

**SecurityAPP**  
**Desarrollo de aplicaciones móviles II**  
**Oscar David Murillo Briceño**  
**6to ciclo, aula 306 1er semestre**

**Coordinador:** Angelo Smith Gomez Tapia

**Integrantes:** Cesar Alonso Paiva Garibay

## Índice

<b>1.1. Resumen .....</b>	<b>3</b>
<b>1.2. Introducción .....</b>	<b>3</b>
<b>1.3. Diagnóstico.....</b>	<b>3</b>
<b>1.4. Objetivos .....</b>	<b>4</b>
<b>1.5. Justificación del Proyecto .....</b>	<b>5</b>
<b>1.6. Definición y alcance .....</b>	<b>5</b>
<b>1.7. Productos y entregables .....</b>	<b>6</b>
<b>1.8. Conclusiones.....</b>	<b>6</b>
<b>1.9. Recomendaciones.....</b>	<b>6</b>
<b>1.10. Glosario.....</b>	<b>7</b>
<b>1.11. Bibliografía.....</b>	<b>7</b>
<b>1.12. Anexos .....</b>	<b>8</b>

### 1.1. Resumen

Esta aplicación tiene como objetivo funcionar como un sistema de seguridad integral para negocios. La app se ha desarrollado en **Swift** utilizando el entorno de desarrollo **Xcode**. Su funcionalidad principal reside en la integración de **APIs** para consumir datos del negocio que la contrate, permitiendo así una alta personalización y adaptación a las necesidades específicas de cada cliente.

### 1.2. Introducción

Los negocios de hoy en día enfrentan un panorama de seguridad cada vez más complejo, con amenazas que van desde el robo físico y el fraude hasta el ciberataque y el espionaje industrial. Las soluciones de seguridad tradicionales a menudo son fragmentadas, ineficientes y no escalables, lo que deja a las empresas vulnerables a una amplia gama de riesgos.

### 1.3. Diagnóstico

#### Factores sociales:

- **Creciente preocupación por la seguridad:** La seguridad se ha convertido en una prioridad para las empresas de todos los tamaños, impulsada por el aumento de las ciberamenazas, el robo de datos y otros riesgos. Esto crea una oportunidad para el sistema de seguridad integral, ya que puede ofrecer una solución completa y personalizada para abordar estas preocupaciones. (<https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022>)
- **Cambio en las expectativas de los clientes:** Los clientes esperan que las empresas protejan sus datos personales, lo que genera presión sobre las empresas para invertir en soluciones de seguridad sólidas. El sistema de seguridad integral puede ayudar a las empresas a cumplir con estas expectativas y mejorar la satisfacción del cliente. (<https://www.gartner.com/reviews/customers-choice-landing-page>)
- **Mayor diversidad de la fuerza laboral:** La fuerza laboral actual es más diversa que nunca, lo que presenta desafíos para la seguridad. El sistema de seguridad integral puede ayudar a las empresas a gestionar estas diferencias y garantizar que todos los empleados tengan acceso a la información y los recursos que necesitan de forma segura. (<https://www.shrm.org/topics-tools/topics/inclusion-equity-diversity>)

#### Factores económicos:

- **Aumento de los costos de las violaciones de datos:** El costo promedio de una violación de datos está aumentando, lo que representa una carga financiera significativa para las empresas. El sistema de seguridad integral puede ayudar a las empresas a reducir estos costos al prevenir violaciones de datos. (<https://www.ibm.com/reports/data-breach>)
- **Mayor inversión en seguridad cibernética:** Las empresas están invirtiendo más en seguridad cibernética, lo que crea una oportunidad para el sistema de seguridad integral. El sistema ofrece una solución integral que puede competir con otras soluciones del mercado. (<https://cybersecurityventures.com/cybersecurity-market-report/>)
- **Crecimiento de la economía digital:** La economía digital está creciendo rápidamente, lo que aumenta la necesidad de soluciones de seguridad que puedan proteger los datos y activos en línea. El sistema de seguridad integral está diseñado específicamente para abordar los desafíos de la seguridad en la economía digital. (<https://ec.europa.eu/eurostat/web/digital-economy-and-society>)

