ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

# CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

## "IMPLEMENTACIÓN DE UN MODELO DE DESARROLLO EVOLUTIVO DE SOFTWARE QUE PERMITA DETECTAR Y MITIGAR ATAQUES DE INGENIERÍA SOCIAL UTILIZANDO TÉCNICAS DE DEEP LEARNING".

**AUTORES:** SANTIAGO DAVID BOSQUE GUANOTASIG
BRYAN ABRAHAN ZURITA BEDOYA

**DIRECTOR:** ING. WALTER FUERTES, PHD


# ÍNDICE

# 01. INTRODUCCIÓN

## Planteamiento del Problema

Poca atención al entorno

Propósitos malévolos

Afectación a gran escala

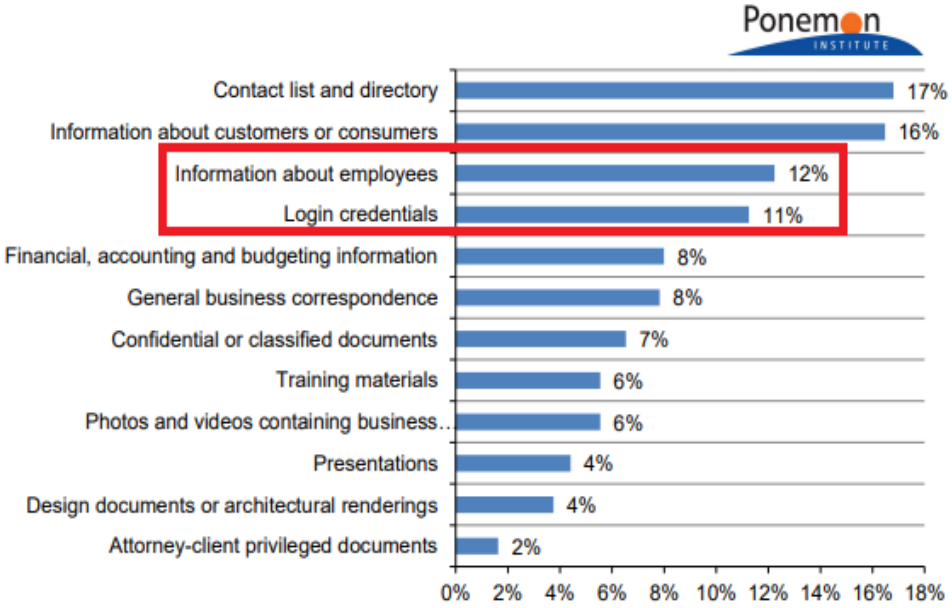
Aprender a resguardar la información

Herramientas y métodos de seguridad vulneradas

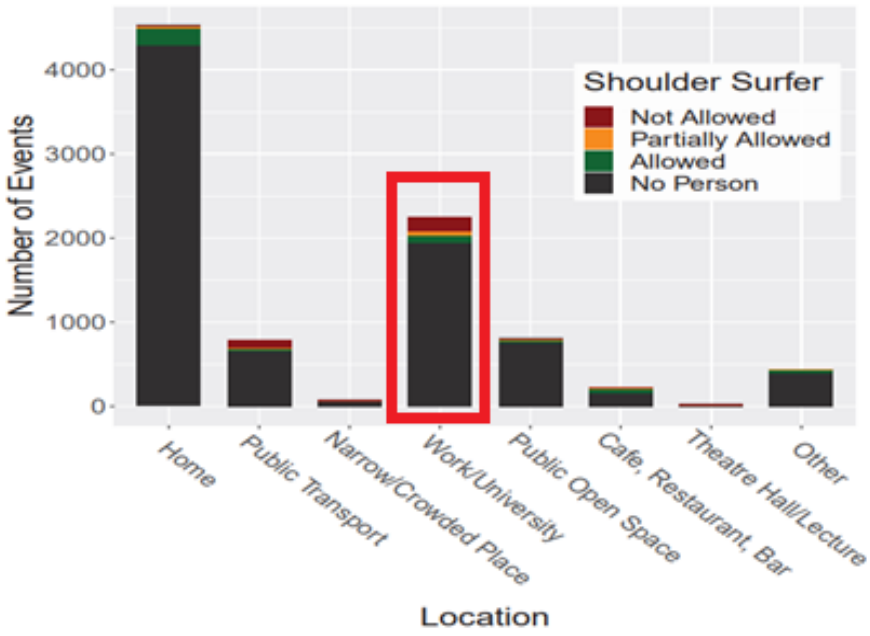

Proteger datos sensibles

# 01. INTRODUCCIÓN

## Justificación




Hackeo Visual (46 empresas, 157 ubicaciones de oficinas, 8 países) (Ponemon Institute, 2016)

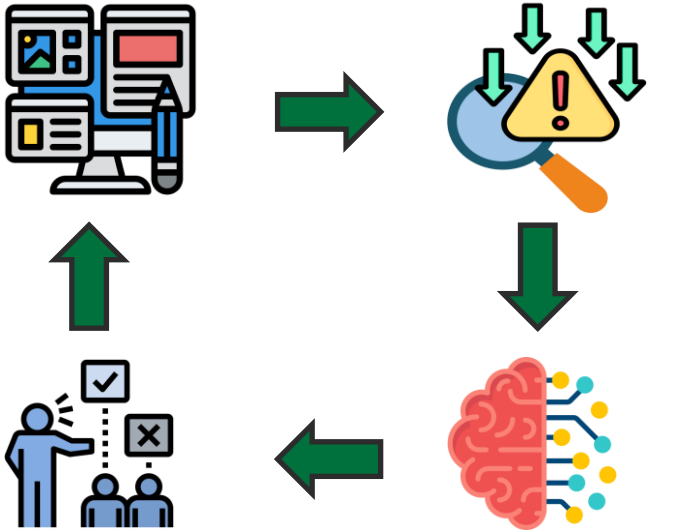



9145 eventos de SSAs en 12 participantes (Schneegass et al., 2022)

# 01. INTRODUCCIÓN

## Objetivos

Objetivo General

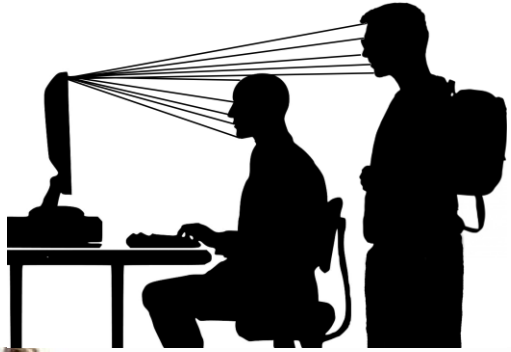


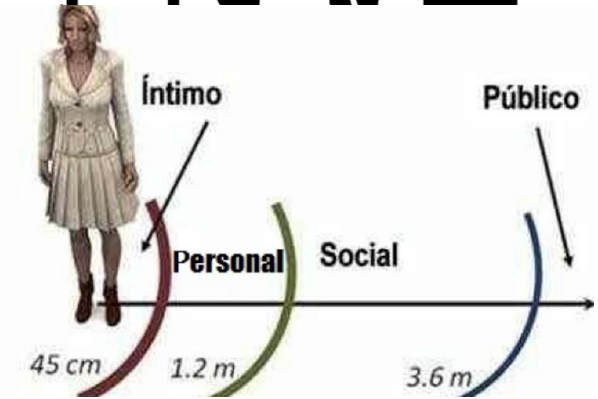

Objetivos Específicos

- Análisis del estado del arte para fundamentar la problemática y soluciones
- Determinar precisión de algoritmos de DL y tecnologías a usar
- Diseñar e implementar el desarrollo de SW
- Realizar pruebas y documentación
- Evaluar e interpretar resultados

