UDEC
UNIVERSIDAD DE CUNDINAMARCA

Proyecto Electiva Profesional II

Cristian Camilo Garzón Rodríguez, Daniel Matthew Castillo Achury y Jhon Sebastian Cagua Gutiérrez

Ingeniero Yesid Javier Reina Clavijo

21 de noviembre de 2022

Proyecto Electiva Profesional II

Cristian Camilo Garzón Rodríguez, Daniel Matthew Castillo Achury y Jhon Sebastian Cagua Gutiérrez

Facultad de Ingeniería, Ingeniería de Sistemas, Universidad de Cundinamarca

801M: Electiva Profesional II

Ingeniero Yesid Javier Reina Clavijo

21 de noviembre de 2022

Tabla de contenidos

Título del proyecto

S.I.S.A.

Social Introspective Support Accompaniment

Planteamiento del Problema

El apoyo social, en las redes sociales online, han sido una ayuda para las personas con problemas de salud mental, en particular, existe un manifiesto sobre la importancia de las "redes informales de apoyo" *(Gottliem, Psicólogo)*. Es necesario recalcar que las redes informales, son aquellas personas que conforman el entorno de una persona, siendo por ejemplo los vecinos, los amigos, etc. Las personas prefieren estas redes, antes de ir a un especialista para ayudar a resolver sus problemas.

Los estudiantes entre 18 y 23 años usaban MySpace para buscar su identidad, participar en la comparación social y expresar aspectos de su personalidad ideal, o características personales que le gustaría tener *(Manago, 2008)*. Este problema usualmente se ha incrementado a medida que crecen los mismos desarrollos para las plataformas informales. Los estudios establecidos, muestran diferentes niveles de apoyo que se establecen en la persona para buscar ayuda, donde se evidencio un incremento en el apoyo informal o redes de gestión autónoma; redes que ellos mismos establecen para poder dar soluciones personales a sus interrogantes y cuestiones independientemente del problema, donde se prueba que la relación de percepción de hijos y padres es decreciente a comparación de la percepción y aceptación de iguales*(Colegio oficial de psicólogos de Madrid)*.

Podemos darnos cuenta que las personas que no tienen una identidad creada, tienden a sentir que su funcionalidad en la existencia es inexistente, por lo tanto comienzan a tomar comportamientos autodestructivos, e incoherentes con respecto al uso de su raciocinio*(Thoits, hipótesis de* ***Identity accumulation hipótesis****)*. Por otra parte se comprueba que no todos los individuos con capacidad de razonar buscamos alguien en una posición mayor para obtener apoyo en términos sociales y personales, sino un nivel de igualdad,(***Revista Internacional Intervención Psicosocial)*****,** dando a conocer que es verídico que buscamos igualdad para poder avanzar y no pensamientos basados en la experiencia sino, vivir la experiencia por vida propia; no aplica en todos los casos, aplica en casos de ansiedad social, no en casos de un nivel mayor de trastornos mentales.

Los miembros de una comunidad la cual está estipulada en una red social online (RSO) pueden actuar de forma hostil, sin miedo a alguna pena merecida, ya que tienen la ventaja del anonimato. Por otra parte, podemos ver las dos caras que tiene las redes sociales frente al anonimato, por una parte la expresión sincera de los sentimientos al sentirse más libres y sin repercusiones gracias al anonimato, pero, por otra parte, este anonimato ayuda a que las personas tengan menos reciprocidad y tienen menos compromiso para llevar las relaciones, ya que no se sienten amarrados a seguir con una relación social.

Justificación del Proyecto

Nuestros estudios, con muchos de los ya existentes, llevaron a la investigación de los efectos negativos en las personas con psicopatologías, que directa e indirectamente buscan aislarse de sus círculos más cercanos, por su condición, son inicialmente la urgente necesidad de un agente tecnológico que aportará positivamente contrarrestando este fenómeno creciente, actualmente en la sociedad a nivel mundial, mayormente impactada en el continente Asiático.

El impacto a nivel social influiría tanto en la vida cotidiana de dichas personas como en el desarrollo comunicativo de las mismas en diferentes escenarios de su vida; tanto profesional como personal. Por otra parte el aspecto cultural e inclusive académico se verán reflejados en una manera considerable, teniendo en cuenta que se necesita un pilar en la sociedad mundial

que se pueda usar como herramienta, ya que paulatinamente se ha trabajado en la reintegración de la población mundial de manera presencial,

Las personas con problemas psicopatológicos pueden ayudados con las redes sociales online, (RSO), esto ayuda a que las personas se sientan integrados en una comunidad en la que tendrán pertenencia (), esto beneficia a la persona, ya que, aquellos usuarios implicados en actividades sociales en la red social pueden experimentar mejoras en el bienestar psicológico (), al percibirse a sí mismo como más capaces para crear y mantener relaciones duraderas, estas comunidades se ayudan entre sí para superar los problemas juntos. Este proyecto también será útil para las personas con dificultades para la interacción social cara a cara, o en riesgo de aislamiento social.

Un proyecto similar es la aplicación móvil YANA, la cual en 2021, fue la app de acompañamiento emocional más descargada en español (EFE News 2021). Esta aplicación fue creada para mejorar la estabilidad de las personas, sin necesidad de un especialista, sin embargo, esta aplicación tiene falencias, ya que al ser una inteligencia artificial, está obligada a responder de forma limitada, esto ya que no se basa en el apoyo social referente a las comunidades, se basa en recibir un apoyo de tipo acompañamiento social. pero, ¿Cuál es la diferencia entre nuestra propuesta de apoyo social y la propuesta de Yana?.

Según fuentes orales, YANA a largo plazo llega a ser muy repetitivo, ya que siempre se basa en las mismas preguntas y mismas respuestas todos los días, esto afecta al usuario, ya que no notará un avance en su proceso de apoyo social. Esto se da porque aunque sea una app muy útil, sigue faltando el factor humano que hemos hablado y hablaremos durante la investigación que estamos haciendo. Esa es la principal diferencia entre nuestro proyecto y YANA, ya que este proyecto se basa en la importancia de las comunidades, al momento de recibir apoyo social, es importante hacer parte de una comunidad para la búsqueda de la identidad, y darle sentido a la existencia.

Objetivo general

Desarrollar una red social informal, en la cual cualquiera pueda acceder, con el fin de brindar servicios de consultoría y sesiones psicológicas profesionales a personas con psicopatologías.

Objetivo específicos

- Ofrecer la red social a profesionales en diversas áreas de conocimiento disciplinar y aplicable para que puedan ofrecer sus servicios dentro de la misma.
- Publicar contenido de psicología educacional para que cualquier usuario pueda adquirir los conocimientos básicos con respecto a psicopatologías específicas y también como ser un acompañante en las mismas.

Alcance del proyecto

En un principio, el aplicativo tendrá el alcance de la comunidad con problemas psicopatológicos. Sin embargo, al ser un aplicativo de uso libre, puede integrarse cualquier persona que necesite de apoyo social, o simplemente interactuar con los distintos módulos del aplicativo. Inicialmente se tiene pensado llegar a la población entre 18 a 29 años, ya que según un estudio que hizo marca, es la edad que predomina para el uso de las redes sociales. Al igual que al igual que una investigación publicada por la revista científica molecular

psychiatry, hay una mayor tendencia, en donde las enfermedades psicopatológicas aparecen mayormente entre los 14 y 25 años.