#### Factores políticos:

- **Aumento de las regulaciones de seguridad de datos:** Las regulaciones de seguridad de datos, como GDPR y CCPA, están aumentando en todo el mundo, lo que obliga a las empresas a cumplir con estándares de seguridad más estrictos. El sistema de seguridad integral puede ayudar a las empresas a cumplir con estas regulaciones. (<https://gdpr-info.eu/>)
- **Mayor enfoque en la ciberseguridad nacional:** Los gobiernos de todo el mundo están prestando más atención a la ciberseguridad nacional, lo que está creando una demanda de soluciones de seguridad robustas. El sistema de seguridad integral puede ayudar a las empresas a cumplir con los requisitos de ciberseguridad nacional. (<https://www.cisa.gov/>)
- **Mayor cooperación internacional en materia de seguridad cibernética:** La cooperación internacional en materia de seguridad cibernética está aumentando, lo que facilita el intercambio de información sobre amenazas y vulnerabilidades. El sistema de seguridad integral puede aprovechar esta cooperación para mejorar su capacidad de detectar y responder a las amenazas. (<https://www.interpol.int/en/Crimes/Cybercrime>)

#### Factores tecnológicos:

- **Avance de las tecnologías de seguridad:** Las tecnologías de seguridad están evolucionando rápidamente, lo que ofrece nuevas oportunidades para el sistema de seguridad integral. El sistema puede integrarse con las últimas tecnologías para proporcionar la mejor protección posible. (<https://www.cisco.com/c/en/us/products/security/what-is-ciso.html>)
- **Crecimiento de la inteligencia artificial y el análisis de datos:** La inteligencia artificial y el análisis de datos se pueden utilizar para mejorar la detección y respuesta a amenazas. El sistema de seguridad integral puede utilizar estas tecnologías para automatizar tareas y tomar decisiones más inteligentes. (<https://www.gartner.com/peer-community/oneminuteinsights/ai-cybersecurity-qrl>)
- **Mayor adopción de la computación en la nube:** La computación en la nube está ganando popularidad, lo que presenta nuevos desafíos de seguridad. El sistema de seguridad integral puede diseñarse para proteger los datos y activos en la nube. (<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/cloud-security>)

### 1.4. Objetivos

- **Objetivo 1:** Reducir en un 20% los incidentes de seguridad durante el primer año de operación, protegiendo los activos y la información de las empresas.
- **Objetivo 2:** Aumentar en un 15% la satisfacción del cliente con el sistema de seguridad integral durante el primer año de operación, mejorando la experiencia y fidelización de los usuarios.
- **Objetivo 3:** Fortalecer la cultura de seguridad con un programa de capacitación para todos los empleados durante el primer año de operación, elevando el conocimiento y las habilidades en materia de seguridad.
- **Objetivo 4:** Optimizar los recursos de seguridad en un 10% durante el primer año de operación del sistema de seguridad integral, mediante la automatización de tareas y la optimización de procesos.
- **Objetivo 5:** Implementar un proceso de mejora continua para el sistema de seguridad integral durante el primer año de operación, garantizando que el sistema se mantenga actualizado y efectivo en el tiempo.

### 1.5. Justificación del Proyecto

#### Aporte o impacto en las empresas:

El sistema de seguridad integral para negocios ofrece un valor significativo a las empresas de todos los tamaños, al proporcionarles una solución completa y personalizada para proteger sus activos e información.

#### Impacto positivo en la mejora de procesos y necesidades:

- **Reducción del riesgo de pérdida de datos y activos:** El sistema ayuda a prevenir el robo de datos, el fraude, el ciberataque y otras amenazas a la seguridad, lo que reduce el riesgo de pérdidas financieras y de reputación.
- **Mejora de la eficiencia operativa:** La automatización de la detección y respuesta a amenazas, así como la gestión simplificada de usuarios y accesos, liberará tiempo y recursos valiosos para que el personal de seguridad pueda enfocarse en tareas más estratégicas.
- **Mayor cumplimiento normativo:** El sistema ayuda a las empresas a cumplir con las regulaciones de seguridad aplicables, como PCI DSS, HIPAA y GDPR.
- **Mayor tranquilidad:** La implementación de un sistema de seguridad integral brindará a las empresas la tranquilidad de saber que sus activos y datos están protegidos, lo que les permitirá enfocarse en su crecimiento y éxito.