# 02. MATERIALES Y TECNOLOGÍAS

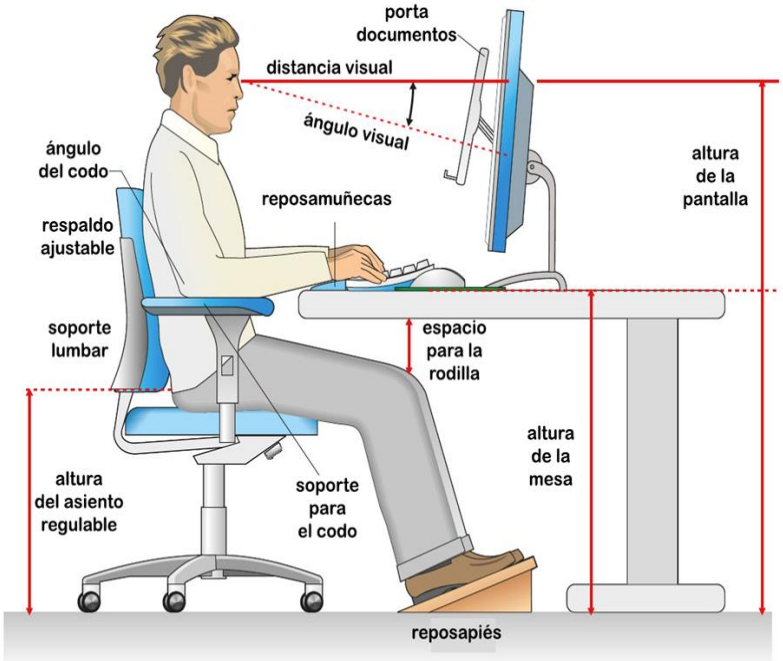
## Marco Teórico






Shoulder Surfing y la Proxémica

Estación de trabajo, posicionamiento del usuario y relación con el Shoulder Surfing



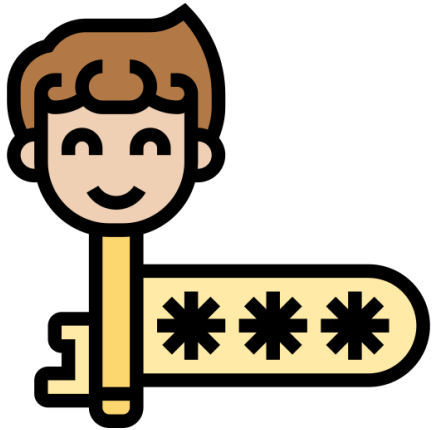
# 02. MATERIALES Y TECNOLOGÍAS

## Marco Teórico

Seguridad de la Información

ISO 27001

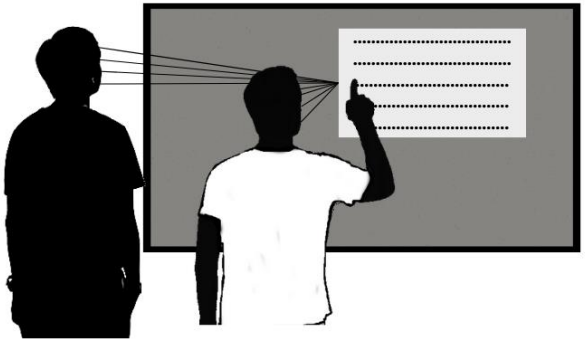
Sistema Gestión de Seguridad de la Información