Beneficiarios

Los beneficiarios serán todas aquellas personas que quieran y deseen recibir de una ayuda psicológica además de las familias de dichas personas debido a que mejorando el estado de ánimo, sentimientos, forma de actuar, de disfrutar de la vida superando sus problemas y de la mente en general se lograra un cambio notable e indirecto en sus familias ya que también puede ser que afecte a familias enteras.

Impacto

Se busca que tenga un impacto positivo y muy considerable que destaque frente a otros aplicativos con ideas similares, donde sus aspectos más relevantes hablen por sí solos y se demuestra cuando los usuarios inviten a sus amigos, familiares, conocidos que disfruten de está gran idea logrando beneficiarse además de colaborar con la sociedad.

Restricciones

- Recursos económicos debido a que si se quiere llegar a tener un buen producto requiere de una inversión para el desarrollo y mantenimiento del aplicativo.
- Capital humano, donde se va requerir un equipo entre desarrolladores, líderes, administrativos que propongan soluciones acordes a las necesidades y velen por el producto.
- Tiempo, debido a que si se requiere desarrollar un buen producto se va a necesitar tiempo de desarrollo, uso por parte del usuario para que acepte el producto.

Riesgos

- Poco rentable frente a mantenimiento de servidores
- Poca inversión

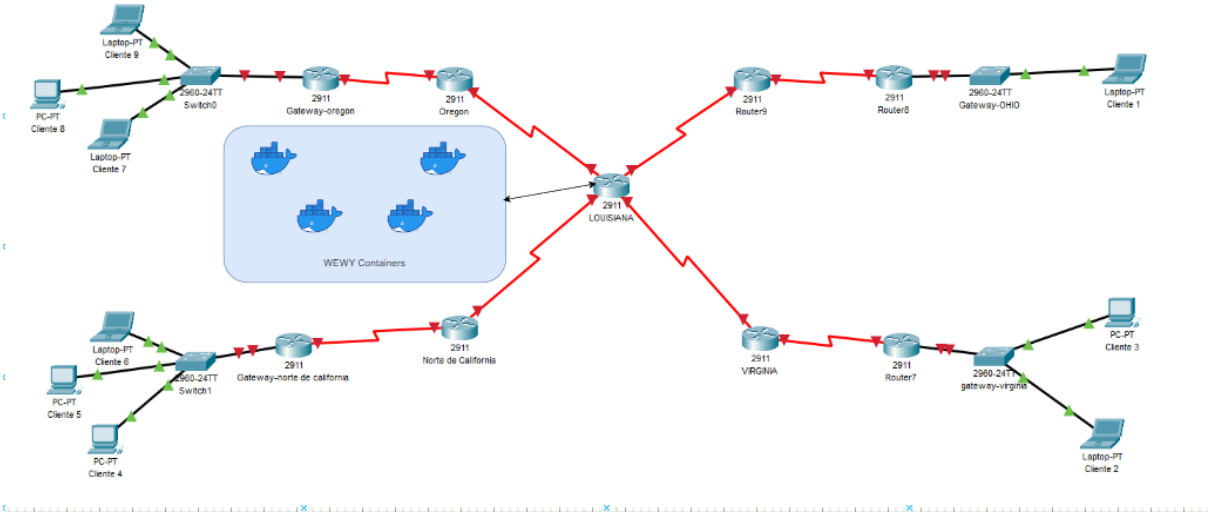
Producto o resultados

El producto final se basa en tres módulos, el primer módulo será la red social, en el cual se podrá hacer comunidades, en los cuales las personas podrán interactuar y ayudarse entre si. Ya que las personas que se sienten integrados en una comunidad, puede notar mejoras en el bienestar psicológico.
El segundo bot tiene que ver con un chatbot basado en deep learning, el cual ayudará a las personas para tener un chatbot con quien se pueda interactuar.
El tercero es un intermediario entre pacientes y psicólogos, para que los psicólogos tengan un espacio donde ejercer su profesión, y un espacio en donde se podrán realizar sesiones virtuales.

Normas y Estándares

- **ISO/IEC 9126:** Esta norma evalúa los productos de software, esta nos indica las características de la calidad y los lineamientos para el uso del aplicativo. Esta nos ayuda a evaluar el producto para definir los requerimientos de la calidad y otros usos.
- **ISO/IEC 25000:** La Norma ISO 25000, proporciona una guía para el uso de las series de estándares internacionales llamados requisitos y Evaluación de Calidad de Productos Software (SQuaRE). La norma establece criterios para la especificación de requisitos de calidad de productos software, sus métricas y su evaluación, e incluye un modelo de calidad para unificar las definiciones de calidad de los clientes con los atributos en el proceso de desarrollo.

Diseño de red en Packet Tracer



Descripción de Topología y Modelo OSI

Para la arquitectura de S.I.S.A se decidió colocar una topología de red de tipo estrella, en donde tendremos situado en un nodo central la sede de LOUISIANA, en donde se encuentra los contenedores docker con el aplicativo., Este enviará a las diferentes sedes para que se puedan comunicar, esto nos ayuda para tener un tráfico de red estable a comparación de otras topologías. Esta tipología nos permite tener una mejor recepción de nuevos usuarios, ya que es fácil sumar nuevos equipos a la red. Para la parte de acceso nos ayudará la topología, ya que la información debe basar a través del nodo central, la seguridad o acceso restringido configurado en el mismo resulta mayor y aceptable.