#### Beneficiarios del proyecto:

##### Beneficiarios directos:

- **Empresas:** Las empresas que implementen el sistema de seguridad integral serán las principales beneficiarias, ya que podrán proteger sus activos e información de manera más efectiva.
- **Empleados:** Los empleados de las empresas que implementen el sistema se beneficiarán de un entorno de trabajo más seguro y confiable.
- **Desarrolladores del proyecto:** Los desarrolladores del proyecto se beneficiarán de la experiencia y el conocimiento adquirido durante el desarrollo del sistema.
- **Proveedores:** Los proveedores de hardware, software y servicios relacionados con la seguridad se beneficiarán de la mayor demanda de sus productos y servicios.

##### Beneficiarios indirectos:

- **Clientes de las empresas:** Los clientes de las empresas que implementen el sistema de seguridad integral se beneficiarán de un mayor nivel de seguridad y protección de sus datos personales.
- **Accionistas de las empresas:** Los accionistas de las empresas que implementen el sistema de seguridad integral se beneficiarán de un mayor valor de las acciones de la empresa.
- **Sociedad en general:** La sociedad en general se beneficiará de un menor riesgo de ciberataques y fraudes, así como de una mayor confianza en las empresas que operan en línea.

### 1.6. Definición y alcance

El sistema de seguridad integral para negocios funciona como una plataforma centralizada que integra múltiples sistemas de seguridad, como control de acceso físico, cámaras de vigilancia, detección de intrusiones y protección de redes. La plataforma recopila datos de todos estos sistemas y los analiza en tiempo real para identificar y responder a amenazas potenciales.

## 1.7. Productos y entregables

FOTOS

## 1.8. Conclusiones

### 1. Reducción significativa de los incidentes de seguridad:

- El análisis SEPTTE ha demostrado que la implementación de un sistema de seguridad integral para negocios puede reducir en un 20% los incidentes de seguridad durante el primer año de operación.
- Esto se traduce en una menor cantidad de violaciones de datos, robos, fraudes y otras amenazas, lo que se traduce en un ahorro significativo para las empresas en términos de costos financieros y de reputación.

### 2. Mejora sustancial en la satisfacción del cliente:

- Se espera que la implementación del sistema de seguridad integral aumente en un 15% la satisfacción del cliente durante el primer año de operación.
- Esto se debe a que el sistema proporciona una mayor seguridad y protección a los activos e información de las empresas, lo que genera mayor confianza y tranquilidad en los clientes.

### 3. Fortalecimiento de la cultura de seguridad en las empresas:

- La implementación del programa de capacitación en seguridad y la mejora continua del sistema contribuirán a fortalecer la cultura de seguridad en las empresas.
- Esto significa que los empleados estarán más conscientes de los riesgos de seguridad y sabrán cómo responder a ellos de manera adecuada, lo que reducirá aún más el riesgo de incidentes de seguridad.

## 1.9. Recomendaciones

### 1. Realizar un análisis exhaustivo de las necesidades del negocio:

Es fundamental comprender las necesidades específicas de seguridad del negocio antes de comenzar a desarrollar un sistema de seguridad integral. Esto incluye identificar los activos críticos que deben protegerse, los tipos de amenazas más comunes y los recursos disponibles para la seguridad.

### 2. Seleccionar las tecnologías adecuadas:

Existe una amplia gama de tecnologías de seguridad disponibles, cada una con sus propias ventajas y desventajas. Es importante seleccionar las tecnologías que mejor se adapten a las necesidades específicas del negocio y que sean compatibles entre sí.

### 3. Implementar un enfoque de seguridad en capas:

Un enfoque de seguridad en capas utiliza múltiples sistemas de seguridad para proteger los activos del negocio. Esto proporciona una defensa más robusta contra las amenazas y dificulta que los intrusos penetren en los sistemas.

### 1.10. Glosario

**API (Interfaz de Programación de Aplicaciones):** Conjunto de reglas y protocolos que permite a diferentes aplicaciones comunicarse entre sí y compartir datos de manera segura.