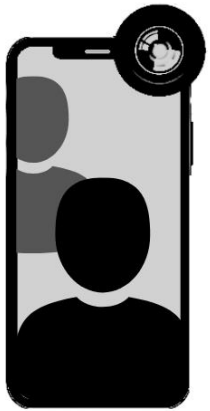


Gestión de Identidad y Acceso

# 02. MATERIALES Y TECNOLOGÍAS

## Estado del Arte



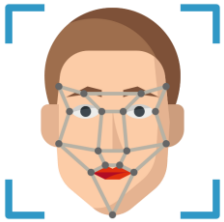


Artefactos y tecnologías que se han utilizado para detectar Shoulder Surfing

Lineamientos para el desarrollo de herramientas para mitigar el Shoulder Surfing

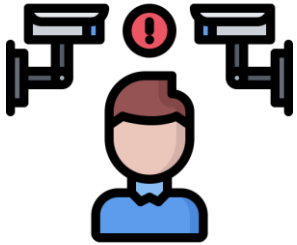
# 02. MATERIALES Y TECNOLOGÍAS

## Estado del Arte



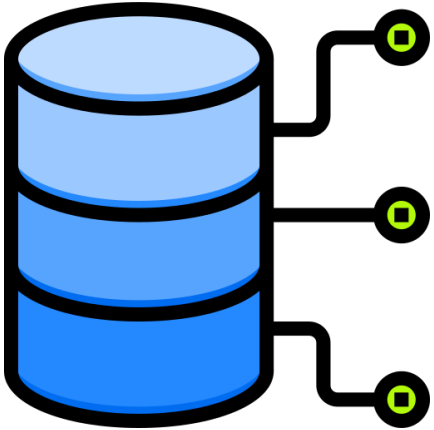
Identificación facial

Cumplimiento de la ley



Videovigilancia


Aplicaciones para la seguridad



Datos personales

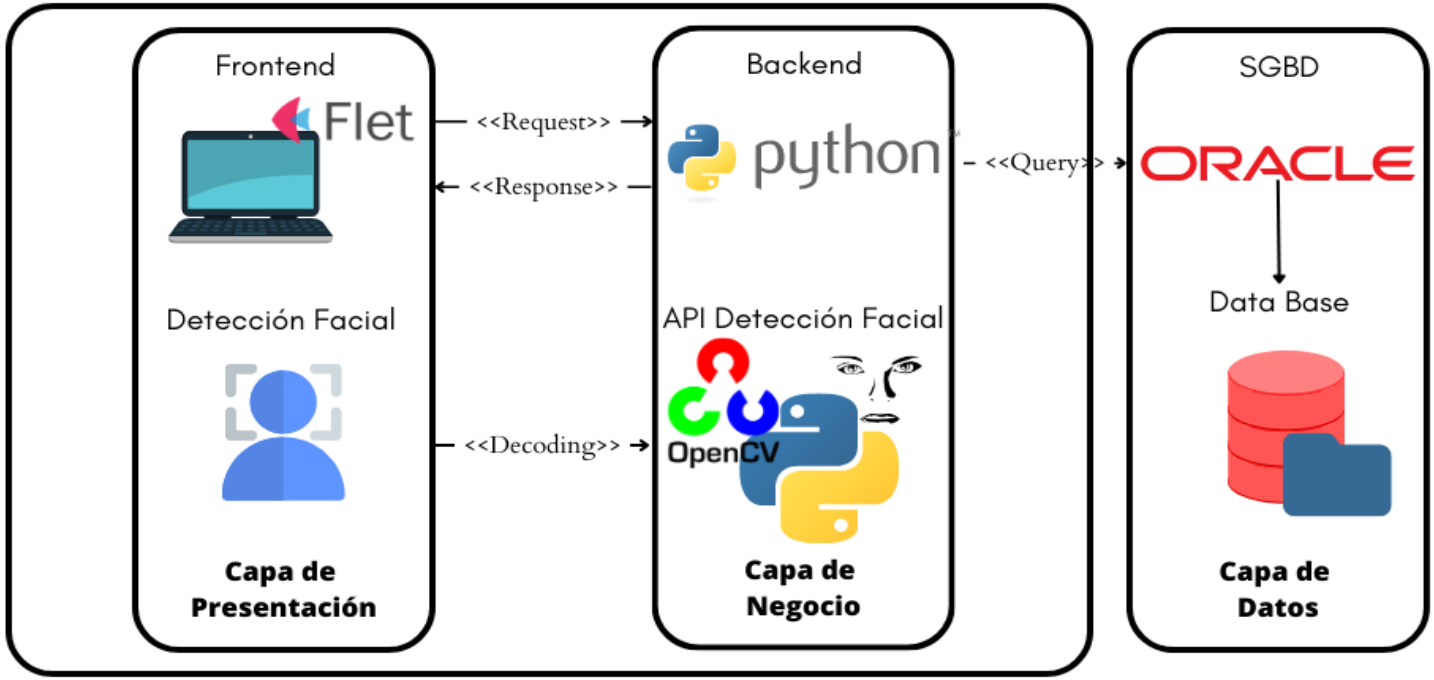
Fotografía

Identificador de PC

# 03. DISEÑO Y DESARROLLO

## Fase de Diseño

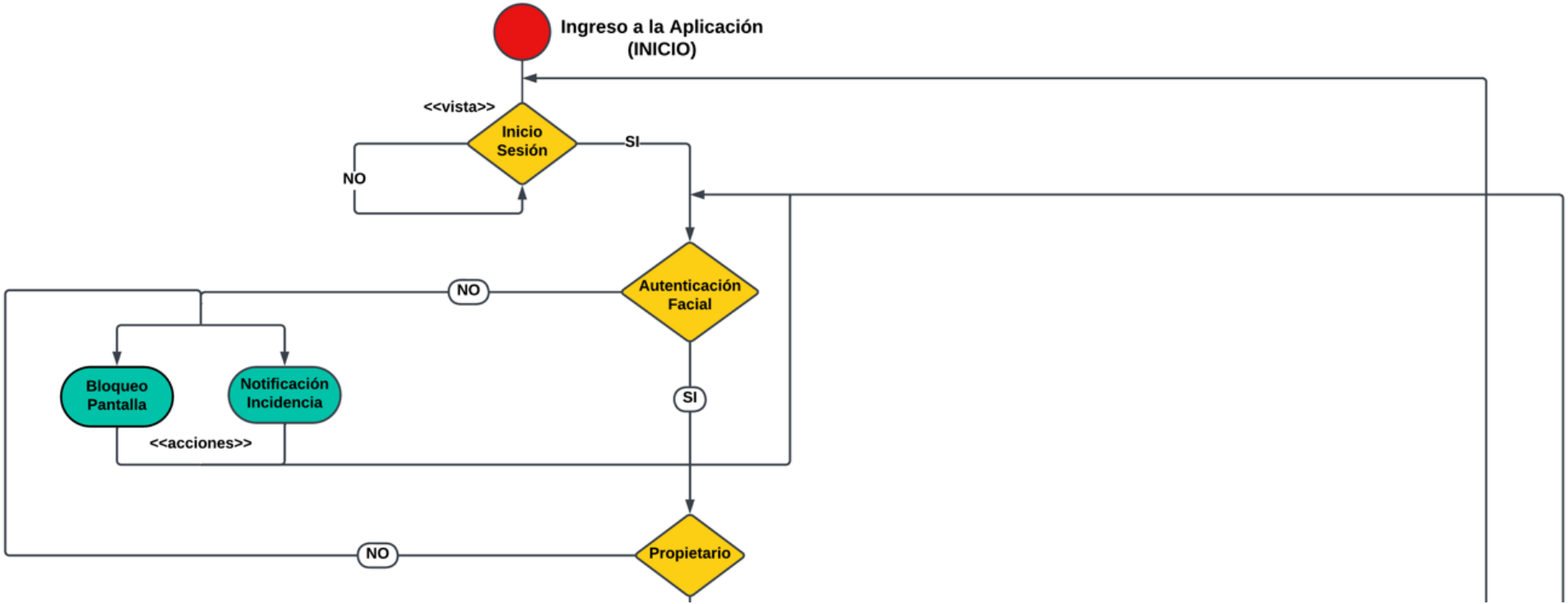