Cronograma de actividades

Tabla 1 y 2

Cronograma general

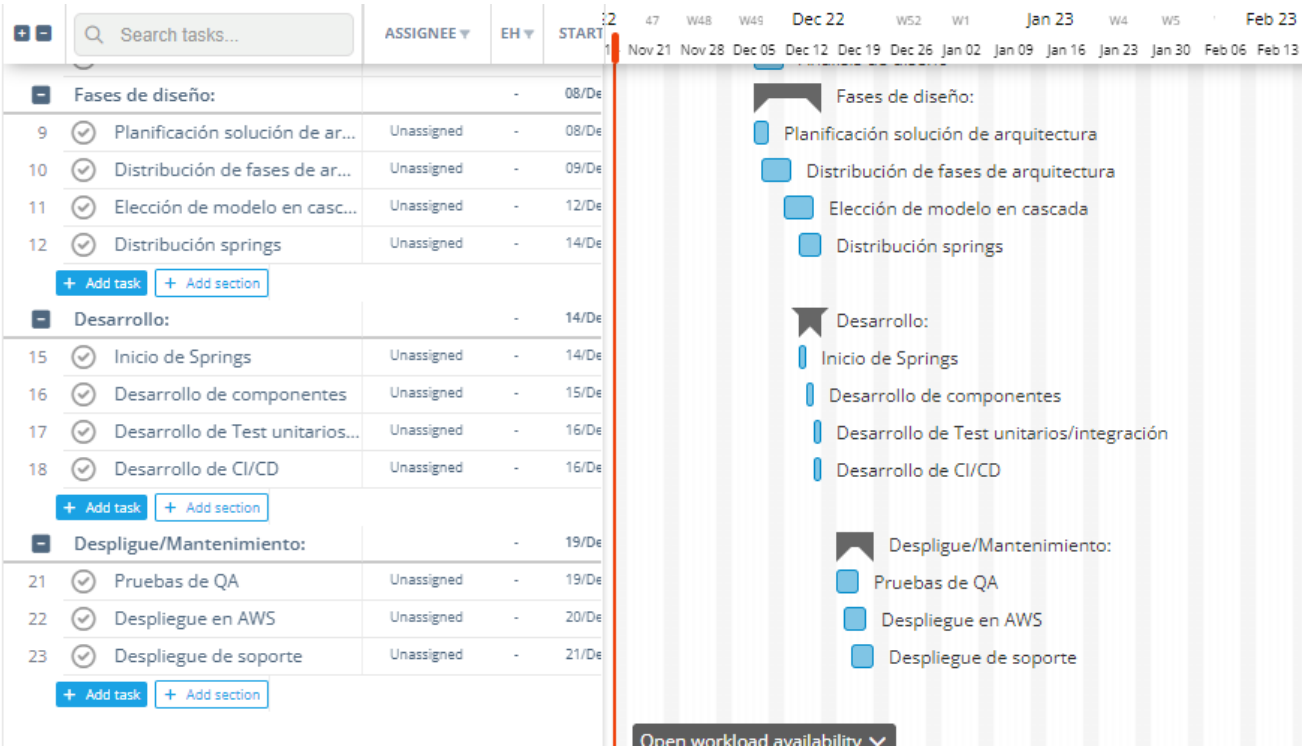


Tabla 3

Cronograma Sebastian

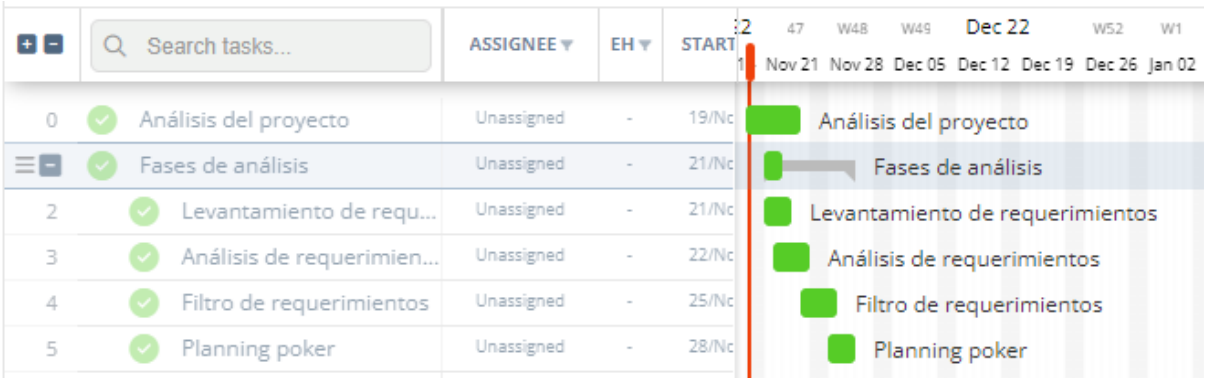


Tabla 4

Cronograma Daniel

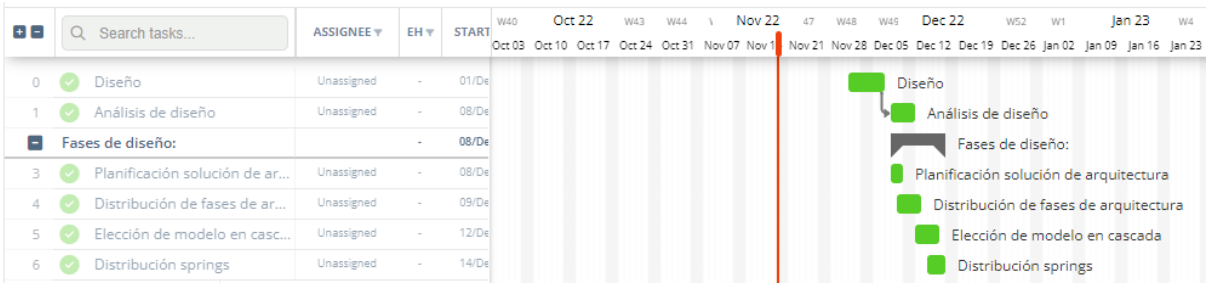
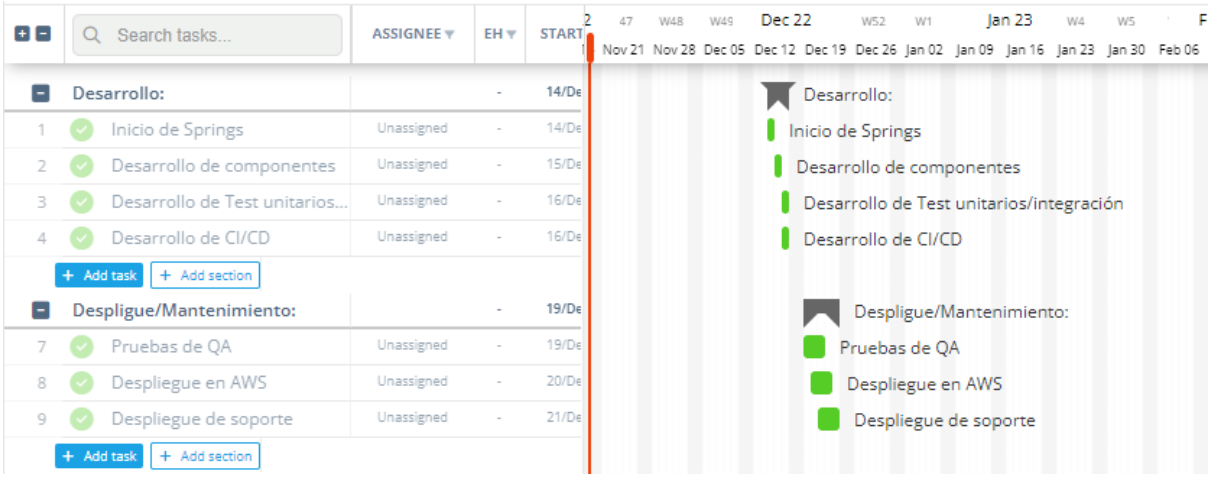


Tabla 5

Cronograma Cristian



1.Caracterización de procesos

Figura 1.