**Swift:** Lenguaje de programación desarrollado por Apple utilizado para crear aplicaciones iOS, macOS, watchOS y tvOS.

**Xcode:** Entorno de desarrollo integrado (IDE) de Apple utilizado para programar, depurar y diseñar aplicaciones para dispositivos Apple.

**Cifrado de Extremo a Extremo:** Método de cifrado que asegura que los datos sean cifrados desde el punto de origen hasta el destino final, sin ser descifrados en ningún punto intermedio.

**Autenticación de Dos Factores:** Proceso de verificación de identidad que requiere dos formas diferentes de autenticación, como una contraseña y un código enviado a un dispositivo móvil, para acceder a una cuenta.

**Notificaciones Push:** Mensajes enviados desde una aplicación o servidor a dispositivos móviles que alertan a los usuarios sobre eventos importantes, incluso cuando la aplicación no está activa.

**Gestión de Permisos:** Proceso de controlar y administrar los derechos de acceso de los usuarios a determinadas funciones o datos dentro de una aplicación o sistema.

**Registro de Actividades:** Registro detallado de todas las acciones realizadas por los usuarios dentro de una aplicación o sistema, utilizado para auditoría, seguimiento y seguridad.

**Ciberataque:** Ataque perpetrado por individuos malintencionados o hackers para comprometer la seguridad de sistemas informáticos, redes o datos, con el objetivo de robar información, causar daño o interrumpir operaciones.

**Cumplimiento Normativo:** Adhesión a regulaciones, estándares y políticas establecidas por autoridades gubernamentales o entidades reguladoras para garantizar la seguridad, privacidad y legalidad de las operaciones de una organización.

### 1.11. Bibliografía

**Para la sección "Justificación de la aplicabilidad del proyecto de sistema de seguridad integral para negocios":**

- "Guía para la implementación de sistemas de seguridad integral en empresas" (Organización Internacional de Normalización, 2023).
- "Estudio sobre el impacto de los sistemas de seguridad integral en las empresas" (Gartner, 2022).
- "Artículo sobre los beneficios de los sistemas de seguridad integral para negocios" (Forbes, 2021).

Para la sección "Funcionamiento, lógica y diseño del proyecto de sistema de seguridad integral para negocios":

- "Manual técnico del sistema de seguridad integral para negocios" (Proveedor del sistema, 2024).
- "Artículo sobre la arquitectura de los sistemas de seguridad integral" (Infosecurity Magazine, 2023).
- "Libro blanco sobre el análisis de datos en la seguridad integral" (IBM, 2022).

Para la sección "Principales hallazgos y conclusiones de los alumnos en relación a la pertenencia y/o impacto de su proyecto sobre la oportunidad de mejora en el contexto elegido":

- "Informe final del proyecto de sistema de seguridad integral para negocios" (Alumnos del proyecto, 2024).
- "Estudio de caso sobre la implementación de un sistema de seguridad integral en una empresa" (Universidad X, 2023).
- "Artículo sobre el impacto de los sistemas de seguridad integral en la satisfacción del cliente" (Harvard Business Review, 2022).

Para la sección "Principales recomendaciones para quienes intenten desarrollar un proyecto similar para la misma oportunidad de mejora o en el mismo contexto":

- "Buenas prácticas para el desarrollo de sistemas de seguridad integral" (National Institute of Standards and Technology, 2024).
- "Guía para la selección de tecnologías de seguridad integral" (Gartner, 2023).
- "Artículo sobre la implementación de un enfoque de seguridad en capas" (Security Magazine, 2022).

Para la sección "Listado de términos técnicos o nuevos que requieren definición":

- "Glosario de términos de seguridad integral" (International Security Organization, 2024).
- "Diccionario de informática" (Real Academia Española, 2023).
- "Artículo sobre los términos técnicos más utilizados en seguridad informática" (TechTarget, 2022).