### Arquitectura de Software



# 03. DISEÑO Y DESARROLLO

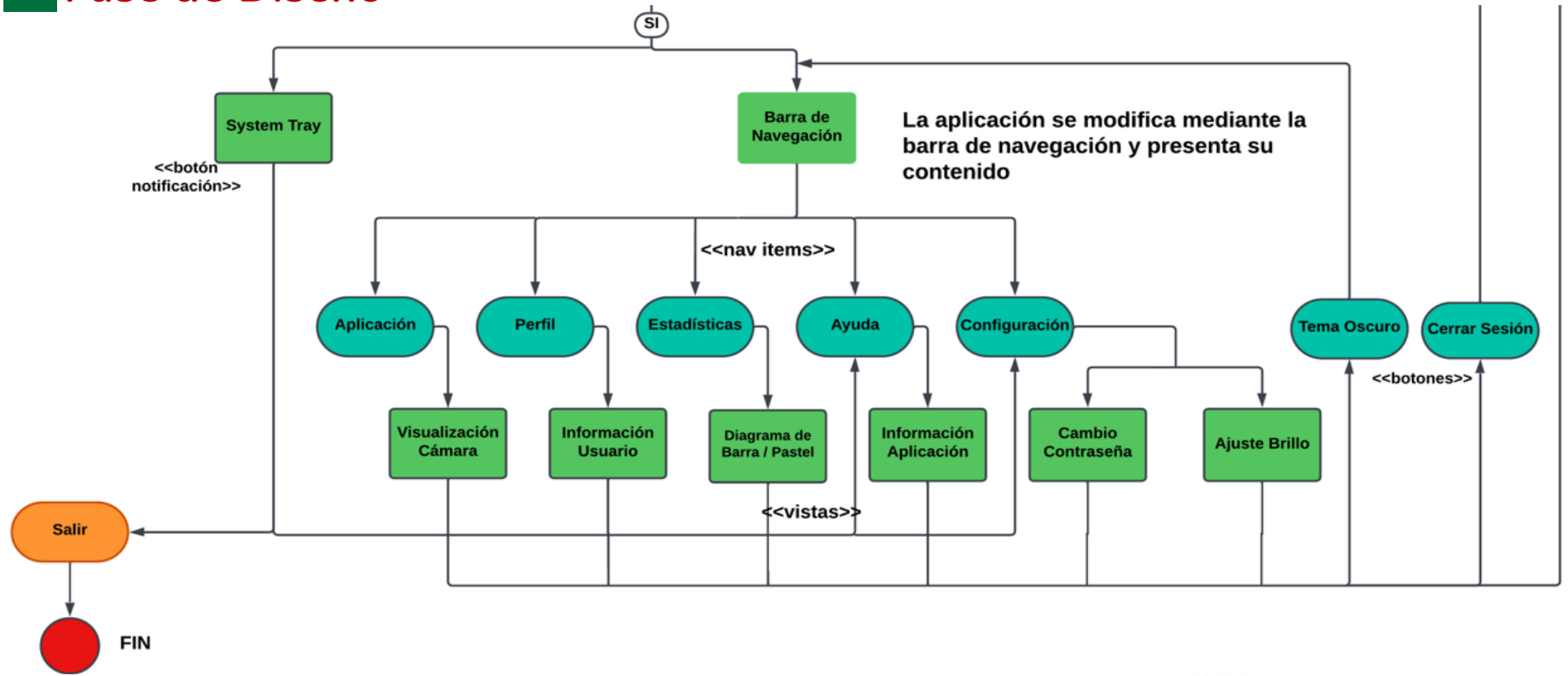
## Fase de Diseño

## Diagrama de Procesos



# 03. DISEÑO Y DESARROLLO

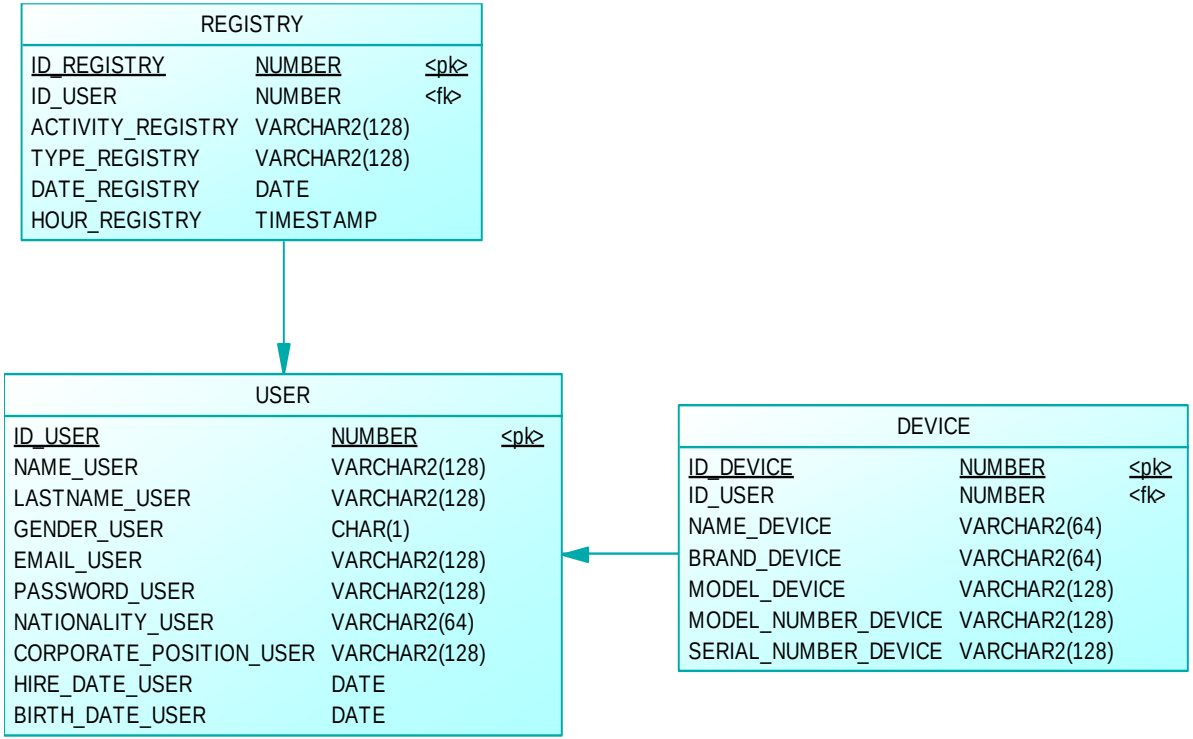
## Fase de Diseño



# 03. DISEÑO Y DESARROLLO

## Fase de Diseño

### Diseño Lógico Base de Datos y Gestor

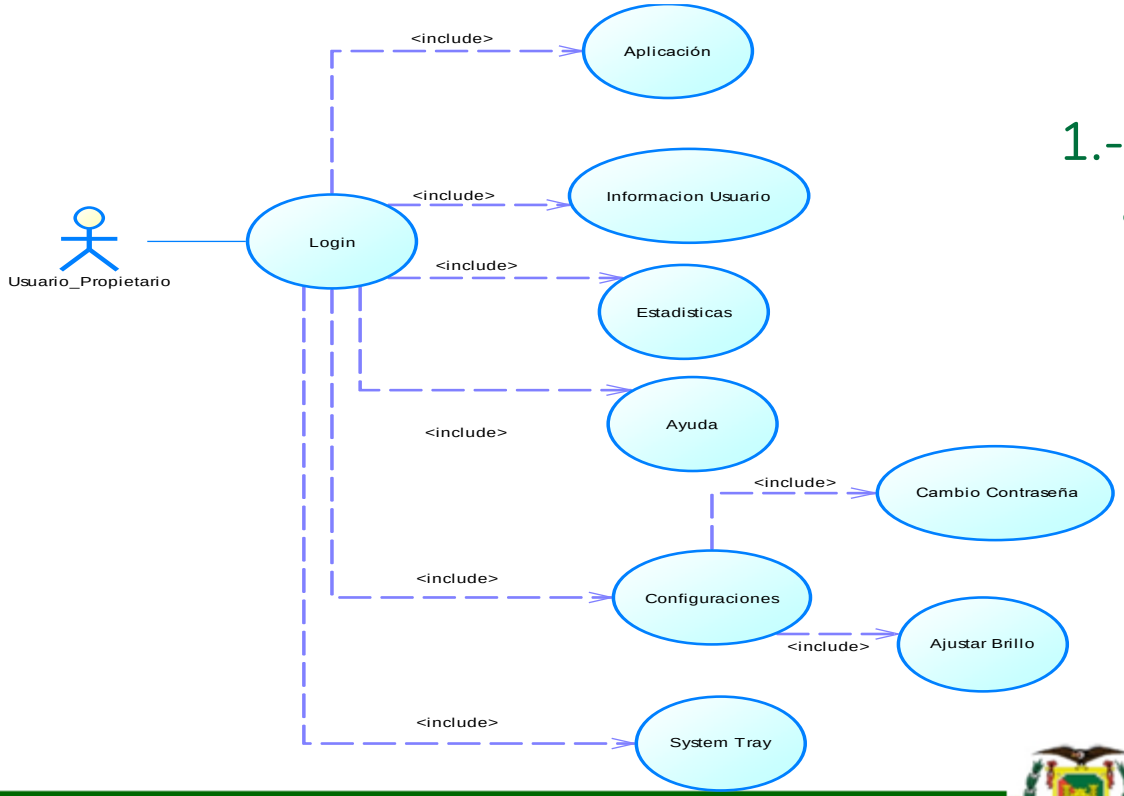



ORACLE DATABASE

# 03. DISEÑO Y DESARROLLO

## Fase de Diseño

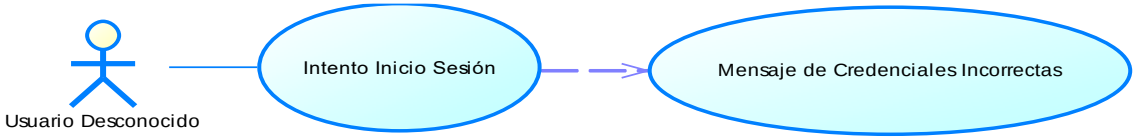
### Casos Uso




1.-Ingresar a la aplicación

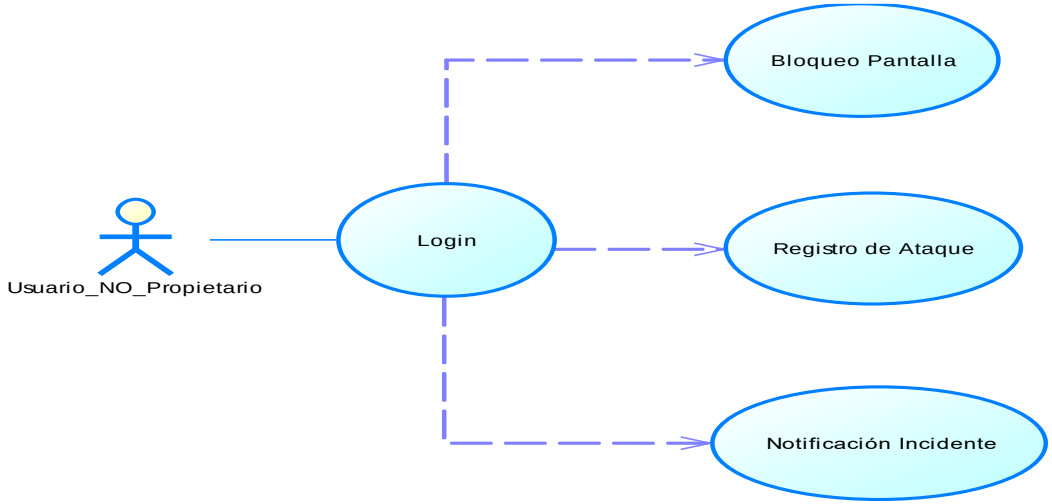
# 03. DISEÑO Y DESARROLLO

## Fase de Diseño




2.- Error de ingreso a la aplicación

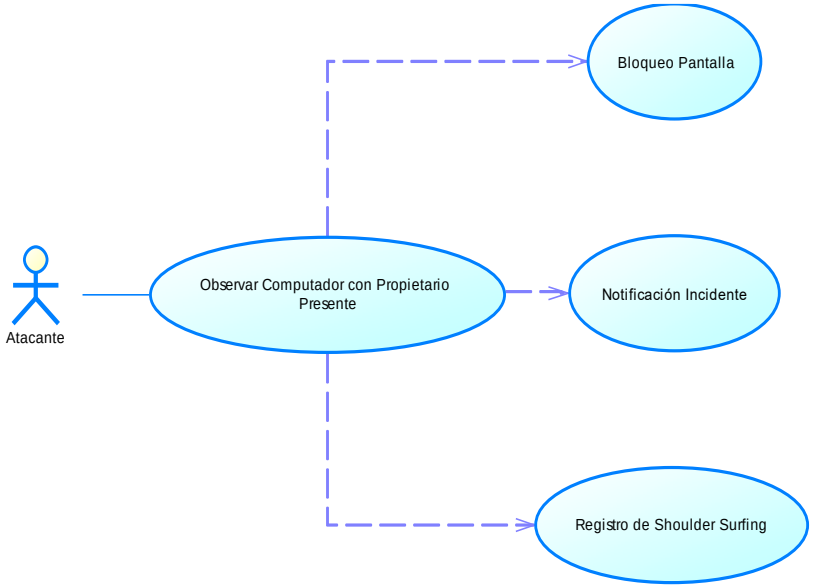
3.-Ingresar a la aplicación con usuario no propietario



