36:37 | 2 | GOBERNADOR REGIONAL DE TACNA GOBERNACION REGIONAL | |
| 4 | DERIVADO 17/02/2022 18:31:24 | 3 | GERENTE REGIONAL GERENCIA REGIONAL DE ADMINISTRACION | TRAMITE CORRESPONDIENTE |
| 5 | RECIBIDO 18/02/2022 08:51:06 | 4 | GERENTE REGIONAL GERENCIA REGIONAL DE ADMINISTRACION | |

GOBIERNO REGIONAL DE TACNA

INFORME Nº 0174-2022-GRA-SGRH/GOB.REG.TACNA

SUB GERENCIA DE RECURSOS HUMANOS

*SUB GERENTE*

— JOSE GILMER ANCHAPURI CALDERON

| | |
|---|---|
| Fecha: | 04/03/2022 Folios: 2 |
| Asunto: | SOLICITUD DE APLICACIÓN DEL PROYECTO DENOMINADO " CONTROL BIOMETRICO OCULAR" |
| Documentos adjuntos: | - SOLICITUD Nº 1 (20220011030836) |

| # | Transaccion / Fecha | | Destino / Responsable | Proveido / Observacion |
|---|---|---|---|---|
| 1 | GENERADO 04/03/2022 15:26:27 | | SUB GERENTE SUB GERENCIA DE RECURSOS HUMANOS | |
| 2 | DERIVADO 04/03/2022 15:27:02 | 1 | GERENTE REGIONAL GERENCIA REGIONAL DE ADMINISTRACION | |
| 3 | **RECIBIDO y ADJUNTADO a 20220011054583** 04/03/2022 15:59:19 | 2 | GERENTE REGIONAL GERENCIA REGIONAL DE ADMINISTRACION | |
| 4 | ~~DERIVADO~~ 04/03/2022 16:14:44 | 3 | SUB GERENTE SUB GERENCIA DE ABASTECIMIENTO | ATENDER SEGUN NORMATIVIDAD EVALUACION Y TRAMITE CORRESPONDIENTE |

GOBIERNO REGIONAL DE TACNA

OFICIO Nº 0618-2022-GRA/GOB.REG.TACNA

GERENCIA REGIONAL DE ADMINISTRACION

*GERENTE REGIONAL*

— ROLANDO DUILIO LIENDO YACTAYO

| | |
|---|---|
| Fecha: | 18/03/2022 Folios: 3 |
| Asunto: | TRASLADO DOCUMENTO PARA SU ATENCION (APLICACION DEL PROYECTO DENOMINADO "CONTROL BIOMETRICO OCULAR") |
| Documentos adjuntos: | - INFORME Nº 0174-2022-GRA-SGRH/GOB.REG.TACNA (20220011044181) |

| # | Transaccion / Fecha | Destino / Responsable | Proveido / Observacion |
|---|---|---|---|
| 1 | GENERADO 18/03/2022 10:10:21 | GERENTE REGIONAL GERENCIA REGIONAL DE ADMINISTRACION | |

En la figura, se visualiza el proceso de reactivación del trámite correspondiente para ejecutar el proyecto dentro de las instalaciones del Gobierno Regional de Tacna, del cual, debido a la persistencia del investigador, y el apoyo de los propios trabajadores, se logró aplicar en las fechas correspondientes de investigación, para así, no esperar que la solicitud sea procesada por diversas áreas u oficinas debido a su demora en atención.

## 4. Documento de Cierre del Proyecto para su Respectivo Despliegue y Aplicación en el Gobierno Regional de Tacna

La fecha indicada en el documento, hace referencia al momento correspondiente de aceptación de los interesados para la ejecución respectiva del despliegue y aplicación del Sistema de Reconocimiento de Iris para control de acceso, SRICA.