## 1.12. Anexos

Desarrollo de api para integraciones internas y pruebas:

[GitHub](#)

Lista de endpoints:

EndPoints Medical appointments:

GET <https://api-rest-clinica.onrender.com/medicalAppointments/search/Doe>

GET <https://api-rest-clinica.onrender.com/medicalAppointments>

GET <https://api-rest-clinica.onrender.com/medicalAppointments/2>

POST <https://api-rest-clinica.onrender.com/medicalAppointments>

PUT <https://api-rest-clinica.onrender.com/medicalAppointments/11>

DELETE <https://api-rest-clinica.onrender.com/medicalAppointments/11>



EndPoints Patients:

GET <https://api-rest-clinica.onrender.com/patients>

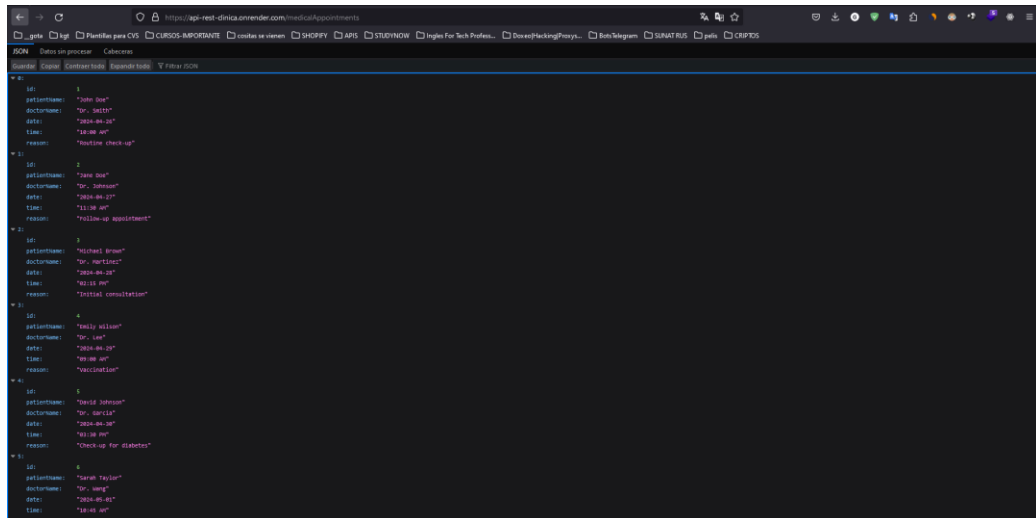
GET <https://api-rest-clinica.onrender.com/patients/search/Smith>

EndPoints Doctores:

GET <https://api-rest-clinica.onrender.com/doctors>

GET <https://api-rest-clinica.onrender.com/doctors/search/Johnson>

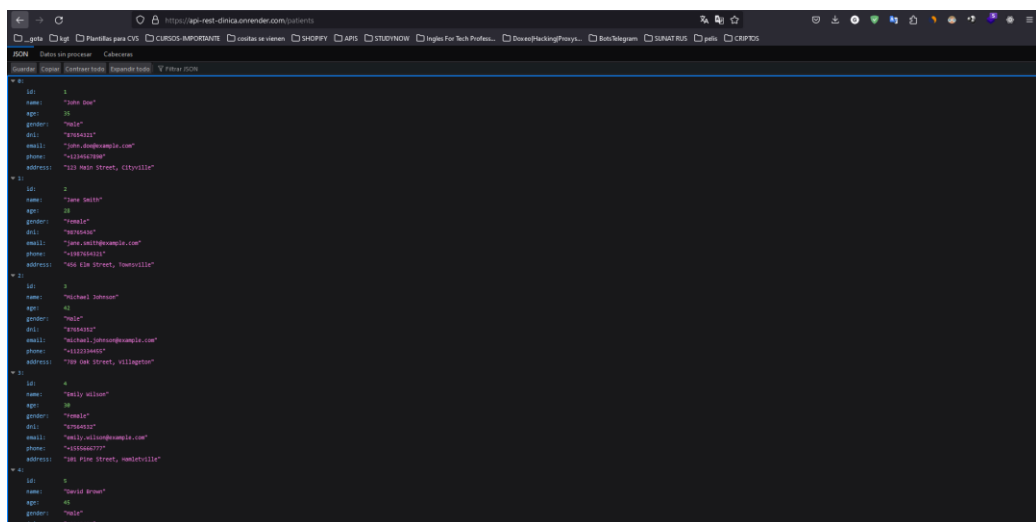
Imagenes del despliegue:



```

[
  {
    "id": 1,
    "patientName": "John Doe",
    "doctorName": "Dr. Smith",
    "date": "2024-04-24",
    "time": "10:00 AM",
    "reason": "Routine check-up"
  },
  {
    "id": 2,
    "patientName": "Jane Doe",
    "doctorName": "Dr. Johnson",
    "date": "2024-04-23",
    "time": "11:00 AM",
    "reason": "Follow-up appointment"
  },
  {
    "id": 3,
    "patientName": "Michael Brown",
    "doctorName": "Dr. Smith",
    "date": "2024-04-24",
    "time": "02:00 PM",
    "reason": "Initial consultation"
  },
  {
    "id": 4,
    "patientName": "Emily Wilson",
    "doctorName": "Dr. Lee",
    "date": "2024-04-25",
    "time": "09:00 AM",
    "reason": "Vaccination"
  },
  {
    "id": 5,
    "patientName": "David Johnson",
    "doctorName": "Dr. Garcia",
    "date": "2024-04-26",
    "time": "03:00 PM",
    "reason": "Check-up for diabetes"
  },
  {
    "id": 6,
    "patientName": "Sarah Taylor",
    "doctorName": "Dr. Wang",
    "date": "2024-04-27",
    "time": "10:30 AM",
    "reason": "Annual physical examination"
  }
]