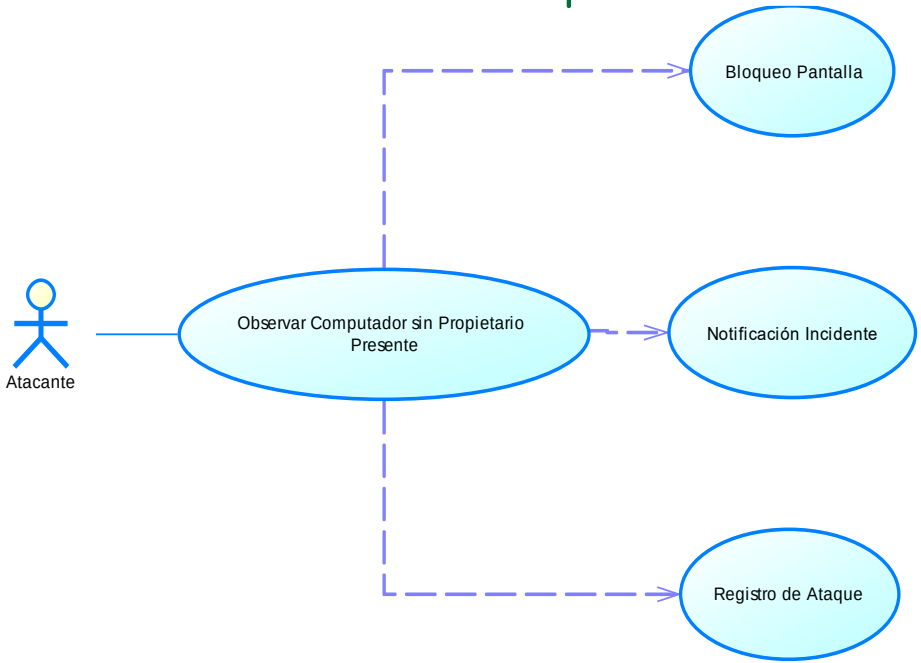
# 03. DISEÑO Y DESARROLLO

## Fase de Diseño

### 4.- Actividad de Shoulder Surfing



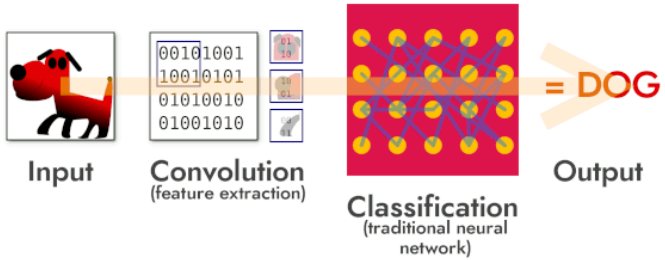

### 5.- Actividad de Ataque



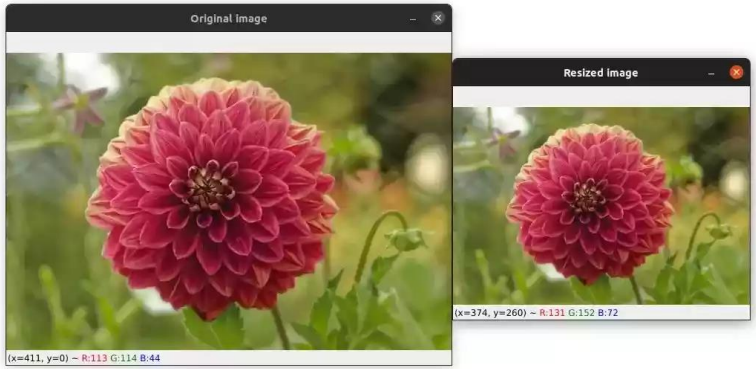
# 03. DISEÑO Y DESARROLLO

## Fase de Desarrollo

### Imágenes y valores reales (BW, RGB)



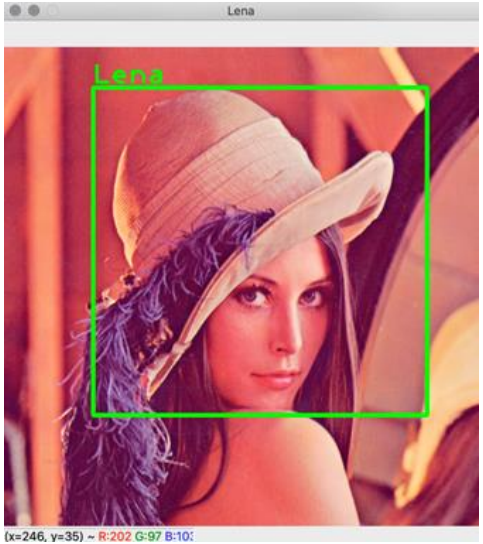

### Redimensión de imágenes





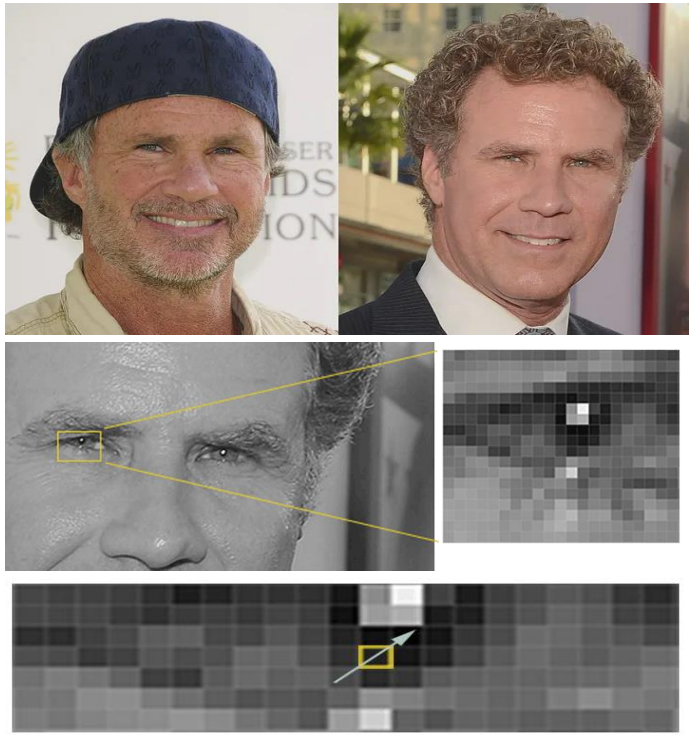
### Efecto espejo

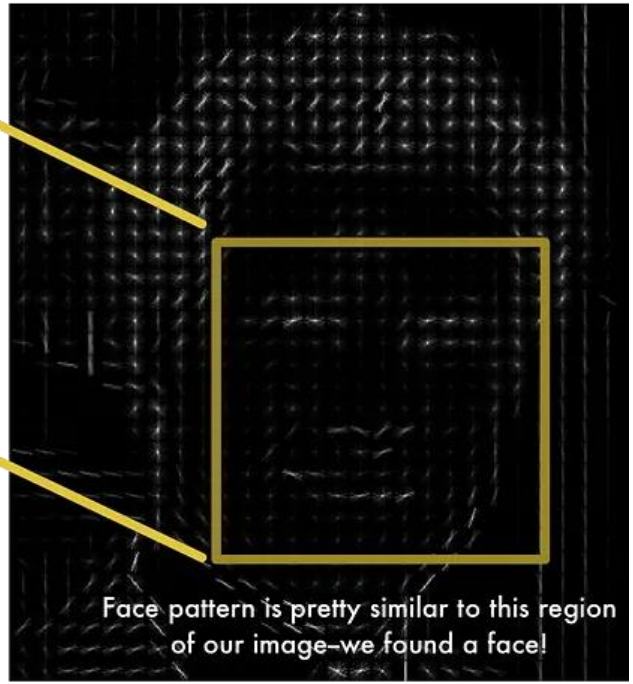
### Enmarcado de rostro



# 03. DISEÑO Y DESARROLLO

## Fase de Desarrollo



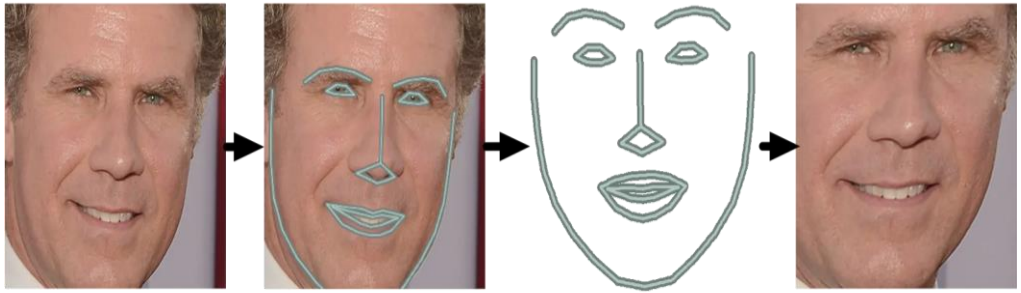



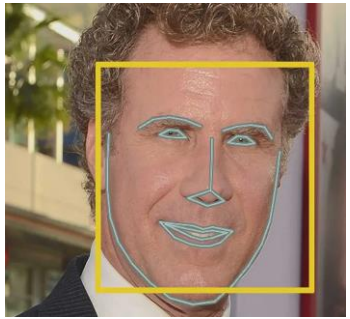

Optimización y Extracción del Gradiente (Geitgey, 2020)

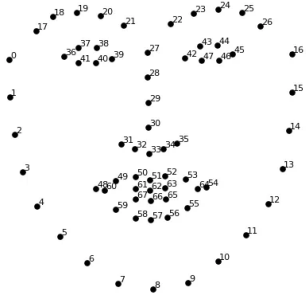
Extracción del Patrón para Detectar Rostros (Geitgey, 2020)