*Documento de cierre del proyecto para su respectivo despliegue y aplicación en el Gobierno Regional de Tacna*

| CONTROL DE VERSIONES | | | | |
|---|---|---|---|---|
| **Versión** | **Identificador** | **Hecho por** | **Fecha** | **Motivo** |
| 1.0 | SRICA_046_000 | Luis Eduardo Mamani Bedregal | 01/03/202 | Se realiza el acta de fin de proyecto. |

| **NOMBRE DEL PROYECTO** | **SIGLAS DEL PROYECTO** |
|---|---|
| Uso de Sistema de Reconocimiento de Iris basado en Deep Learning para la identificación humana en el control de acceso al área de Tesorería del Gobierno Regional de Tacna – Tacna 2020. | SRICA |

| **ACTA DE FIN DE PROYECTO** | |
|---|---|
| **Lugar** | **Fecha** |
| Gobierno Regional de Tacna | 01/03/2022 |
| **Encargado** | **Cargo** |
| Luis Eduardo Mamani Bedregal | Director del Proyecto |

| **RAZÓN DE FINALIZACIÓN** | |
|---|---|
| **Razón** | |
| Entrega de todos los productos de conformidad con los requerimientos establecidos. | X |
| Entrega parcial de productos y cancelación de otros de conformidad con los requerimientos establecidos. | |
| Cancelación de todos los productos asociados con el proyecto. | |

| **ACEPTACIÓN DE LOS PRODUCTOS O ENTREGABLES** | | | |
|---|---|---|---|
| **Fase** | **Entregable** | **Aceptación** | **Observaciones** |
| Inicio | Estructura de desglose del trabajo (EDT) | X | |
| | Estructura de desglose de recursos (RBS) | X | |
| | Cronograma del proyecto | X | |
| | Plan de gestión de cambios | X | |
| | Plan de gestión de la configuración | X | |
| | Plan de dirección del proyecto | X | |
| | Plan de gestión de costos | X | |
| | Estimación de duraciones de actividades | X | |
| | Presupuesto del proyecto | X | |
| | Plan de gestión de riesgos | X | |
| | Informe de seguimiento de riesgos | X | |
| | Plan de gestión de calidad | X | |
| | Solicitud de cambios | X | |
| | Aprobación de cambios | X | |
| | Control de cambios | X | |
| | Informe de auditoría de la configuración | X | |
| | Control de versiones | X | |
| | Documento de análisis de brecha | X | |
| Elaboración | Requerimientos funcionales y no funcionales | X | |
| | Especificación detallada de casos de uso y prototipos | X | |
| | Diagrama de casos de uso | X | |
| | Diagrama de paquetes | X | |
| | Diagrama de clases | X | |
| | Diagrama de secuencia | X | |
| | Diagrama de componentes | X | |
| | Diagrama de despliegue | X | |
| | Especificación de requerimientos de software (SRS) | X | |
| | Documento de arquitectura de software (SAD) | X | |
| | Estándar de codificación | X | |
| | Diagrama entidad-relación | X | |
| | Modelo lógico | X | |
| | Modelo físico | X | |
| | Diccionario de datos | X | |
| Construcción | Código fuente | X | |
| | Inteligencia artificial (modelos de deep learning) | X | |
| | Equipo biométrico | X | |
| | Plan de pruebas | X | |
| | Pruebas unitarias | X | |
| | Pruebas de despliegue | X | |
| | Informe de pruebas | X | |
| Transición (Cierre) | Manual técnico | X | |
| | Manual de usuario | X | |

Para cada entregable aceptado, se da por entendido que:

- El entregable ha cumplido los criterios de aceptación establecidos en la documentación de requerimientos.
- Se ha verificado que los entregables cumplen los requerimientos.
- Se ha validado el cumplimiento de los requerimientos funcionales y de calidad definidos.

Por consiguiente, se cumple con los entregables indicados del proyecto para su respectivo despliegue y funcionamiento en el Gobierno Regional de Tacna, destinado al control de acceso del almacén del área de Tesorería ubicado en la Sede Hipólito Unanue.

Así mismo, el Sistema de Reconocimiento de Iris para control de acceso, SRICA, al encontrarse dentro del campo tecnológico e informático, se realizó la notificación al área de Tecnología de la Información, presentando el respectivo documento solicitado por la misma área, donde se indicó el plan de trabajo para el apoyo correspondiente dentro de sus capacidades.

*Carta y proceso de remisión del plan de trabajo a OTI para la aplicación del proyecto en el Gobierno Regional de Tacna*

Tacna, 02 de Marzo del 2022.

Señor:
Ingº Rolando Álvarez
Director de OTI
Gobierno Regional de Tacna

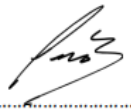
ASUNTO: Remito Plan de trabajo para la aplicación del Proyecto "**Sistema De Reconocimiento De Iris Para Control De Acceso**"

De mi consideración:

Por el presente me es grato saludarlo y a su vez hacerle llegar el PLAN DE TRABAJO que establece las acciones a realizar para la ejecución, implementación y desarrollo del proyecto denominado "**Sistema De Reconocimiento De Iris Para Control De Acceso**". Asimismo, debo hacer de su conocimiento que, para la ejecución de alguna de las actividades previstas en el Plan, el suscrito será asistido por un (01) personal de apoyo, cuyas generales son: Daniel Mamani Molina, con DNI Nrº 00412456.

Sin otro particular y con la gratitud por el apoyo concedido quedo de Ud.

Atentamente



.....

Bach. Luis Eduardo Mamani Bedregal
DNI 72463957

**SISTEMA DE RECONOCIMIENTO DE IRIS PARA CONTROL DE ACCESO**

**Descripción del Proyecto:**

1. **Aspectos Técnicos:**

   El "Sistema de Reconocimiento de Iris para control de acceso" es un sistema biométrico que controlará el acceso solo de personas autorizadas a lugares y/o áreas restringidas por la entidad.

   Este proyecto consta de dos componentes: hardware y software.

   - *Hardware:* Equipo biométrico (elaborado por medios propios) que se encargará de capturar el iris de la persona, y otorgar el acceso correspondiente. Emite sonidos y luces para indicar accesos concedidos o fallos. El equipo biométrico será instalado en el área previamente designado.
   - *Software:* Procesos y algoritmos de software que permitirán, con ayuda del equipo biométrico, transformar y procesar los datos biométricos de cada persona. Estos procesos son instalados en servidores, y la comunicación es por red local.

2. **Características del Proyecto:**

   El proyecto permite la captura inicial del iris de la persona para su registro en el sistema. Esta captura se realiza mediante una cámara ocular para ser procesada por los algoritmos desarrollados, el cual será la "llave de paso" que distingue cada persona de otra.

   Al contemplar el iris como identificador personal, y al ser un elemento no invasivo para el equipo biométrico (es decir, no hay contacto directo / físico con el lector), la suplantación de identidad es nula.

   Cabe recalcar que la estructura del iris es única por persona, incluso ambos iris de la persona son diferentes entre sí. Se estima que el patrón de similitud del iris entre dos personas es de 1 en $10^{78}$, es decir, el 0% de probabilidad.

3. **Lugar deseado para la implementación del Proyecto**

   El presente proyecto permite salvaguardar bienes tangibles e intangibles de la entidad y/o del área considerada de vital importancia, y que requiere seguridad en su acceso, por lo que su enfoque está dirigido a áreas críticas o restringidas donde sólo accede personal autorizado.

   Se recomienda áreas donde se encuentren activos importantes, donde el flujo de personas no sea constante, y que solo algunas personas tengan acceso a esa área o ambiente (ya sea accesos por llave, identificador, fotocheck, u otros distintos a la funcionalidad del presente proyecto).

**Plan de Trabajo:**

| Descripción de las actividades | Detalle | Participantes |
|---|---|---|
| 1) Toma de medidas | Se tomarán las medidas del lugar donde se instalará el equipo biométrico. | • Luis Eduardo Mamani Bedregal, con DNI 72463957 (autor principal)<br>• Daniel Mamani Molina, con DNI 00412456 (ayudante) |
| 2) Instalación del software | Se instalarán los componentes de software necesarios para el funcionamiento del proyecto. | • Luis Eduardo Mamani Bedregal, con DNI 72463957 (autor principal) |
| 3) Instalación del equipo biométrico | Se instalará el equipo biométrico mediante el cual se capturará el iris del personal que tiene acceso al área correspondiente. | • Luis Eduardo Mamani Bedregal, con DNI 72463957 (autor principal)<br>• Daniel Mamani Molina, con DNI 00412456 (ayudante) |
| 4) Proyecto en ejecución | Se iniciará el desarrollo y ejecución de la investigación. ** | • Luis Eduardo Mamani Bedregal, con DNI 72463957 (autor principal) |

** Dentro de las mismas actividades, se contempla la aplicación de ficha de evaluación (inicio – final) como instrumento recolector de información para la presente investigación.