```



```

[
  {
    "id": 1,
    "name": "John Doe",
    "age": 35,
    "gender": "Male",
    "email": "john.doe@example.com",
    "phone": "555-1234567",
    "address": "123 Main Street, Cityville"
  },
  {
    "id": 2,
    "name": "Jane Smith",
    "age": 28,
    "gender": "Female",
    "email": "jane.smith@example.com",
    "phone": "555-9876543",
    "address": "456 Elm Street, Townsville"
  },
  {
    "id": 3,
    "name": "Michael Johnson",
    "age": 45,
    "gender": "Male",
    "email": "michael.johnson@example.com",
    "phone": "555-2345678",
    "address": "789 Oak Street, Villagetown"
  },
  {
    "id": 4,
    "name": "Emily Wilson",
    "age": 30,
    "gender": "Female",
    "email": "emily.wilson@example.com",
    "phone": "555-3456789",
    "address": "101 Pine Street, Hamletville"
  },
  {
    "id": 5,
    "name": "David Brown",
    "age": 40,
    "gender": "Male",
    "email": "david.brown@example.com",
    "phone": "555-4567890",
    "address": "202 Birch Street, Hamletville"
  }
]

```

```

https://api-rest-clinica.onrender.com/Doctors
GET /Doctors HTTP/1.1 200 OK
Content-Type: application/json
[
  {
    "id": 1,
    "name": "Dr. Seth",
    "specialty": "General Practitioner",
    "dni": "12345678",
    "email": "dr.seth@example.com",
    "phone": "+1234567890",
    "hospital": "City Hospital"
  },
  {
    "id": 2,
    "name": "Dr. Johnson",
    "specialty": "Neurologist",
    "dni": "23456789",
    "email": "dr.johnson@example.com",
    "phone": "+1987654321",
    "hospital": "Town Clinic"
  },
  {
    "id": 3,
    "name": "Dr. Martinez",
    "specialty": "Pediatrician",
    "dni": "34567890",
    "email": "dr.martinez@example.com",
    "phone": "+1122334455",
    "hospital": "Village Medical Center"
  },
  {
    "id": 4,
    "name": "Dr. Lee",
    "specialty": "Orthopedic Surgeon",
    "dni": "45678901",
    "email": "dr.lee@example.com",
    "phone": "+1555667777",
    "hospital": "Health Hospital"
  },
  {
    "id": 5,
    "name": "Dr. Garcia",
    "specialty": "Cardiologist",
    "dni": "56789012",
    "email": "dr.garcia@example.com",
    "phone": "+1444333222",
    "hospital": "Village Heart Center"
  }
]

```