# 03. DISEÑO Y DESARROLLO

## Fase de Desarrollo

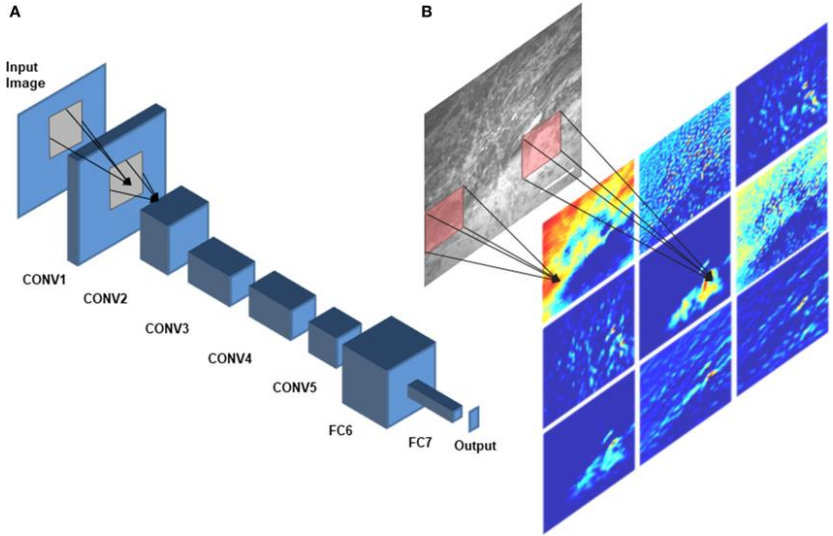






Pasos del Reconocimiento Facial (Geitgey, 2020)