Mapa de procesos del proyecto

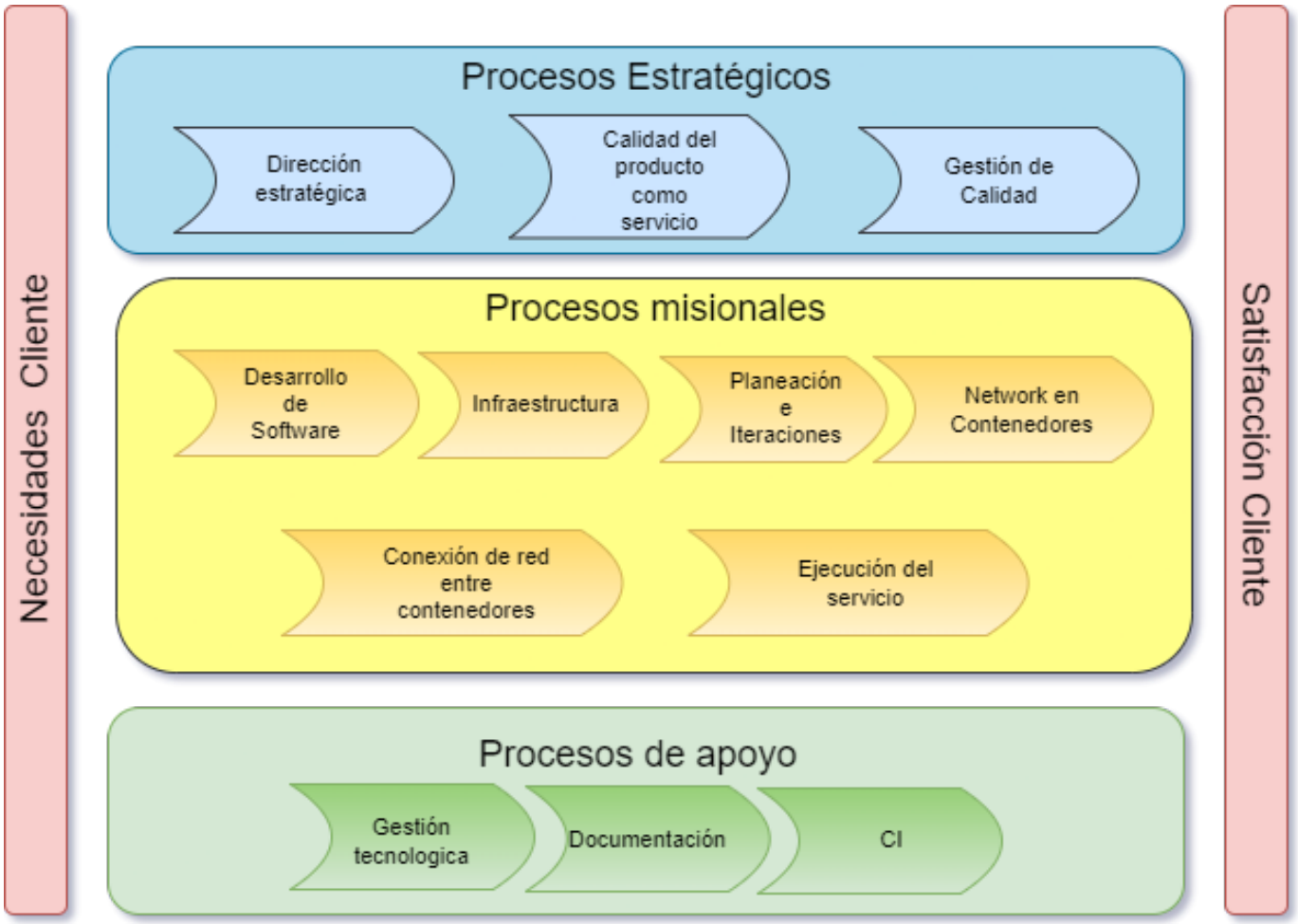


Tabla 1. *Caracterización del Mapa de procesos, proceso Desarrollo de Software*

	Información	Descripción
1.	Nombre del proceso	Proceso de Desarrollo de Software
2.1.	Responsable	Equipo de trabajo: Cristian Camilo Garzón Rodriguez, Jhon Sebastian Cagua Gutierrez, Daniel Mattthew Castillo Achury
2.2	Objetivo	Desarrollar un software que se exponga en la web con el fin, con un entorno de integración continua, usando las metodologías ágiles; usando una arquitectura de microservicios y contenedores con redes internas para la comunicación entre ellos.
2.3	Alcance	Desde su desarrollo hasta su despliegue en servidores de *aws*, acompañado de las metodologías ágiles para el entorno de integración continua(C.I.), un mínimo producto viable es el esperado.
3.	Procedimiento (Identificar actividades)	• Planeación del Software

		desacoplado. ● Planeación del modelo de datos. ● Definición de arquitectura. ● Implementación de sprints. ● Testing ● Deploy en producción ● Preparación de entorno de integración continua.
4.	Proveedores	Estudiantes dueños del proyecto; el equipo de trabajo.
5	Entradas	● Especificaciones funcionales. ● Arquitectura de microservicios. ● Infraestructura de despliegue e integración continua.
6	Salidas	● Software funcionando en una red interna de contenedores. ● Software expuesto a través de amazon web service (aws). ● Documentación de la

		red interna en la que funciona la arquitectura explicando los balanceadores de carga y Gateway.
7	Cliente	Usuarios con una característica en común como lo son las psicopatologías clasificadas como leves, entre ellas están: Aislamiento social, ansiedad, depresión y trastorno del impostor. Profesionales de artes humanas y psicológicas las cuales quieran ofrecer sus servicios a través de la app.
8	Recursos	Elementos físicos: Computadoras para el desarrollo del software. Elementos de talento humano: Equipo de trabajo de II PA 2022. Servicios: Aws como hosting para nuestra aplicación web. Entorno de integración continua como lo es GitLab. Repositorio remoto para el

		desarrollo organizado de las versiones como GitLab.
9	Controles	Gestión de Software, Ingeniería de Software, implementación de redes internas (VPS), funcionalidad con simultaneidad.

Tabla 2. *Caracterización del Mapa de procesos, proceso Control de Infraestructura y conexión entre contenedores.*

	Información	Descripción
1.	Nombre del proceso	Proceso de Desarrollo de Software
2.1.	Responsable	Equipo de trabajo: Cristian Camilo Garzón Rodriguez, Jhon Sebastian Cagua Gutierrez, Daniel Mattthew Castillo Achury
2.2	Objetivo	En un entorno de integración continua,con una arquitectura de microservicios y contenedores con redes internas para la comunicación entre ellos, se pretende controlar y mantener conectado por medio de infraestructura de aws los contenedores de los microservicios.
2.3	Alcance	Despliegue en servidores de aws logrando un entorno de integración continua.
3.	Procedimiento (Identificar actividades)	• Planeación infraestructura desacoplada. • Control de arquitectura.

		• Adquisición de una cuenta con aws. • Implementar un contenedor con suficiente memoria y si llega a ser necesario replicación del mismo para así asegurar la integridad de los datos. • Testing • Deploy en producción • Preparación de entorno de integración continua.
4.	Proveedores	Amazon Web Services
5	Entradas	• Documentación de clusters de aws. • VPS para desplegar en producción
6	Salidas	• Contenedores estables hosteados por aws. • Funcionamiento de una red interna de contenedores por medio de docker-compose.

7	Cliente	Usuarios con una característica en común como lo son las psicopatologías clasificadas como leves, entre ellas están: Aislamiento social, ansiedad, depresión y trastorno del impostor. Profesionales de artes humanas y psicológicas las cuales quieran ofrecer sus servicios a través de la app.
8	Recursos	Elementos físicos: Cluster de aws Elementos de talento humano: Equipo de trabajo de II PA 2022. Servicios: AWS con un VPS de la costa oeste preferiblemente. Contenedores de docker. Imágenes públicas de docker. Sostenimiento mensual del cluster de AWS.
9	Controles	Gestión de Software, Ingeniería de Software, implementación de redes internas (VPS), funcionalidad con

		simultaneidad.