**Cronograma del Plan de Trabajo:**

| Actividad ** | Días | | | | Responsables |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 ~ 25 | |
| Toma de medidas del lugar donde se instalará el equipo biométrico. | X | | | | • Luis Eduardo Mamani Bedregal (autor principal)<br>• Daniel Mamani Molina (ayudante) |
| Instalación de los componentes de software necesarios para el funcionamiento del proyecto. | X | X | | | • Luis Eduardo Mamani Bedregal (autor principal) |
| Instalación del equipo biométrico mediante el cual se capturará el iris del personal que tiene acceso al área correspondiente. | | X | X | | • Luis Eduardo Mamani Bedregal (autor principal)<br>• Daniel Mamani Molina (ayudante) |
| Desarrollo y ejecución de la investigación. | | | | X | • Luis Eduardo Mamani Bedregal (autor principal) |

** Considerar 3 días extras de holgura como adicional al cronograma presentado (considerando solo días laborales).

Para el desarrollo del presente Plan de Trabajo, se considerará como fecha de inicio la conformidad de aprobación y determinación del área y/o zona de ejecución por parte de la entidad para ejecutar el presente proyecto. Cabe recalcar que se están estimando la cantidad de días que transcurrirán desde la fecha de inicio acordada.

GOBIERNO REGIONAL DE TACNA

CARTA S/N

— LUIS EDUARDO MAMANI BEDREGAL

DNI: 72463957 ~ bedregale@gmail.com ~ 952020236 ~ PJ A B LEGUIA MZ F LT 24, TACNA, TACNA, TACNA

| | | | |
|---|---|---|---|
| Fecha: | 02/03/2022 | Folios: | 5 |
| Asunto: | REMITO PLAN DE TRABAJO PARA LA APLICACIÓN DEL PROYECTO "SISTEMA DE RECONOCIMIENTO DE IRIS PARA CONTROL DE ACCESO" | | |
| Archivo PDF: | Ver archivo | | |

| # | Transaccion / Fecha | Destino / Responsable | Proveido / Observacion |
|---|---|---|---|
| 1 | GENERADO<br>02/03/2022 12:53:50 | DIRECTOR<br>OFICINA DE SECRETARIA Y ARCHIVO INSTITUCIONAL | |
| 2 | **DERIVADO** 1<br>02/03/2022 13:58:13 | DIRECTOR<br>OFICINA DE TECNOLOGIA DE LA INFORMACION | |

## Anexo 13. Costo de investigación

### 1. Descripción

El costo de investigación se ha planteado desde el inicio de la investigación, estimando los recursos que se utilizaron. A medida que la investigación se iba realizando, se agregaron algunos costos no planificados.

### 2. Costos

*Costo de Investigación*

| Materiales | | |
|---|---|---|
| Recurso | Cantidad | Costo (S/.) |
| Hojas blancas | 2 paquete | 25,00 |
| Cinta métrica | 1 | 20,00 |
| Computadora de escritorio | 1 | 3200,00 |
| Impresora | 1 | 280,00 |
| Kit Raspberry Pi v4 | 1 | 365,00 |
| Sensor ultrasonido para el módulo Raspberry Pi v4 | 1 | 20,00 |
| Módulo relay para el módulo Raspberry Pi v4 | 1 | 10,00 |
| Módulo de cámaras para el módulo Raspberry Pi v4 | 2 | 730,00 |
| Componentes electrónicos para el módulo Raspberry Pi v4 | - | 150,00 |
| Electroimán | 1 | 160,00 |
| Complementos del electroimán | 1 | 180,00 |
| Botón No Touch | 1 | 60,00 |
| Caja del Equipo Biométrico | 1 | 20,00 |
| Mueble Soporte del Equipo Biométrico | 1 | 95,00 |
| Cables de red UTP | 6 metros | 15,00 |
| Cables de Conexión Eléctrica | 6 metros | 15,00 |
| Multímetro | 1 | 120,00 |
| Imprevistos | - | 200,00 |
| Servicios | | |
| Recurso | Unidad | Costo (S/.) |
| Internet | 12 meses | 1188,00 |
| Electricidad | 12 meses | 600,00 |

| | | |
|---|---|---|
| Movilidad local | 3 meses | 250,00 |
| Teléfono | 12 meses | 660,00 |
| Imprevistos | - | 200,00 |
| Licencias | | |
| Recurso | Unidad | Costo (S/.) |
| Windows 10 Professional | 1 licencia | 450,00 |
| Microsoft Office 2019 | 1 licencia | 100,00 |
| Microsoft Azure | 1 mes | 550,00 |
| Imprevistos | - | 200,00 |
| TOTAL (S/.) | | 9863,00 |

El costo total de la investigación fue de S/. 9863,00 nuevos soles, nueve mil trescientos trece y 00/100 nuevos soles.