Red Neuronal Convolucional



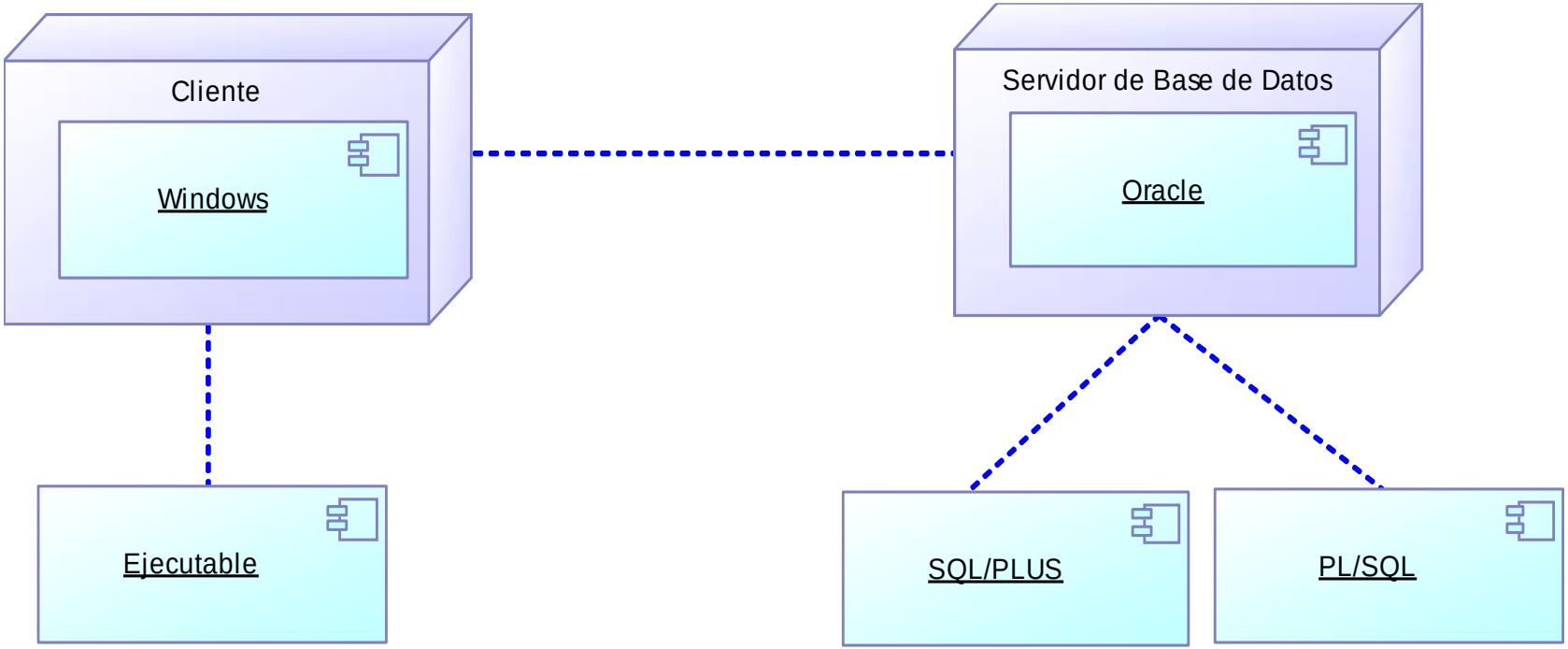

Modelo Computacional

$$Y = F(\text{  })$$

$$Y = \text{Daniela}$$

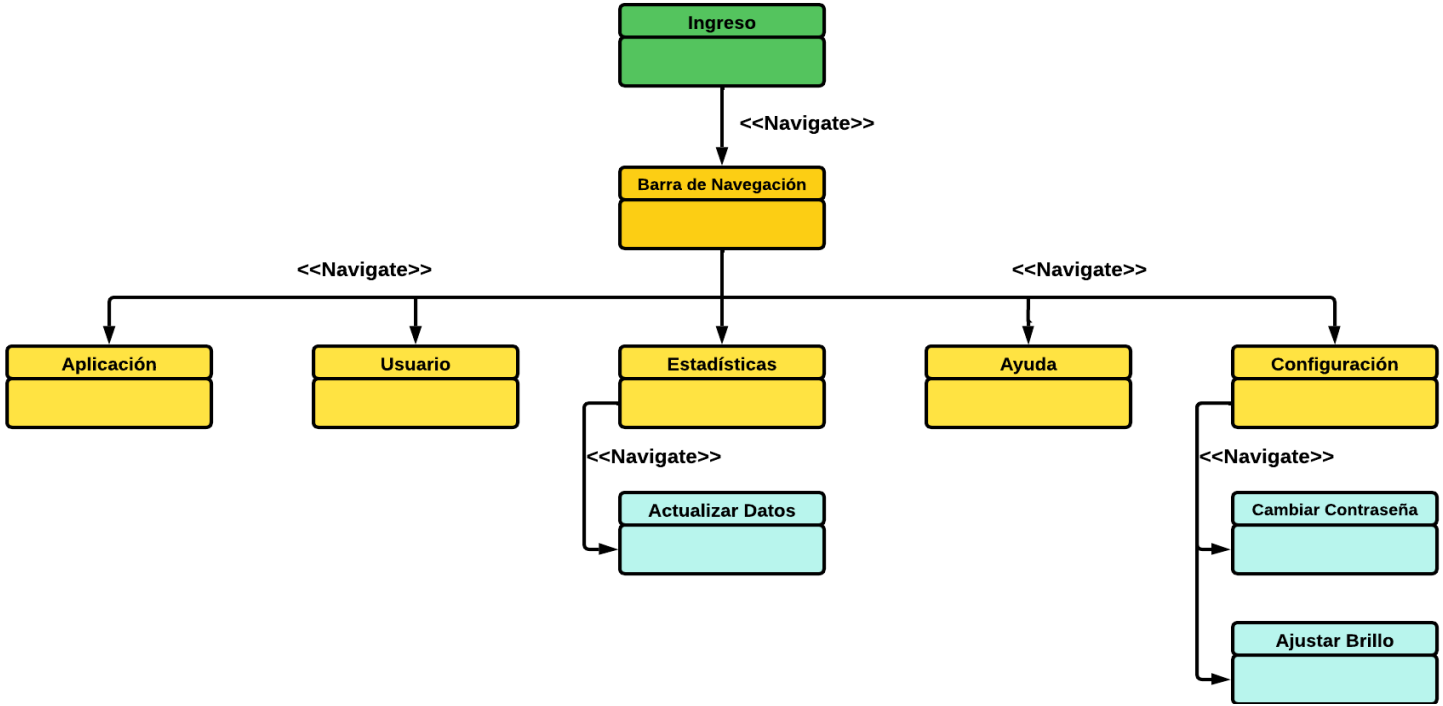
# 04. APLICACIÓN DE LA HERRAMIENTA

## Instalación y Modelo de Despliegue



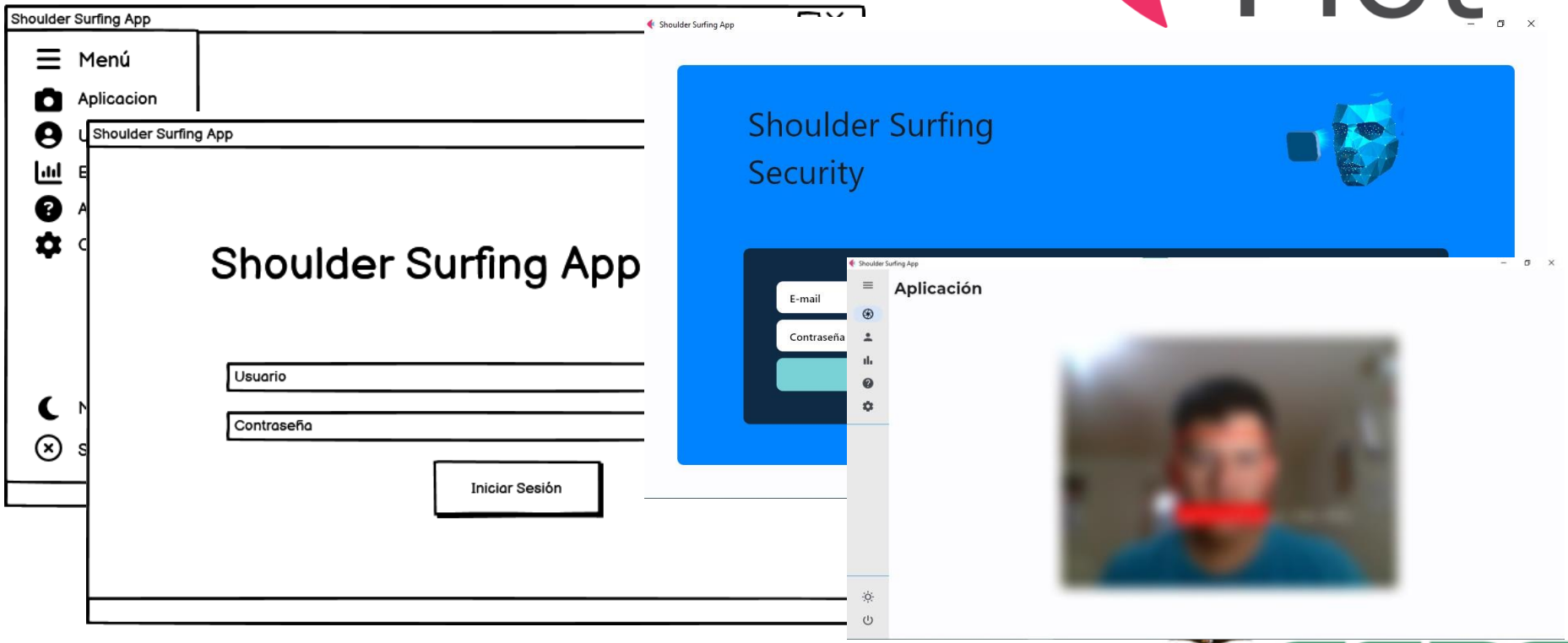
# 04. APLICACIÓN DE LA HERRAMIENTA

## Modelo de Navegación



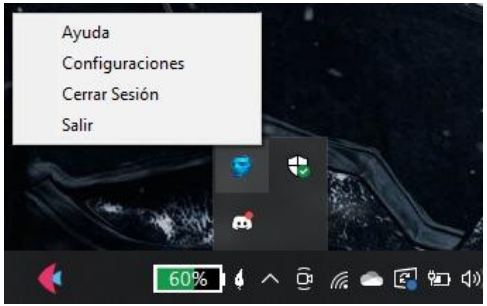
# 04. APLICACIÓN DE LA HERRAMIENTA

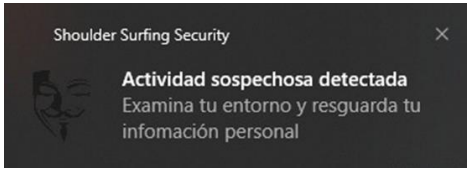
## Puesta en Marcha

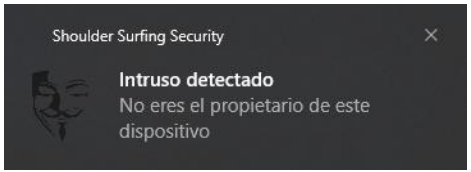


# 04. APLICACIÓN DE LA HERRAMIENTA

## Video Demostrativo

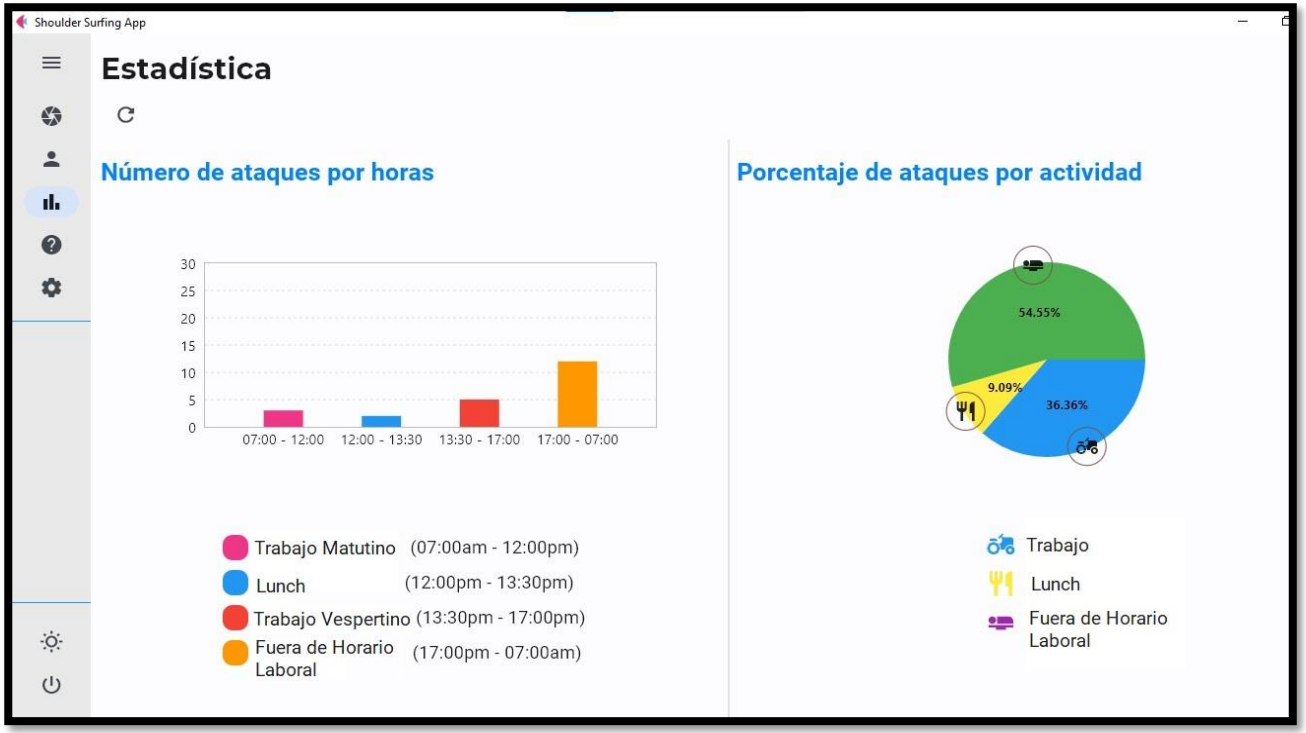




ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

# 05. RESULTADOS

## Generación de Resultados mediante Gráficos Estadísticos




**19.96 %**

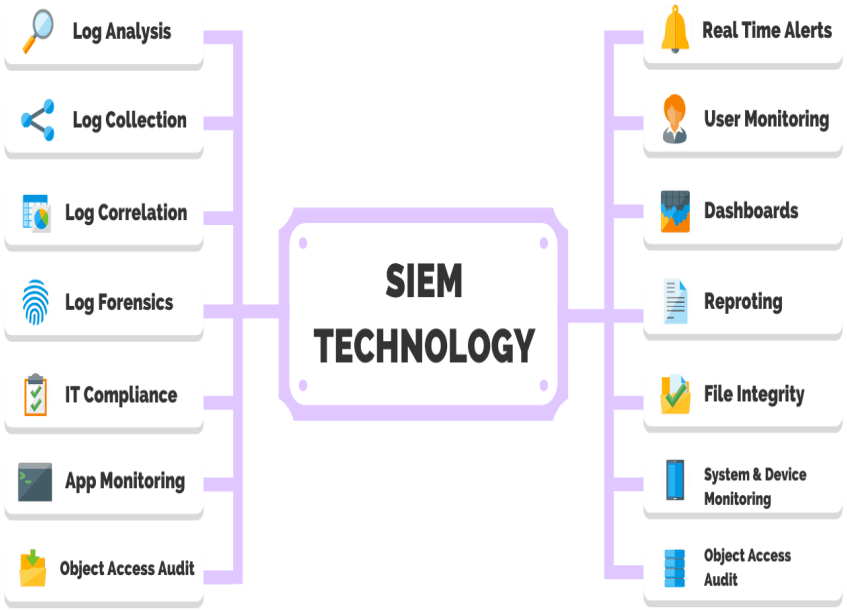
**38.42 %**


**41.61 %**

# 05. RESULTADOS

## Generación de Resultados mediante Archivo Log

### Security Information and Event Management




shoulder_surfing_log.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
Logging started at 2023-07-18 15:06:39.770980
 PRODUCT:              Shoulder Surfing Security
 FILE:                 C:\Users\bryan\Documents\shoulder_surfing_log.txt
 COMPUTER:             DESKTOP-CTTNHB8
 SYSTEM:               Windows 10
 USER:                 bryan
 STARTED:              2023-07-18 15:06:39.770980
------------------------------------------------------------
Suspicious activity detected history:
 bryanzurita                    98.73%                  2023-07-18 15:45:18.850772
 bryanzurita                    93.6%                   2023-07-18 15:48:11.979321
 bryanzurita                    97.27%                  2023-07-18 16:00:16.307452
 bryanzurita                    98.76%                  2023-07-18 16:04:28.513636
 bryanzurita                    96.93%                  2023-07-18 16:05:25.431799
 bryanzurita                    98.78%                  2023-07-18 16:22:55.407043
 Desconocido                    ??.??%                  2023-07-18 17:58:22.278801
 Desconocido                    ??.??%                  2023-07-18 18:10:39.125716
 Desconocido                    ??.??%                  2023-07-18 18:13:18.961217
 santiagobosque                 89.4%                   2023-07-18 22:45:02.926824
 santiagobosque                 81.37%                  2023-07-19 00:29:36.249171
 santiagobosque                 81.99%                  2023-07-19 00:39:58.239265
 santiagobosque                 88.88%                  2023-07-19 00:40:28.881159
 Desconocido                    ??.??%                  2023-07-19 12:13:27.195395
```

# 05. RESULTADOS

## Análisis de Tiempos de Respuesta según el Número de Rostros

| # Imágenes | t1 | t2 | t3 | t4 | t5 | Promedio |
|---|---|---|---|---|---|---|
| 5 | 5.01 | 5.32 | 5.06 | 5.17 | 5.16 | 5.14 |
| 10 | 8.51 | 8.60 | 8.53 | 8.59 | 8.61 | 8.57 |
| 15 | 11.05 | 10.92 | 11.01 | 11.13 | 10.89 | 11.00 |
| 20 | 14.02 | 14.43 | 14.02 | 14 | 14.16 | 14.13 |
| 25 | 17.29 | 17.22 | 17.5 | 17.64 | 17.25 | 17.38 |