Tabla 3. *Caracterización del Mapa de procesos, proceso Calidad del producto como servicio.*

	Información	Descripción
1.	Nombre del proceso	Calidad del producto como servicio
2.1.	Responsable	Equipo de trabajo: Cristian Camilo Garzón Rodriguez, Jhon Sebastian Cagua Gutierrez y Daniel Mattthew Castillo Achury
2.2	Objetivo	Asegurar la disponibilidad del servicio, para que el mismo se pueda ofrecer como un producto en cualquier momento y desde cualquier lugar, asegurando la calidad.
2.3	Alcance	Aseguramiento de la calidad de todo el servicio mejorando puntos débiles con respecto a la norma ISO 9001
3.	Procedimiento (Identificar actividades)	• Aplicar los principios de la Gestión de calidad

		en procesos. ● Enfoque en procesos principales. ● Establecer unas iteraciones entre planificar, hacer, verificar y actuar. ● Establecer un pensamiento basándose en los riesgos posibles. ● Relación con otras normas basadas en sistemas de gestión.
4.	Proveedores	Ninguno por el momento.
5	Entradas	● Identificación de riesgos ● Documentación y caracterización de procesos operativos y de infraestructura.
6	Salidas	● Documento con evidencias de las actividades para la gestión de calidad. ● Auditoría interna sobre todos los procesos.
7	Cliente	La organización propietaria

		de la aplicación, en este caso el equipo de trabajo y sus clientes potenciales.
8	Recursos	Documentación ISO 9001:2015
9	Controles	Gestión de Procesos internos y externos, aseguramiento de calidad, gestión en alta calidad.

Tabla 4. *Caracterización del Mapa de procesos, proceso de Seguridad con redes internas entre contenedores.*

	Información	Descripción
1.	Nombre del proceso	Seguridad de network interna entre contenedores.
2.1.	Responsable	Equipo de trabajo: Cristian Camilo Garzón Rodriguez, Jhon Sebastian Cagua Gutierrez y Daniel Mattthew Castillo Achury
2.2	Objetivo	Asegurar la red de comunicación entre contenedores para el

		funcionamiento del software.
2.3	Alcance	Aseguramiento de la red para que solamente puedan comunicarse entre contenedores.
3.	Procedimiento (Identificar actividades)	• Construir imágenes propias dentro del entorno de docker. • Configurar network para que se establezca comunicación entre cada contenedor. • Probar contenedores en modo bridge. • Monitorear y mejorar la configuración.
4.	Proveedores	Docker Inc.
5	Entradas	• API y Front terminadas. • Configuración de RIE (Red interna expuesta)
6	Salidas	• Comunicación de contenedores por una misma red dentro de docker.

7	Cliente	Todos los clientes potenciales del software.
8	Recursos	Docker Inc. IDEA.
9	Controles	Monitorización del entorno tanto de desarrollo como de producción.

ISO 27001

- **Políticas de seguridad de la información:** Nuestro aplicativo, al ser un servicio hosteado en AWS, cuenta con las políticas de seguridad que contiene AWS para su uso.
- **Gestión de recursos:** El aplicativo tendrá un diseño escalable, al ser almacenado en contenedores docker, se puede gestionar el escalado y desescalado para las instancias, de esa manera ahorrar la mayor parte de recursos en la infraestructura
- **Seguridad física y ambiental:** La infraestructura de aws, está hecha para que solo personal autorizado pueda entrar a los clusters. Aparte de tener alarmas anti incendios y anti inundaciones, para que ningún daño ambiental pueda suceder dentro de las instalaciones.

- **Seguridad de las comunicaciones:** El aplicativo usa una topología estrella, el cual hace que para tener acceso al aplicativo, debe pasar primero por el nodo principal, esto nos ayuda a tener una mayor seguridad en para las comunicaciones.

Requisitos

- **Establecer las responsabilidades:** AWS tiene políticas de seguridad en las cuales por parte de la infraestructura, solo personal autorizado puede entrar, y para la administración de instancias AWS, el dueño del aplicativo, entra por vía autenticación.

2.Seguridad física a implementar

De acuerdo al planteamiento del proyecto, dónde se busca implementar una red virtual entre contenedores para asegurar la red en términos de calidad, disponibilidad y confidencialidad de acuerdo al estándar ISO 9001. La seguridad física que involucra al

proyecto está establecida desde dos puntos claves, inicialmente la infraestructura física estará encargada por un proveedor adquirido como IaaS (Infraestructure as a Service), con gran prestigio como AWS, dado que la solución que ofrecen para el aseguramiento de la infraestructura física de red de los contenedores es demasiado rigurosa, ya que cuenta con certificaciones en aseguramiento de la información y gestión de calidad como lo son: *ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015, CSA STAR CCM v3.0.1.*

Por otra parte, la seguridad física de cada contenedor, dado su naturaleza y medio dónde se desarrolla, sus adaptaciones a la red tienen diversas funciones ofrecidas directamente por *Docker Inc,* dónde sus adaptaciones de red cuentan con tipos muy específicos como lo son *Bridge, Host, Overlay, Ipvlan, Maclvan y None*, en este caso, usados para asegurar la información y seguridad misma en cuanto accesos sobre recursos dentro de la red.

Así sé justifica directamente el aseguramiento de la calidad de la información sin dejar de mencionar la conexión entre contenedores sin necesitar una configuración de alto nivel, dejando los porcentajes en cuanto a los principios fundamentales al asegurar la infraestructura física y lógica del proyecto en niveles altos, como Prevención en un 90%, Disuasión 7% y Reacción un 2.5% dando más visibilidad y confianza al respecto del proyecto.

4.Medios de protección

4.1.Medios de protección física.

Dado que la infraestructura será adquirida por medio de un IaaS, la protección de la seguridad física, se dará en términos de terceros, pero configurada por el personal interno; el equipo de trabajo determinado por el proyecto, teniendo en cuenta que solo personal autorizado de AWS puede acceder a los servidores de cada uno de los ECS. Por esa parte más adelante se explicará la seguridad de la infraestructura física establecida por Amazon.

4.2.Medios electrónicos de protección.

Teniendo en cuenta el grado de rigurosidad de la aplicación y la implementación de red para que la comunicación de dichas aplicaciones tengan una disponibilidad máxima y un rango de error demarcado en minutos de error, dónde el mejor medio de protección electrónico son la implementación de alertas tempranas dentro del servicio y en la infraestructura, para así mismo asegurar la disponibilidad de los clientes, con accionables clave para su mismo propósito. El medio tecnológico mejor establecido por el equipo de trabajo es el medio de la observabilidad y las métricas las cuales nos darán visibilidad temprana de los elementos que se deban proteger y resguardar.

4.3.Medios metodológicos de protección.

El principal medio metodológico escogido por parte del equipo de trabajo es el de *Interrupción de las rutas de ataque* una metodología que recientemente se ha desarrollado en una creciente época de aumento de ciberataques a nivel empresarial y gubernamental, donde lo que se busca es proteger, resguardar y prevenir el AD (Active Directory) dónde se resguardan las credenciales, accesos y permisos con respecto a infraestructura lógica y tecnológica.

4.4.Fuerza de respuesta.

La fuerza de respuesta va encaminada de la mano con la metodología con la cual se asegura la protección de la infraestructura de red, hablando en términos físicos y lógicos. El primer paso en cuanto a la fuerza de respuesta es *explorar y monitorear*, movimiento lateral a lo largo del servicio y entorno del objetivo, *elevar* los privilegios del forense en uso para poder tener un acceso privilegiado sobre los demás y así tener un panorama más cercano, por consiguiente se prosigue a *evadir*, ocultando las huellas forenses del cometido y revisando caso por caso para encontrar algún rastro, y por último se *establece y exfiltra,* dónde al identificar el problema, se establecen accionables codificables para así mismo exfiltrar el cometido y establecer políticas de seguridad y cumplimiento para asegurarse dentro de la organización.

5.Competencia Metodológica

Las competencias metodológicas con respecto al proyecto se establecen desde la seguridad como un sistema de información, conteniendo así mismo la comunicación, donde la equidad del análisis preliminar, se tienen en cuenta factores dónde se exponen los más críticos en el marco del proceso a nivel organización y a nivel operativo, donde los pilares según estándares como ISO 27002:2013 e ISO 27001 son:

5.1.Prevención.

Se establecen medidas de seguridad, principalmente la asignación de roles y credenciales con Active Directory para asegurar la autorización y por consiguiente la autenticación de cada uno de los involucrados en el proyecto, excluyendo directamente a los individuos con perversas intenciones en la afectación de la red o el sistema completo.

5.2.Inhibición.

De acuerdo al estándar, dado el caso en recibir un ataque de cualquier tipo, interno o externo se debe identificar las huellas forenses para el análisis y determinación de la fuente del causal maligno y tomar acciones en pro de la mejoría para la seguridad y disminuir el riesgo.

5.3.Capacidad de respuesta.

Al recibir ataques con respecto a la infraestructura y a la seguridad lógica en la infiltración, para asegurar la disponibilidad del servicio dejando atrás el ataque, se establecen métricas de disponibilidad con respecto a las IPs que están intentando establecer comunicación con el servicio, dejando así un ataque de denegación de servicios como lo es DOS, para identificar los clientes malintencionados y los clientes de usuarios existentes normalmente, por lo menos puedan seguir estableciendo comunicación con el servicio, así mismo para un ataque de denegación de servicios distribuido DDOS.

5.4.Formación.

Una vez un ataque finalizado, una caída del servicio o diferentes problemas de acción en cuanto a la identificación del caso en tiempo después de haber terminado el ataque y reconocer al responsable, para determinar acciones que hagan que ese caso en particular no volviese a ocurrir.

5.5.Inversión.

Dado el proyecto, los costos para su implementación y validación son grandemente elevados, ahora pensar que los servicios de esta magnitud, en términos de precios, se debe tener en cuenta que los riesgos para la implementación y aseguramiento de la calidad y la información

5.6.Mediciones.

Estas mediciones se hacen de tipo producto y también tecnológico, para que la visibilidad sea mucho más grande y así mismo detectar qué porcentaje es el afectado y cómo reducirlo a futuro sin deteriorar el servicio.

5.7.Eficiencia.

La eficiencia juega un papel fundamental en el desarrollo de las actividades correspondientes al aseguramiento de la calidad de cada uno de los servicios proporcionados.

5.8.Integración.

Dado el nivel del proyecto, se tendrá un equipo de integración del mismo tipo de desarrollo, ya que no se cuenta con la cantidad de personal correspondiente a cada tarea frente al contexto, donde se contará con sinergia de acuerdo a los

5.9.Transparencia.

La transparencia dentro del proyecto estará dada sobre la automatización dado que en dónde existen procesos dependientes de personal humano el porcentaje de error establecido implícitamente entre ellos es de un alto puntaje, la automatización sobre AD y diferentes temas de automatización serán el proceso clave.

5.10.Confidencialidad

Con respecto a la seguridad de la información a nivel confidencial, se llevará por medidas de cumplimiento, dentro del equipo de trabajo, dónde el aseguramiento de la información y de la infraestructura, recaerá sobre una única persona en este caso el Estudiante Daniel Matthew Castillo Achury, usando una bóveda de contraseñas para asegurar las credenciales y la información dependiendo de el nivel o la rigurosidad de la misma, si es información accesible, confidencial o sensible.

6. Información general del proyecto

El proyecto a grandes rasgos consiste en crear un chatbot el cual sea capaz de entablar una conversación mediante mensajes de texto con los usuarios logrando entender lo que están solicitando e intentar solucionar sus problemas, los temas sobre los cuales el chatbox será capaz de tratar son temas psicológicos ya que se busca que las personas puedan recibir asistencia psicológica.

Como el proyecto es un software es primordial poder cargarlo a la red para que las personas puedan acceder a él y puedan disfrutar del servicio, por ello es necesario un lugar donde

poder alojar el software, que tenga almacenamiento necesario para que el aplicativo funcione, que sea seguro, que pueda soportar todo tipo de ataques sofisticados de la actualidad, que se mantenga a lo largo del tiempo además de que pueda ser accesible desde cualquiera parte del mundo.

Por todas estos razones es muy complicado suplir todas estas necesidades sin los recursos economicos, tecnologicos y de capital humano necesarios, por ello se decidió adquirir un servicio de nube como lo es AWS (Amazon Web Services) el cual es capaz de solventar todo lo ya mencionado y lo más importante a un costo asequible.

7. Instrucciones del proyecto

Con el siguiente proyecto se busca poder afianzar los conocimientos que se han ido adquiriendo a lo largo del periodo académico en cuanto a redes, seguridad, proyectos, además de ello la importancia de aplicar los conocimientos en un proyecto de está envergadura nos ofrece una mayor visión del desarrollo de procesos indispensables en una infraestructura física y lógica ya sea una sede empresarial o en el desarrollo de un software.

Algunos de los conocimientos adquiridos se pueden reflejar en la explicación de la infraestructura con su respectivo diagrama el cual ilustra ideas, fases y componentes del proyecto propuesto, siempre teniendo en cuanto aspectos a destacar para está materia como los componentes de redes además de la parte de seguridad todo esto bajo un acoplamiento y apropiación de las nuevas tecnologías que dominan el sector como lo es AWS.

También se puede encontrar la explicación y funcionamiento a detalle de los procesos del software englobando en tres grandes áreas de procesos como lo son los misionales, estratégicos y de apoyo.

Por último se puede destacar el gran trabajo de interpretación, diseño y análisis por parte del equipo de trabajo que logró identificar esos objetivos los cuales se alcanzaron con satisfacción, gracias a esto se pudo proponer este desarrollo de este aplicativo.

8. Planos de la identidad

El proyecto siendo un aplicativo o software se implementara y estará alojado en un servidor de la empresa de Amazon más específicamente en los servicios de AWS (Amazon Web Services) la cual es la plataforma en la nube más adoptada y completa en el mundo, que ofrece más de 200 servicios integrales de centros de datos a nivel global. Millones de clientes, incluso las empresas emergentes que crecen más rápido, las compañías más grandes y los organismos gubernamentales líderes, están usando AWS para reducir los costos, aumentar su agilidad e innovar de forma más rápida.

Por está razón con mucha facilidad cumplira amplias espectativas como suplir dichos servicios a más de 20 clientes al mismo tiempo ya que este depende únicamente de los recursos económicos que la empresa en este caso el proyecto SISA abone a AWS para que este ofrezca los recursos digitales pertinentes sin ningún problema ya que este servicio es escalable, dinámico, elástico y se ajusta a las necesidades de los clientes.

Un punto importante a destacar es que, como estos servicios son tan demandados y usados a nivel mundial está empresa destina bastantes recursos economicos en brindar una buena seguridad, estabilidad y protección de la información y de recursos digitales de gran valor intrínseco para cada uno de sus clientes por ello es viable afirmar que están más que seguros los datos empresariales y aquellos datos brindados por los usuarios.

Figura 1.

Servicios de seguridad de AWS

9. Ventajas y desventajas de la ubicación de los dispositivos

Ventajas

- Facilidad de acceso y uso de los recursos
- Facilidad de corrección de problemas
- Acceso desde cualquier parte
- Recuperación de datos
- Infraestructura no costosa
- Seguridad más avanzada y detallada

Desventajas

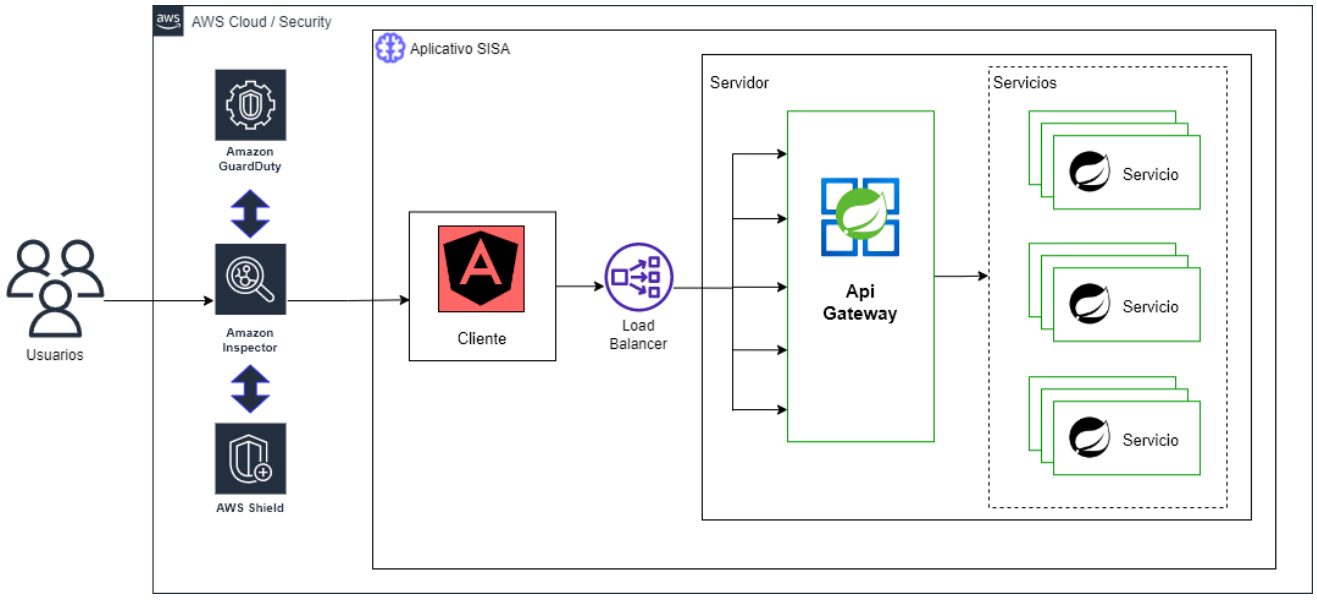
- Posible opción de pago
- Se debe conectar a internet
- Vulnerabilidad a ciberataques

10. Distribución de componentes de seguridad por pisos

Recordando que como el servicio a ofrecer se encuentra alojada en internet más específicamente en los servidores de Amazon Web Services, estos son los encargados de ofrecer toda la seguridad necesaria al software allí alojado, protegiéndolo de ataques o ciberataques, permitiendo que este no fallará por alguna causa externa común en países latinoamericanos.

Por esto razón como primera barrera se tienen los servicios de AWS dentro de los cuales vienen incluidos los componentes de seguridad física y virtual, luego de este proceso ya se da paso a utilizar los servicios del aplicativo propuesto.

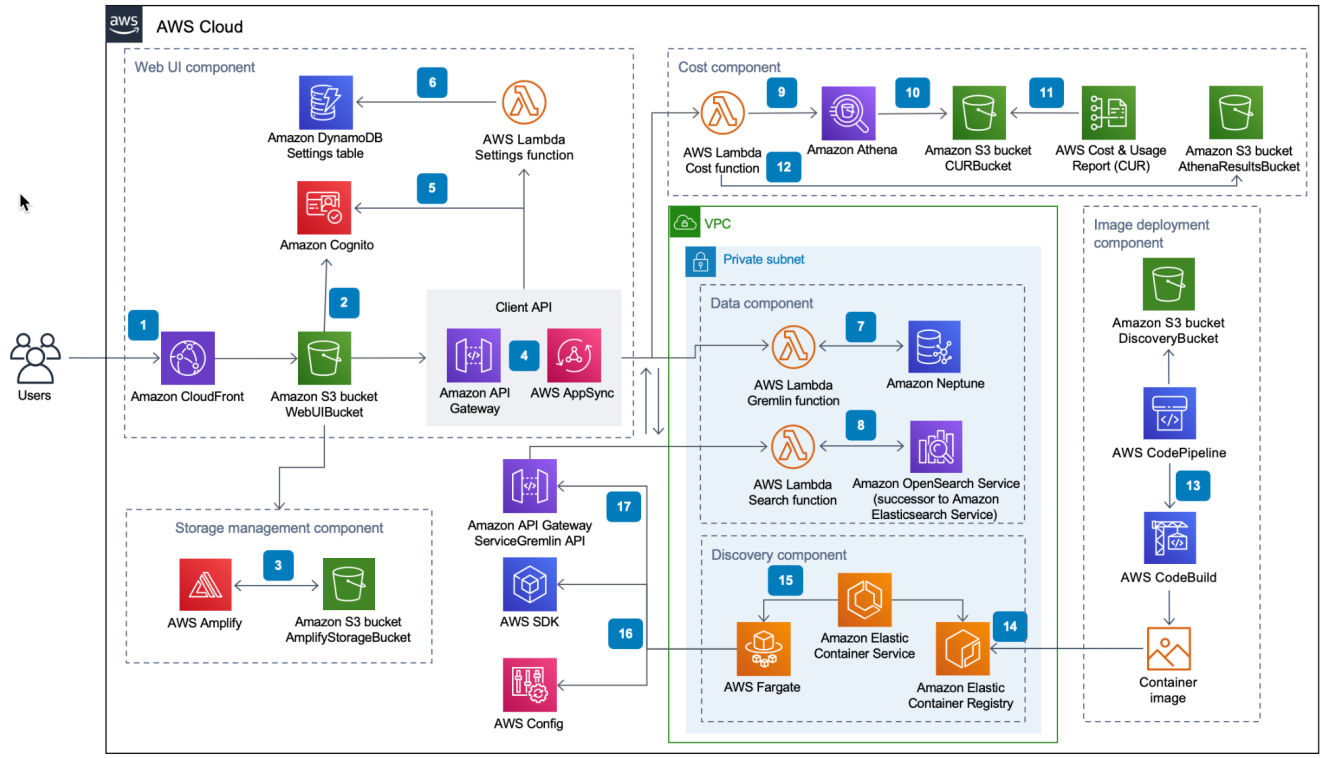
Figura 2.
Componentes de seguridad física



Dentro del siguiente diagrama podemos encontrar la infraestructura física y virtual de AWS donde provee los diferentes servicios que tiene a su disposición en el que podemos encontrar los servicios de seguridad los cuales son indispensables para este proyecto.

Figura 3.

Infraestructura tecnológica, seguridad y servicios de AWS



Para tener una mayor perspectiva del diagrama, ingrese al siguiente link [Infraestructura tecnológica, seguridad y servicios de AWS]

11. Descripción de Seguridad Física

El proyecto, al ser un aplicativo desplegado en la nube, no contamos con recursos físicos, sin embargo en la infraestructura que se va a ser desplegada (AWS), posee recursos físicos alojar diferentes aplicaciones de manera internacional, por lo tanto, nos vamos a enfocar en la seguridad física que tiene amazon en todas sus sedes.

Amazon Web Services (AWS) posee una infraestructura la cual cuenta con 27 sedes en las cuales cada uno de los centros de datos. Para acceder a estos centros de datos, AWS proporciona acceso físico al centro de datos solo a los empleados autorizados. Todos los empleados que necesiten tener acceso al centro de datos primero deben solicitar el acceso y proporcionar una justificación empresarial válida. Estas solicitudes se conceden en función del principio de privilegios mínimos, según el cual las solicitudes deben especificar a qué capa del centro de datos requiere acceso la persona, con limitaciones temporales. Las solicitudes las revisa y aprueba el personal autorizado y el acceso se revoca cuando finaliza el tiempo solicitado. Una vez concedido el acceso, las personas solo tienen acceso a las áreas especificadas en sus permisos.

Para que terceros puedan acceder al centro de datos, lo solicitan empleados de AWS autorizados, que deben rellenar una solicitud de acceso de terceros y proporcionar una justificación empresarial válida. Estas solicitudes se conceden en función del principio de privilegios mínimos, según el cual las solicitudes deben especificar a qué capa del centro de datos requiere acceso la persona, con limitaciones temporales. Estas solicitudes las aprueba el personal autorizado y el acceso se revoca cuando finaliza el tiempo de la solicitud. Una vez concedido el acceso, las personas solo tienen acceso a las áreas especificadas en sus permisos. Todos los visitantes a los que se les concede acceso deben presentar su identificación cuando llegan al sitio, firmar el registro de entrada e ir acompañados de personal autorizado.

El acceso a los centros de datos se revisa periódicamente. El acceso se revoca automáticamente cuando se anula el historial de un empleado en el sistema de recursos humanos de Amazon. Además, cuando caduca el acceso de un empleado o contratista en virtud de la duración de la solicitud aprobada, se revoca su acceso aunque continúe siendo empleado de Amazon.

El acceso físico a los centros de datos de AWS se registra, se monitoriza y se mantiene. AWS correlaciona la información obtenida de los sistemas de monitorización lógicos y físicos para mejorar la seguridad según sea necesario.

12. Analisis y Descripcion de los dispositivos a Instalar

- **CCTV**

  Los puntos de acceso físico a las salas de servidores se graban con cámaras de televisión de circuito cerrado (CCTV). Las imágenes se conservan de acuerdo con los requisitos legales y de conformidad.

  Se han instalado sistemas de detección de intrusiones electrónicas en la capa de datos para monitorear, detectar y alertar automáticamente al personal acerca de los incidentes de seguridad. Los puntos de entrada y salida de las salas de servidores están protegidos con dispositivos que requieren que cada persona proporciona autenticación multifactor antes de concederle la entrada o la salida. Estos dispositivos harán sonar las alarmas si la puerta se fuerza sin autenticación o se mantiene abierta. Asimismo, se han configurado dispositivos de alarma en las puertas para detectar aquellos casos en los que una persona sale o entra en una capa de datos sin proporcionar autenticación multifactor. Las alarmas se envían inmediatamente a los centros de operaciones de seguridad de AWS de funcionamiento ininterrumpido para que se apliquen acciones inmediatas de registro, análisis y respuesta.

  El acceso físico está controlado en los puntos de acceso del edificio por personal de seguridad profesional mediante videovigilancia, sistemas de detección de intrusiones y otros recursos electrónicos. El personal autorizado utiliza mecanismos de autenticación multifactor para tener acceso a los centros de datos. Las entradas a las salas de servidores están protegidas con dispositivos que hacen sonar las alarmas para iniciar una respuesta a un incidente si la puerta se fuerza o se mantiene abierta.

13. Descripción de los Dispositivos

NOMBRE Y EQUIPO DEL MODELO
Cámaras en las instalaciones
Sensores de movimiento
Puertas de seguridad
Sensores de temperatura
Sistema de detección de incendio

Debido a que no tenemos conocimiento de la infraestructura que tiene amazon, lo que se hará por consiguiente, es dar una breve especificación de qué equipos se utiliza para la seguridad física de amazon web services, sin dar un número de unidades, ya que no sabemos el tipo de arquitectura física que tiene, en las 27 sedes distintas que tiene al rededor del mundo.

Cámara en las instalaciones

Las sedes de amazon están vigiladas con cámaras de televisión de circuito cerrado, las cámaras principales están en la entrada y salida de los servidores, estas cámaras son necesarias para poder ver cuando haya un inconveniente,

Sensores de movimiento

Estos sensores de movimiento están colocados en las entradas de los servidores, antes de entrar solo lo puede desactivar una persona autorizada.

Puertas de seguridad

Las puertas para la entrada a los servidores, tienen un sensor por si se abre forzosamente la puerta, o si se deja por bastante tiempo abierta la puerta, esto mandará una alarma al servicio de seguridad.

Sensores de temperatura

Dentro de las instalaciones, para el correcto funcionamiento de los servidores, y que no haya un posible daño en los servidores, hay sensores de temperatura, para que no llegue a altas temperaturas, y se puedan dañar los servidores, en el momento que suba la temperatura, se acondicionó la sala de servidores, para que no haya ningún daño en el hardware.

Sistema de detección de incendios

En las instalaciones de los servidores, hay sensores de humo, lo cual mandan una alerta al momento de haber un incendio, ya que los servidores trabajan por dentro a altas temperaturas, pueden generar un incendio, por lo tanto es importante la instalación de estos sensores.

14. Conclusiones

Es importante tener en cuenta la seguridad al momento de construir un proyecto, se deben tener en cuenta varios factores externos, que usualmente no se tienen en cuenta, pero eso no le quita importancia. La seguridad de una aplicación viene tanto desde el software, y asi mismo, hasta la parte del hardware y toda su parte externa. Teniendo en cuenta la seguridad, podemos saber qué puntos débiles puede haber al momento de implementar el proyecto.

15. Referencias

[1] ISO 9001:2015 https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-5:v1:es

[2] Centro de datos de aws: data center infrastructure

[3] Página web https://daniel-cas.github.io/wewy-chatbot-webpage/