| # Imágenes | Promedio | Incremento según el Valor Anterior |
|---|---|---|
| 5 | 5.14 | |
| 10 | 8.57 | 3.42 |
| 15 | 11.00 | 2.43 |
| 20 | 14.13 | 3.13 |
| 25 | 17.38 | 3.25 |
| **Promedio de Incremento** | **≈** | **3.06** |

**5**
t ≈ 5.14s

**10**
t ≈ 8.57s

**20**
t ≈ 14.13s

**50**
t ≈ 32.68s

**100**
t ≈ 63.28s

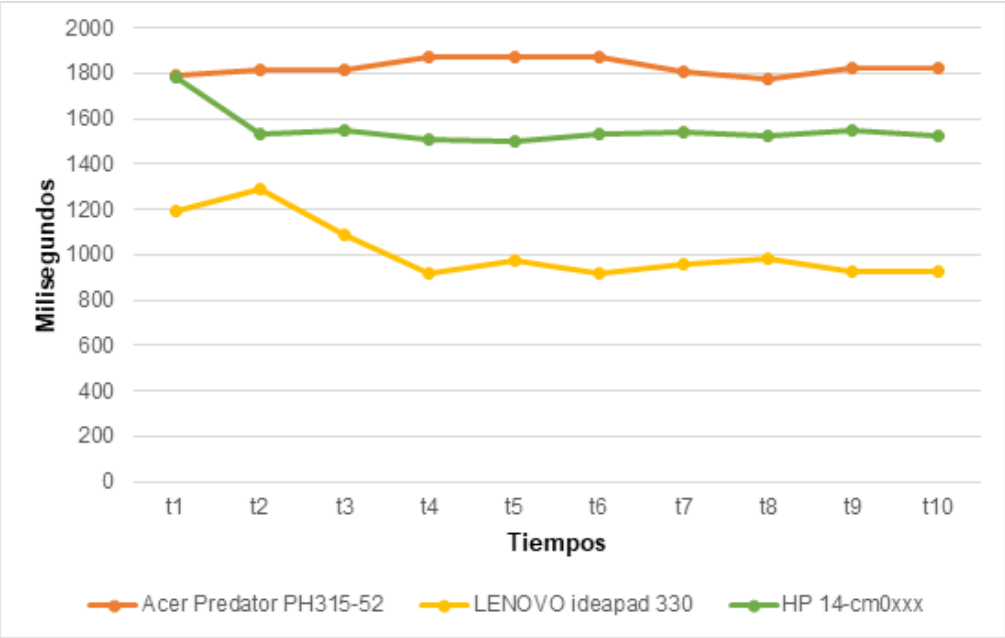
**500**
t ≈ 308.08s

Tiempo ≈ Pendiente * Número de imágenes + (Intercepto – Promedio de Incremento)

**Tiempo ≈ 0.612 * Número de imágenes + 2.08**

# 05. RESULTADOS

## Análisis de Tiempos de Respuesta para la Mitigación




| Dispositivo | Resolución de Webcam | Sistema operativo | CPU | Memoria | Disco |
|---|---|---|---|---|---|
| **Acer Predator PH315-52** | 1280x720 HD | Windows 11 Home 64-bit | Intel Core i7-9750H - 2.60GHz | SODIMM 16GB - 2667 MHz | SSD NVMe - 250GB |
| **LENOVO ideapad 330** | 640x480 | Windows 10 Home 64-bit | Intel Core i3-8130U - 2.20GHz | SODIMM 12GB - 2133MHz | HDD - 1TB |
| **HP 14-cm0xxx** | 640x360 | Windows 10 Home Single Language 64-bit | AMD A9-9425 RADEON R5 - 3.1GHz | SODIMM 8GB - 1866MHZ | HDD - 1TB |

# 06. CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

- Con la implementación técnicas de Deep Learning se logró desarrollar un modelo de software el cual puede detectar y mitigar ataques de Ingeniería Social “Shoulder Surfing” permitiendo así aumentar los niveles de seguridad de la información.

- Se encontró y analizo bases teóricas los cuales ayudan a consolidar los fundamentos correspondientes a la problemática y las posibles soluciones tecnológicas.

- Con el apoyo de LFW Labeled Faces in the Wild se consiguió determinar la precisión y margen de error de los algoritmos de Deep Learning, además se diseñó la arquitectura de software incluyendo programas, algoritmos reutilizables, diseño de la base de datos, diseño de interfaces, usabilidad y navegabilidad.

- Se realizaron pruebas del modelo de desarrollo de software y se realizó la documentación correspondiente según el progreso y las acciones.

- Se evaluaron e interpretaron cada uno de los resultados obtenidos tras la validación e implantación del modelo de desarrollo de software.

# 06. CONCLUSIONES Y RECOMENDACIONES

## Recomendaciones

- Es recomendable que para obtener un correcto funcionamiento del aplicativo se lo implemente en un lugar adecuado, que tenga las condiciones de luz optimas, sistema de videovigilancia, estaciones de trabajo limpias sin obstáculos, y constante actualización de fotografías.

- Se puede acoplar a otros ámbitos como el académico, siendo una herramienta que impida la copia en exámenes en línea o que una persona que no es la que deba rendir el examen pueda hacerlo.

- Aplicar un constante versionamiento, en el cual se pueden implementar mejoras, corrección de errores, optimización de rendimiento y actualizaciones de seguridad.

- Es indispensable realizar capacitaciones constantes en el ámbito tecnológico y socializar la variedad de artefactos y herramientas como la desarrollada en este estudio.

# ¡GRACIAS!

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA