

Trabajo Práctico Integrador

Grupo 7 - Versión 2.1

Curso k4001

Integrantes

Camacho Ruiz, Juan Carlos
Makinson Ale, Christian Francis
Mamani Gutierrez, Cristina Elizabeth

Índice

Índice	1
Introducción	4
Contexto	4
Objetivo general	4
Objetivos específicos	5
Estructura del documento	5
Relevamientos	5
Minuta 7/5/2021	5
Requerimientos	6
Especificación de los Submódulos	6
Submódulo de Turnos para Pacientes	6
Submódulo Historia Clínica	6
Submódulo de Perfil Personal del Médico	6
Características de los usuarios	7
Requerimientos Funcionales	7
Requerimientos no Funcionales	13
Planificación	18
Estructura del Desglose del Trabajo	18
Especificación de roles	19
Desarrollo	20
Especificación de los Sprints	20
Sprint 1	21
Sprint 2	21
Sprint 3	21
Sprint 4	21
Sprint 5	22
Sprint 6	22
Sprint 7	22
Sprint 8	22
Diagrama de GANTT	22
Implementación	22
Costo de Recursos Humanos	23
Análisis de Riesgos	24
RIESGO 1	24
Plan de mitigacion	24
Plan de contingencia	24
RIESGO 2	24

Plan de Mitigación	25
Plan de Contingencia	25
RIESGO 3	25
Plan de Mitigación	25
Plan de Contingencia	25
RIESGO 4	25
Plan de Mitigación	25
RIESGO 5	26
Plan de Mitigación:	26
Diseño de Arquitectura de Software	27
Análisis técnico y funcional	27
Arquitectura de SW actual	28
Infraestructura de HW actual	28
Diagrama de Arquitectura de SW Propuesta	29
Autenticación de usuarios	30
Lógica de negocio para la vacunación COVID	30
Backup and Recovery con MongoDB en la nube	32
Seguridad de datos sensibles	32
Infraestructura de Hardware y Redes Propuesta	33
Redes	36
Auditoría	36
Aspectos a consultar y evaluar en la visita	35
Falencias o fallas de seguridad consideradas	36
Auditoría Interna	38

Historial de cambios

Fecha	Version	Descripción
18-05-21	1.0	Presentación de la primera entrega.
22-06-21	1.1	Corrección de la primera entrega
27-08-21	1.2	<ul style="list-style-type: none"> - Se agrega la sección "<i>Diseño de Arquitectura de Software</i>". - Se incluye diagrama de SW y HW y redes. - Se modifican los RF y RNF
17-10-21	2.1	<ul style="list-style-type: none"> - Se modifica la WBS-EDT - Se modifican los RF y RNF - Se modifican los diagramas de SW y HW

Introducción

Contexto

Estamos transcurriendo abril del año 2020, hace un mes se declaró una pandemia mundial debido al virus SARS-COV2 (Coronavirus).

La empresa requiere que el 80% de su personal pueda trabajar de manera remota, y que a las sucursales asista el mínimo personal necesario para admisión de pacientes, personal de guardia, de internación (sólo para casos urgentes, se suspenden todas las cirugías programadas que no requieren de atención urgente) y el mínimo personal de IT para dar soporte a los usuarios que no pueda brindarse en forma remota.

La empresa cuenta con un software Core que incluye un módulo de admisión (para recepcionar pacientes ambulatorios y admitir los pacientes para internación), un módulo de facturación (para el cual se carga la prestación para la posterior presentación a las obras sociales o para el cobro a particulares), un módulo de cirugías (donde se gestiona el uso de quirófanos y de instrumentación) y un módulo de farmacia (donde se registra la compra y consumo de medicación e insumos).

Tanto las consultas por sospecha de Covid como las consultas programadas deberán empezar a atenderse por Telemedicina (servicio que actualmente no brinda la institución).

Objetivo general

En el presente informe se detalla la solución para el problema propuesto por el cliente Sanatorios Trisalud.

Con el objetivo de crear un sistema digital capaz de realizar todas las operaciones que hoy presencialmente no se puede y sean posibles de manera virtual dentro del marco de la pandemia, reutilizando los recursos existentes en el sistema del cliente.

Objetivos específicos

- Desarrollo del módulo de telemedicina, para la administración de atención médico-paciente de manera remota
- Desarrollo de un submódulo que gestiona el historial médico del paciente de forma segura y confidencial

- Desarrollo de una agenda de turnos tanto para el médico como para el paciente.
- Realizar mejoras en el sistema existente para soportar la concurrencia a los servidores, durante la obligatoriedad del trabajo remoto.

Estructura del documento

Comenzaremos con la definición de los submódulos que serán desarrollados como solución y consecuente a estos la especificación de los requerimientos necesarios dividido en aquellos que son de carácter funcional y no funcional.

Luego, a partir de estos, se detalla la planificación del proyecto, comenzando por la EDT, siguiendo con la explicación del proceso utilizando una metodología Agile y se planificación de los costos.

Por último, el documento contará con un análisis de riesgos y con los planes de mitigación y contingencia relacionados.

Relevamientos

Minuta 7/5/2021

La información relevada fue:

- Los usuarios que van a utilizar el sistema son los empleados administrativos, el staff médico, el personal de IT y los pacientes.
- La cantidad de empleados está entre los 600 a 800.
- La cantidad de médicos trabajan en planta de manera simultánea son 10 médicos en piso, mínimo. Jornadas de 12 hs.
- Los médicos atienden a un paciente cada 30 minutos.
- Los pacientes de alta complejidad son aquellos que necesitan internación. Mediana complejidad aquellos que necesitan estudio médicos y los de baja complejidad los que pueden ser atendidos de manera remota.
- No hay límite de tiempo y se cuenta con un amplio presupuesto.
- Con la conexión de internet se trabaja cómodamente, pero no sobra con los 200 usuarios conectados simultáneamente

Requerimientos

Especificación de los Submódulos

El módulo Telemedicina contará con 4 submódulos:

Submódulo de Login

Este submódulo será creado para la autenticación de usuarios del sistema.

Submódulo de Turnos para Pacientes

Este submódulo será creado para poder sistematizar y agendar los turnos solicitados por los pacientes. En la solución el sistema deberá permitir al paciente solicitar un turno con el especialista que desee dentro de una agenda de disponibilidades y llenar un formulario con número de afiliado si lo tuviera y la preferencias del medio de comunicación Whatsapp o google meet.

Submódulo Historia Clínica

Para poder centralizar información y hacer más efectivo el servicio hacia los pacientes será de gran importancia poder visualizar y/o consultar las historias clínicas.

El Sanatorio ya cuenta con un módulo de Historial clínico, pero es muy precario por lo cuál este mismo se desarrollará desde cero.

Las funcionalidades serán consultas, modificaciones y actualizaciones en el historial clínico, habilitando estas misma según el tipo de usuario (paciente, médico o administrador IT)

Se podrá completar un formulario de los datos personales del paciente, cargar recetas, imágenes, pdf de estudios realizados.

Submódulo de Perfil Personal del Médico

Este submódulo será creado para que el médico tenga un espacio personalizado donde pueda acceder a sus datos personales y modificarlos, acceder a su agenda y acceder a la historia clínica de los pacientes a atender, así como también confirmar la asistencia a un turno.

Características de los usuarios

Los usuarios de la aplicación web de telemedicina:

- Usuario: Persona física que utiliza el sistema.
- Administrador IT: Usuario encargado de mantener el sistema.
- Paciente: Usuario que realiza la consulta médica que puede ser resuelta de forma virtual o presencial.

- Médico: Usuario interno del sanatorio.

Requerimientos Funcionales

ID	RF01
Nombre	Ampliación de VPN
Descripción	Se mantendrá el datacenter actual, como fue informado por el analista, el sistema actual funciona correctamente y se ampliará los MB del tráfico mensual para la VPN actual. Lo necesario para tener 200 usuarios concurrentes por turno.
Usuario	Administrador - Empleado
Prioridad	Alta

ID	RF02
Nombre	Desarrollo de app web de telemedicina
Descripción	Se desarrollará una app web para el módulo de telemedicina y de ella se dividirá en 3 funcionalidades como submódulos <ul style="list-style-type: none"> • Turnos para pacientes • Historial clínico • Perfil personal del médico Se desplegará en un servidor cloud (AWS) y se contratará el servicio EC2
Usuario	Paciente - Medico - Administrador
Prioridad	Alta

ID	RF03
Nombre	Autenticación de usuarios - app web de telemedicina

Descripción	<p>Al ingresar a la app web se mostrará una lista desplegable con los diferentes tipos de usuarios. Y se solicitará un usuario y contraseña para acceder a las funcionalidades de la app web.</p> <p>Si no se contara con una cuenta creada, entonces:</p> <ul style="list-style-type: none"> • Si el usuario fuera un paciente, se le solicitará completar un formulario con sus datos personales, nombre y apellido, dni, email, número de teléfono, número de afiliado, fecha de nacimiento, género. La contraseña deberá contar con la siguientes medidas de seguridad: <ul style="list-style-type: none"> ○ Mínimo 8 caracteres y 30 como máximo. ○ Mínimo 1 mayúscula, 1 minúscula, 1 número y 1 símbolo. • Si fuera un médico o administrador, tendría que solicitar la creación de una cuenta al sector IT de la clínica. Una vez brindado el usuario y contraseña, en el primer ingreso, será obligatorio que cambien la contraseña, para que así sea conocida solo por el usuario.
Usuario	Paciente - Medico - Administrador
Prioridad	Alta

ID	RF04
Nombre	Solicitud de turnos para pacientes - Submódulo
Descripción	<p>El sistema debe permitir a los pacientes solicitar turnos, con la posibilidad de filtrar primero por especialidad y luego por sucursal en la que se quiera atender.</p> <p>El sistema deberá mostrar las fechas y horarios disponibles de dicha especialidad y los datos del médico.</p> <p>Luego el paciente debe seleccionar la opción que desee, el medio preferido para realizar la consulta google meet (debe ingresar un email) o whatsapp (debe ingresar un número) y con eso queda el turno confirmado y registrado en una base de datos.</p> <p>Por último el sistema debe notificar al médico relacionado.</p>
Usuario	Paciente
Prioridad	Alta

ID	RF05
Nombre	Notificación de turno

Descripción	Un día antes al turno previamente agendado se le enviará al paciente y al médico una notificación vía email para recordarle el turno ya pactado, en caso de que el paciente no pueda asistir se le brindara la opción de realizar la cancelación del mismo.
Usuario	
Prioridad	Media

ID	RF06
Nombre	Modificar un turno
Descripción	El sistema debe permitir a los pacientes modificar un turno, cancelando el registrado y reservando uno nuevo en otro horario disponible. Por último el sistema debe notificar al médico relacionado.
Usuario	Paciente
Prioridad	Alta

ID	RF07
Nombre	Ejecutar un turno
Descripción	El sistema debe permitir al médico registrar el inicio de una consulta desde su perfil personal y la finalización del mismo también. Al finalizar la consulta el médico lo hará agregando una descripción de la misma.
Usuario	Paciente - Médico
Prioridad	Alta

ID	RF08
Nombre	Filtrar Búsqueda para Solicitud de Turno
Descripción	El sistema debe permitir a los pacientes filtrar a los turnos posibles según médico específico, especialidad o ambas. En el caso de filtrado por médico, del mismo, deberían aparecer los datos: Nombre, Apellido, Especialización, Horarios Disponibles. Una vez filtrado deberían aparecer solo los turnos relevantes a las condiciones especificadas.
Usuario	Paciente

Prioridad	Alta
------------------	------

ID	RF09
Nombre	Historial de turnos
Descripción	El sistema debe permitir a los pacientes que puedan consultar su historial de turnos. En el que figure: sede, especialización, médico, fecha, horario, diagnóstico, análisis pedidos y recetas.
Usuario	Paciente
Prioridad	Alta

ID	RF10
Nombre	Visualización con Agenda
Descripción	El sistema debe permitir a los médicos visualizar su carga laboral. Mediante una interfaz gráfica el médico puede ver los datos de los turnos que le corresponden en el día/semana/mes/año, incluyendo nombre del paciente, horario, detalle de la consulta. También debe poder ingresar a los datos clínicos del paciente desde la información del turno.
Usuario	Médico
Prioridad	Alta

ID	RF11
Nombre	Recetas digitales
Descripción	El sistema debe permitir acceder al módulo preexistente de farmacia y extender sus funcionalidades para permitir el recetado virtual de medicamentos. Para esto el médico llenará un formulario en el cual indique el nombre y apellido del paciente, identificador del medicamento, obra social y número correspondiente del paciente y por último la cantidad de ese medicamento que se debe recetar. Este formulario y su información es luego procesada por el módulo preexistente.
Usuario	Paciente
Prioridad	Alta

ID	RF12
-----------	------

Nombre	Consultar historia clínica del paciente
Descripción	Una vez que se registre un turno, el médico debe poder acceder a la historia clínica del paciente ordenada por fecha. Luego de finalizar el turno el médico todavía podrá acceder a su historia clínica durante un mes. La historia clínica de un paciente solo puede ser consultada por los médicos que lo hayan atendido.
Usuario	Médico
Prioridad	Alta

ID	RF13
Nombre	Agregar información a la historia clínica del paciente
Descripción	Una vez que se termina un turno o durante el mismo, el sistema debe permitir una actualización de la historia clínica del paciente agregando los datos y estudios relacionados con el turno.
Usuario	Paciente - Médico
Prioridad	Alta

ID	RF14
Nombre	Consulta por videollamada
Descripción	La consulta de paciente-médico se realizará por videollamada, utilizando google/meet. En caso contrario se realizará por whatsapp. La reunión tendrá una duración máxima de 35 minutos. Si a la hora de pedir la consulta el paciente eligió como medio de comunicación google meet, el médico creará el link de la sala de meet y la compartirá al paciente, 10 minutos antes de la consulta por email. En caso contrario, lo llamara por whatsapp en la fecha y horario de la consulta.
Usuario	Paciente - Médico
Prioridad	Alta

ID	RF15
Nombre	Consulta de estudios clínicos

Descripción	El paciente podrá consultar desde el módulo de telemedicina su historia clínica, y podrá descargar los resultados de estudios clínicos que hayan sido cargados previamente por un médico.
Usuario	Paciente
Prioridad	Media

ID	RF16
Nombre	Facturación
Descripción	El sistema debe permitir que el médico pueda facturar los turnos realizados desde el módulo de su perfil personal. Una vez que un turno termine (sea porque se atendió al paciente o hubo una ausencia del mismo) el médico debe poder registrarlo y luego realizar la facturación comunicándose con el módulo homónimo preexistente del sistema.
Usuario	Paciente
Prioridad	Media

ID	RF17
Nombre	Pre-Admision
Descripción	El sistema debe permitir que, si así lo encuentra necesario, el médico que realizó una consulta debe poder, luego, desde su perfil personal, pre-admitir a un paciente a internación conectándose con el módulo preexistente de admisión y así dejando en manos el proceso al staff que trabaja en las sucursales.
Usuario	Medico
Prioridad	Media

ID	RF18
Nombre	Servicio Cloud Computing
Descripción	Se contratará el servicio de cloud computing en Amazon Web Services, para el despliegue del módulo de telemedicina de esta forma se evitará realizar una gran inversión inicial y será más accesible en casos en que sea necesario escalar elásticamente debido a picos de demanda.

	<p>Se contratará a un experto con certificación en AWS para que lleve a cabo la estrategia de seguridad en la nube.</p> <ul style="list-style-type: none"> - configuración de Amazon S3 - control de cambios - permisos y credenciales - controles de seguridad - gestión de identidades y claves
Usuario	Paciente - Medico - Administrador
Prioridad	Media

ID	RF19
Nombre	Registro de pacientes vacunados
Descripción	<p>Se llevará un registro de los pacientes vacunados. Los ministerios nos brindaran los listados de nombre y apellido, dni, fecha y hora del turno, tipo de vacuna, número de lote de los pacientes a vacunar.</p> <p>Cuando el pacientes se presente en la sucursal asignada previamente para vacunarse, se le tomará presentismo y se le hará algunas preguntas de protocolo y también se registraron</p>
Usuario	Medico - Administrador
Prioridad	Media

ID	RF20
Nombre	Registro de turnos para vacunación
Descripción	<p>Los turnos disponibles se almacenará en un Mongo DB. Por un lado se guardará en una colección los turnos disponibles para los pacientes de CABA y en otra colección estarán los pacientes de la provincia de Buenos Aires.</p>
Usuario	Sistema
Prioridad	Alta

ID	RF21
Nombre	Obtención de turnos disponibles
Descripción	Para este requerimiento se desarrollará un cron que se ejecutará en un SO Linux periódicamente para invocar a la API Observer para que este último pueda obtener los turnos disponibles que son obtenidos desde las APIs de los Ministerios. La API Observer se integrará con Amazon SQS para manejar las solicitudes que no pudieron procesarse.
Usuario	Sistema
Prioridad	Media

ID	RF22
Nombre	Procesar turnos disponibles
Descripción	Se consultará el módulo de Turnos para empezar a gestionar el turno del paciente. Esta tarea será responsabilidad de la API Central Vacunación.
Usuario	Sistema
Prioridad	Media

ID	RF23
Nombre	Notificar al paciente sobre su turno disponible
Descripción	Mediante los medios de contacto que el paciente tenga cargado en el sistema, se le enviará una notificación por cada uno de los medios de contacto.
Usuario	Sistema
Prioridad	Media

Requerimientos no Funcionales

ID	RNF01
Nombre	Usabilidad
Descripción	Las interfaces del sistema serán intuitivas para los usuarios de cualquier edad. Y tendrá un tiempo de adaptación máximo de 5 días o 40hs de uso. También proporciona mensajes de error precisos y orientados al usuario final.

Prioridad	Alta
------------------	------

ID	RNF02
Nombre	Fiabilidad
Descripción	<p>Se subirán las historias clínicas a un servicio de nube AWS, con el objetivo de tener disponible una versión por fuera de los servidores físicos de la clínica y así resguardarse de un posible fallo de los mismos.</p> <p>El historial clínico será guardado en un servidor cloud, con las regulaciones y restricciones necesarias que exige la ley de protección de datos sensibles en nuestro país.</p> <p>Por eso mismo, el servidor cloud que elegiremos estará en Europa, ya que ellos cumplen con las leyes vigentes de Argentina.</p>
Prioridad	Alta

ID	RNF03
Nombre	Seguridad de los datos
Descripción	<p>Todos los datos de usuario deben permanecer íntegros, confidenciales y seguros.</p> <p>Todas las comunicaciones entre los módulos existentes será a través de VPN. Mientras que el acceso de la página web de telemedicina y vacunación será por protocolo http</p> <p>Y las contraseñas del módulo de telemedicina y vacunación deben estar encriptadas utilizando el algoritmo RSA.</p>
Prioridad	Alta

ID	RNF04
Nombre	Alta disponibilidad
Descripción	<p>El módulo de telemedicina y vacunación estarán en un servidor cloud. Que nos permitirá realizar configuración y contratación de diferentes servicios, que pueden llegar a brindarnos una disponibilidad de 99,9%</p> <p>Mientras que el data center actual, será duplicado una copia exacta en otra sucursal. Y se replicara los servidores de aplicación y base de datos</p>
Prioridad	Alta

ID	RNF05
Nombre	Servicio de Internet Simétrico
Descripción	Se contratará a dos proveedores diferentes de internet simétrico con un ancho de banda de 300Mbps para la sucursal CABA y la sucursal Norte.
Prioridad	Alta

ID	RNF06
Nombre	Seguridad
Descripción	Se guardarán los logs que se generen por comunicación entre módulos y quienes consulten a la base de datos.
Prioridad	Alta

ID	RNF07
Nombre	Accesibilidad
Descripción	La aplicación web a desarrollar será web responsive, que permitirá una buena experiencia de navegación independientemente del dispositivo que se utilice.
Prioridad	Media

ID	RNF08
Nombre	Interoperabilidad
Descripción	El sistema nuevo debe poder comunicarse y utilizar los módulos de farmacia, facturación y admisión
Prioridad	Alta

ID	RNF09
Nombre	Tolerancia a fallas para la obtención de turnos disponibles

Descripción	El procesamiento de un turno disponible es una funcionalidad relevante, por eso se contempla que esta solicitud pueda fallar y en caso de que suceda, se encolará en un servicio de cola de mensajes que nos provee AWS.
Prioridad	Alta

ID	RNF10
Nombre	Alta disponibilidad para el procesamiento de turnos disponibles
Descripción	En determinados momentos el volumen de procesamiento de turnos disponibles puede ser muy grande, por eso se deberá balancear la carga para poder atender a todas esas peticiones. Para esto se usarán los LOAD BALANCER que nos provee AWS.
Prioridad	Alta

ID	RNF11
Nombre	Seguridad en almacenamiento de los turnos disponibles
Descripción	Los turnos disponibles almacenados serán almacenados bajo las normas de seguridad que nos ofrece AWS y de nuestro lado se seguirá las mejores prácticas para mantener la integridad y confidencialidad provistas por la Resolución 47/2018.
Prioridad	Alta

ID	RNF12
Nombre	Flexibilidad y performance en almacenamiento de turnos disponibles
Descripción	El tipo de información matchea con los de tipo clave-valor y al ser una db no relacional, el tipo de información a guardar puede modificarse de manera muy simple. La buena performance de mongo DB es gracias a su capacidad para manejar grandes cantidades de datos no estructurados.
Prioridad	Alta

Planificación

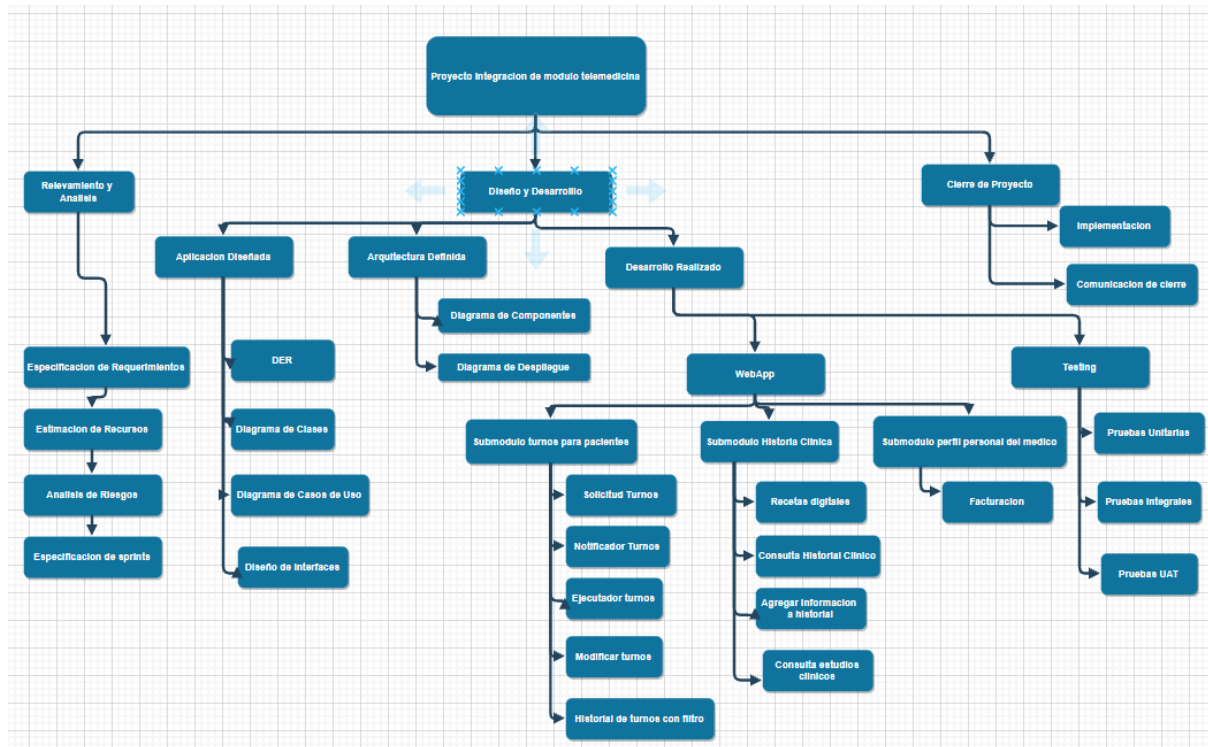
Estructura del Desglose del Trabajo

1. Relevamiento y análisis
 - 1.1. Especificación de requerimientos
 - 1.2. Estimación de recursos
 - 1.3. Análisis de riesgos
 - 1.4. Especificación de sprints
2. Diseño y desarrollo
 - 2.1. Aplicación web telemedicina
 - 2.1.1. DER
 - 2.1.2. Diagrama de clases
 - 2.1.3. Diagrama de casos de usos
 - 2.1.4. Diseño de interfaces
 - 2.2. Arquitectura diseñada
 - 2.2.1. Diagrama de componentes
 - 2.2.2. Diagrama de despliegue
 - 2.3. Desarrollo realizado
 - 2.3.1.1. Web App
 - 2.3.1.1.1. Submodulo de Login
 - 2.3.1.1.1.1. Creación de usuario
 - 2.3.1.1.1.2. Modificación de usuario
 - 2.3.1.1.2. Submódulo turnos para pacientes
 - 2.3.1.1.2.1. Solicitud turnos
 - 2.3.1.1.2.2. Notificador turnos
 - 2.3.1.1.2.3. Ejecutor turnos
 - 2.3.1.1.2.4. Modificar turnos
 - 2.3.1.1.2.5. Historial de turnos con filtro
 - 2.3.1.1.3. Submódulo historia clínica
 - 2.3.1.1.3.1. Recetas digitales
 - 2.3.1.1.3.2. Consulta historial clínico
 - 2.3.1.1.3.3. Agregar información historial
 - 2.3.1.1.3.4. Consulta de estudios médicos
 - 2.3.1.1.4. Submódulo perfil personal médico
 - 2.3.1.1.4.1. Facturación
 - 2.3.1.2. Testing
 - 2.3.1.2.1. Pruebas unitarias
 - 2.3.1.2.2. Pruebas integrales
 - 2.3.1.2.3. Pruebas UAT

2.3.2. Cierre del proyecto

2.3.2.1. Implementación

2.3.2.2. Comunicación de cierre



EDT en: <https://app.diagrams.net/#G1agTenAlAjHxzTK3R7b0SBuvhZVJrVm3Q>

Especificación de roles

El equipo de trabajo consta de:

- 1 Product Owner
- 1 Scrum Master
- 2 desarrolladores BackEnd
- 2 desarrolladores FrontEnd
- 1 Arquitecto Software
- 1 Cloud Service Specialist con certificación AWS
- 2 QA / Tester
- 1 Especialista en Seguridad

El Product Owner tendrá el conocimiento de las necesidades del producto y buscará el mayor rédito o retorno de éste. Será el encargado de gestionar el Product Backlog.

El Scrum Master será el encargado de coordinar las reuniones, será el enlace para el equipo.

Se contará con un equipo de desarrollo BackEnd y uno FrontEnd que estará integrado por un desarrollador Sr y otro Ssr.

El Arquitecto/a de software será el encargado o encargada de estructurar la infraestructura del equipo y los QA/Tester estarán encargados/as de encontrar errores durante y luego del desarrollo.

Para la Arquitectura diseñada por el Arquitecto/a se tendrá un especialista en servicios cloud con certificación en AWS para la integración a la nube de los datos. Por último se utiliza un Especialista en Seguridad para todo el equipo, manteniendo siempre la integridad de datos y evitando las posibles fallas de seguridad (algo particularmente importante dado el alcance del proyecto y los datos personales de individuos que usarán el producto).

Desarrollo

En base a un análisis de metodologías, se decidió utilizar la metodología ágil Scrum para la realización del proyecto. Las características principales por las cuáles se eligió este método son:

- Agilidad: Por definición este método prioriza la velocidad, lo cuál en el contexto de la pandemia es de gran beneficio.
- Productividad: Gracias a las constantes reuniones y la planificación desacoplada y retroalimentativa se obtiene una mayor velocidad de progreso y entregables demostrables.
- Flexibilidad: Esta metodología permite la incorporación de comentarios y feedback dentro del flujo de desarrollo haciendo al proyecto permeable a nuevos requerimientos o consideraciones que devienen del avance real del mismo.

Especificación de los Sprints

Los sprints serán de 10 días hábiles (dos semanas), con una jornada laboral de 8 horas, por lo que cada Sprint durará 80 hs y dado que se estima una duración de 4 meses, habrá un total de 8 Sprints (2 Sprint por mes) y 640 hs totales. Es un proyecto de gran envergadura pero de mucha urgencia debido a las condiciones del contexto de pandemia, por lo que debe haber un desarrollo que permita velocidad y eficiencia.

Sprint 1

- Estudio de las tecnologías disponibles y requeridas.
- Creación de los diagramas de Diseño de Software.
- Creación de los diagramas de Arquitectura de la solución.
- Diseño de las interfaces.

En este primer Sprint, se buscará generar una base de diseño para el desarrollo del proyecto. Se estudiará el estado del arte y los requerimientos de la solución nueva y para la adaptación a la existencia de módulos previos. Se creará la base de Arquitectura de Software para el proyecto. Se diseñarán, además, las interfaces de la solución para visualizar y crear una base para el desarrollo posterior de los mismos.

Sprint 2

- Creación del sistema de autenticación.
- Desarrollo de las interfaces para toma de turnos: solicitud, notificación y ejecutor de turnos.
- Desarrollo de las interfaces de usuario para ingreso.

En este Sprint se trabajará sobre el submódulo de turnos para pacientes. Se creará todo el sistema de sesiones e interfaces consecuentes. Se desarrollará el front end para las interfaces de toma de turno (funcionalidades especificadas) y acceso de usuario.

Sprint 3

- Desarrollo de la toma de turnos, funcionalidades: solicitud, notificación y ejecutor de turnos.
- Desarrollo de las interfaces para la toma de turnos: Modificación de turno e Historial de turnos con filtros.
- Desarrollo de las interfaces historia clínica: Recetas clínicas y Historial Clínico)

En este Sprint se seguirá trabajando sobre el submódulo de toma de turnos sobre las funcionalidades y las interfaces trabajando el Front End y el Back End también. Se dará comienzo al trabajo sobre el submódulo de historia clínica.

Sprint 4

- Desarrollo de la toma de turnos, funcionalidades: Modificación de turno e Historial de turnos con filtros.
- Desarrollo de la historia clínica, funcionalidades: Recetas clínicas y Historial Clínico).
- Desarrollo de las interfaces de historia clínica: agregar información a historial y consulta de estudios clínicos.

En este Sprint se finalizará el submódulo de toma de turnos y se continuará con el módulo de historia clínica comenzando el Back End y continuado con el Front End.

Sprint 5

- Desarrollo de la historia clínica, funcionalidades: agregar información a historial y consulta de estudios clínicos.
- Desarrollo de la interfaz de perfil personal del médico.

En este Sprint se finalizará el desarrollo del submódulo de historia clínica en el Back End y se comenzará el Front End del último submódulo de perfil personal del médico.

Sprint 6

- Desarrollo de las funcionalidades de facturación.
- Desarrollo de base de datos.
- Realización de pruebas unitarias sobre desarrollos.

En este Sprint se comenzará con las pruebas unitarias, en particular las concernientes a los desarrollos previamente realizados. Se finalizará el submódulo

de perfil personal con el Back end concerniente a la facturación. Además, se desarrollarán los elementos requeridos para almacenar datos en una base de datos.

Sprint 7

- Integración con base de datos.
- Pruebas unitarias sobre bases de datos.
- Pruebas integrales del sistema.

En este Sprint se integrará el desarrollo con lo realizado para el almacenamiento de datos en una BD y se realizarán pruebas unitarias para verificar el correcto funcionamiento. Con todos los trabajos de desarrollo finalizados, se realizarán las pruebas integrales del sistema.

Sprint 8

- Integración con el servicio.
- Desarrollo de modificaciones sobre resultados de pruebas integrales del sistema.
- Realización de pruebas UAT.

En este último Sprint se integrará lo realizado con el servicio real antes desarrollando las modificaciones pertinentes dadas las pruebas integrales previamente realizadas. Por último, una vez utilizado por los usuarios, se realizarán pruebas de aceptación de usuario.

Diagrama de GANTT

Se generó un diagrama para visualizar la dependencia y duración de las tareas además de la carga para cada equipo. Dejamos a disposición este [Diagrama de GANTT de los Sprints](#).

Implementación

Luego de cada Sprint dedicado al desarrollo, se realizarán pruebas integrales para verificar el funcionamiento del sistema integralmente; para luego poner en producción al sistema y entregárselo al cliente. Con el sistema se le entregará un Manual de usuario al cliente para que pueda capacitar a los profesionales en su uso. De todas formas, estaremos siempre en contacto por cualquier duda o imprevisto que pueda surgir durante los primeros meses del uso del sistema.

Costo de Recursos Humanos

En cuanto a la consideración de costo relacionado con uso de mano de obra capacitada para el proyecto, se considera la siguiente tabla de valores para el costo mensual:

Recurso Humano	Cantidad	Valor	Costo Total	Fuente
Product Owner	1	150,000.00	150,000.00	https://www.glassdoor.com.ar/Sueldos/product-manager-sueldo-SRCH_KO0.15.htm
Scrum Master	1	163,000.00	163,000.00	https://www.glassdoor.com.ar/Sueldos/scrum-master-sueldo-SRCH_KO0.12.htm#:~:text=El%20sueldo%20nacional%20promedio%20de,es%20de%20%24140,000%20en%20Argentina.
Desarrollador Sr.	2	228,000.00	456,000.00	https://www.glassdoor.com.ar/Sueldos/desarrollador-senior-sueldo-SRCH_KO0.20.htm#:~:text=El%20sueldo%20nacional%20promedio%20de,es%20de%20%24198,868%20en%20Argentina.
Desarrollador Ssr.	2	122,000.00	244,000.00	https://www.glassdoor.com.ar/Sueldos/desarrollador-java-ssr-sueldo-SRCH_KO0.22.htm#:~:text=El%20sueldo%20nacional%20promedio%20de,es%20de%20%2495,023%20en%20Argentina.
Arquitecto de Software	1	232,000.00	232,000.00	https://www.glassdoor.com.ar/Sueldos/arquitecto-de-software-sueldo-SRCH_KO0.22.htm#:~:text=No%20se%20informa%20C3%B3%20ninguna%20remuneraci%C3%B3n%20en%20efectivo%20adicional,sueldos%20de%20Arquitecto%20de%20Software%20en%20tu%20C3%A1rea.
Cloud Service Specialist con certificación AWS	1	175,000.00	175,000.00	https://www.glassdoor.com.ar/Pago-mensual/Globant-Cloud-Engineer-Pago-mensual-E150678_D_KO8.22.htm
QA/Tester Sr.	2	142,000.00	284,000.00	https://www.glassdoor.com.ar/Sueldos/qa-senior-sueldo-SRCH_KO0.9.htm
Especialista en Seguridad	1	164,000.00	164,000.00	https://www.glassdoor.com.mx/Sueldos/buenos-aires-especialista-en-seguridad-informatica-sueldo-SRCH_IL_0_12_IC2242084_KO13.50.htm#:~:text=El%20sueldo%20promedio%20de%20un,de%20%24136%20C984%20en%20Buenos%20Aires.
TOTALES:	11		1,868,000.00	

Teniendo en cuenta que la duración del proyecto es de 4 meses, **el costo sería de 7,472,000 millones de pesos.**

Análisis de Riesgos

RIESGO 1

Nombre	Contagio de COVID en el equipo
--------	--------------------------------

Probabilidad	Impacto
Media	Medio
Severidad	
Alto	
Descripción	Dentro del contexto de la pandemia si un miembro del equipo de desarrollo se contagia y tiene algunas complicaciones o tiene algún familiar al cual debe cuidar, entonces esto lo llevará a un impedimento prolongado de sus tareas generando un retraso significativo en las entregas pactadas.
Componentes afectados	Todo el proyecto

Plan de mitigacion

Se desarrollará el proyecto con una metodología agile que permita desacoplar al máximo los trabajos entre los profesionales además de reforzar prácticas de control de salud sencillas y frecuentes entre los trabajadores.

Plan de contingencia

En caso de que haya un contagio que no permita la correcta realización de las tareas del equipo se reducirá la velocidad de desarrollo y se pasarán a realizar solo las tareas fundamentales para la mejor producción posible teniendo en cuenta que no hay equipos de un solo trabajador en las áreas.

RIESGO 2

Nombre	Cambio repentino del equipo de trabajo
Probabilidad	Impacto
Media	Medio
Severidad	
Alto	
Descripción	El proyecto se lleva a cabo en época de pandemia, por lo cual la demanda de personal calificado en el sector IT subió exponencialmente. Nos enfrentamos a posibles fugas de talentos de nuestro capital humano.
Componentes afectados	Todo el proyecto

Plan de Mitigación

Se realizarán encuestas bimestrales para evaluar el clima laboral. Se evaluará el desempeño laboral de los empleados y esto nos ayudará a desarrollar estrategias de administración salarial para retener a los empleados con mayor desempeño o necesarios para el proyecto. Se ofrecerán bonos de captación, bonos por proyectos satisfactorios e incrementos salariales más de 3 veces al año con fin de no perder poder adquisitivo frente a la inflación.

Plan de Contingencia

En caso del cese de la relación laboral se debe priorizar quedar en buenos términos y dar la posibilidad de reincorporarse en algún futuro.

Si el empleado que renuncia es un fundamental para el desarrollo de nuestro proyecto se debe considerar ofrecer una contraoferta si su renuncia se debe a una cuestión salarial.

El área de recursos humanos debe mantenerse en búsqueda constante de nuevos talentos especialmente en los perfiles IT claves para el desarrollo del proyecto.

RIESGO 3

Nombre	Cambios en normativas del Gobierno		
Probabilidad	Impacto	Severidad	
Media	Medio	Alto	
Descripción	Actualmente se encuentra vigente una ley de protección de datos. Si llegase a haber un cambio durante el tiempo que tarda en desarrollarse este proyecto, entonces esto puede ocasionar un cambio significativo en el desarrollo.		
Componentes afectados	Todo el proyecto		

Plan de Mitigación

Se estará pendiente de los cambios que puedan a llegar a surgir con la ley de protección de datos. Lo que se pretende con esto es estar al tanto de estos cambios desde el primer momento y que no nos sorprenda, para así poder tener más tiempo para realizar las modificaciones necesarias.

Plan de Contingencia

Llegado el caso en el que surja algún cambio en esta ley de protección de datos, se analizará y se evaluará la misma para decidir si se realiza una replanificación en caso de que se incluya la misma. Esto es en caso de que el cambio en la ley exija también un cambio en los requerimientos.

RIESGO 4

Nombre	Problemas de conectividad		
Probabilidad	Impacto	Severidad	
Media	Medio	Medio	
Descripción	Debido a la pandemia, el trabajo se realizará en modalidad 100% remoto. En este contexto si llegaran a aparecer problemas en la conexión a internet ya sea por cortes de luz o por fallas con el ISP entonces esto luego podría ocasionar retrasos en los plazos de entrega de las tareas.		
Componentes afectados	Todo el proyecto		

Plan de Mitigación

Para poder solventar estos retrasos que pudieran llegar a surgir por estos problemas de conectividad, las tareas que quedaron en stand by se delegarán hacia otros colaboradores menos atareados, para ello el colaborador que tuvo el problema de conectividad deberá notificar en tiempo y forma a su par o líder directo para visualizar esta anomalía.

RIESGO 5

Nombre	Discrepancia y conflicto entre los miembros del equipo		
Probabilidad	Impacto	Severidad	
Media	Medio	Baja	
Descripción	El impacto que el COVID-19 causó en las personas es uno de los principales desafíos a los que se enfrentaron las organizaciones.		

	Si aparecen situaciones en las que no se llega a un acuerdo ya sea en la toma de decisiones dentro del equipo u opiniones y hasta discusiones entre los miembros del equipo entonces esto puede generar un mal clima de trabajo debilitando al equipo.
Componentes afectados	Todo el proyecto

Plan de Mitigación:

Con el fin de mitigar este riesgo, se favorecerá un ambiente de confianza para generar comodidad total entre los trabajadores.

Definir una cultura colaborativa para que todos puedan tener en mente las metas y los objetivos conjuntos.

Emplear siempre una cultura constructiva, implicar a los trabajadores en la visión de futuro y mantenerlos motivados para adaptar e innovar es clave para que sus aportaciones sean válidas a nivel individual y grupal.

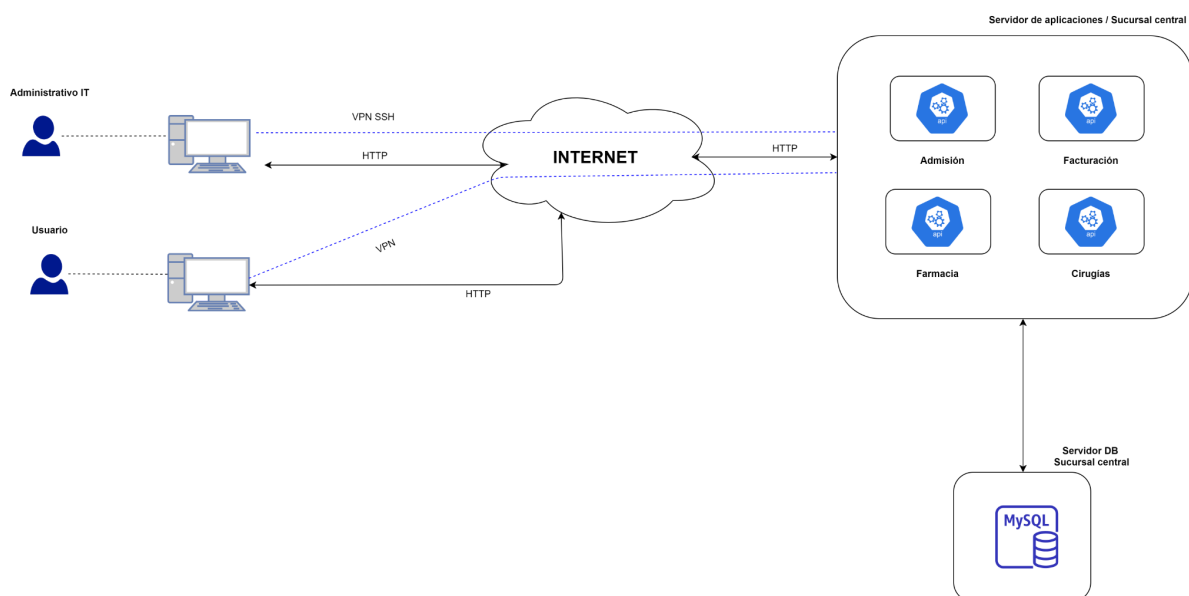
Ejecutar dinámicas de grupo para fortalecer el trabajo en equipo y el compañerismo.

Diseño de Arquitectura de Software

Análisis técnico y funcional

Al momento de realizar este documento, consideramos que el sistema actual no tiene la capacidad de soportar la incorporación de los nuevos módulos (Telemedicina y vacunación).

Arquitectura de SW actual



El software actual es un sistema al cual se accede por una VPN montada sobre internet. En las condiciones actuales el sistema funciona correctamente, pero con la actualización de los nuevos módulos va a comenzar a crecer, en número de usuarios y solicitudes, y el sistema actual no proyecta un escalamiento vertical u horizontal del mismo.

Infraestructura de HW actual

La infraestructura actual es insuficiente para las necesidades de almacenamiento, procesamiento y alta disponibilidad requeridas y deberá ser ampliado.

Actualmente poseen dos servidores físicos, un servidor de aplicaciones y un servidor de la DB. Y no cuenta con un backup para recuperación de datos.

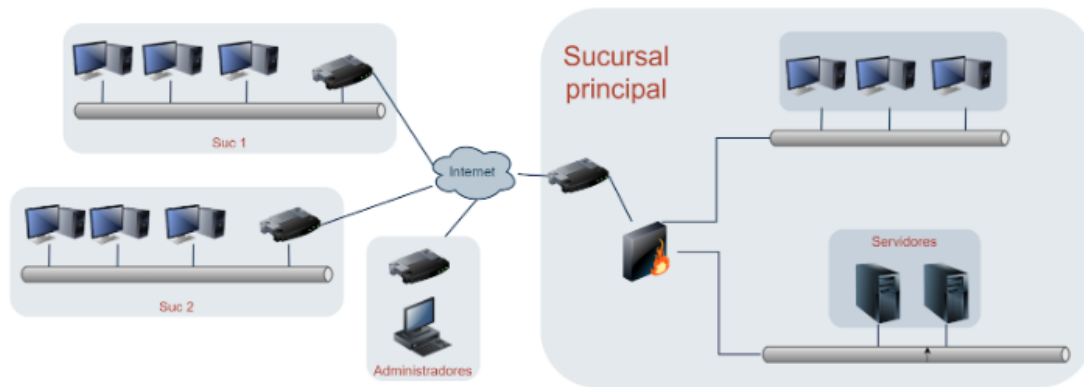
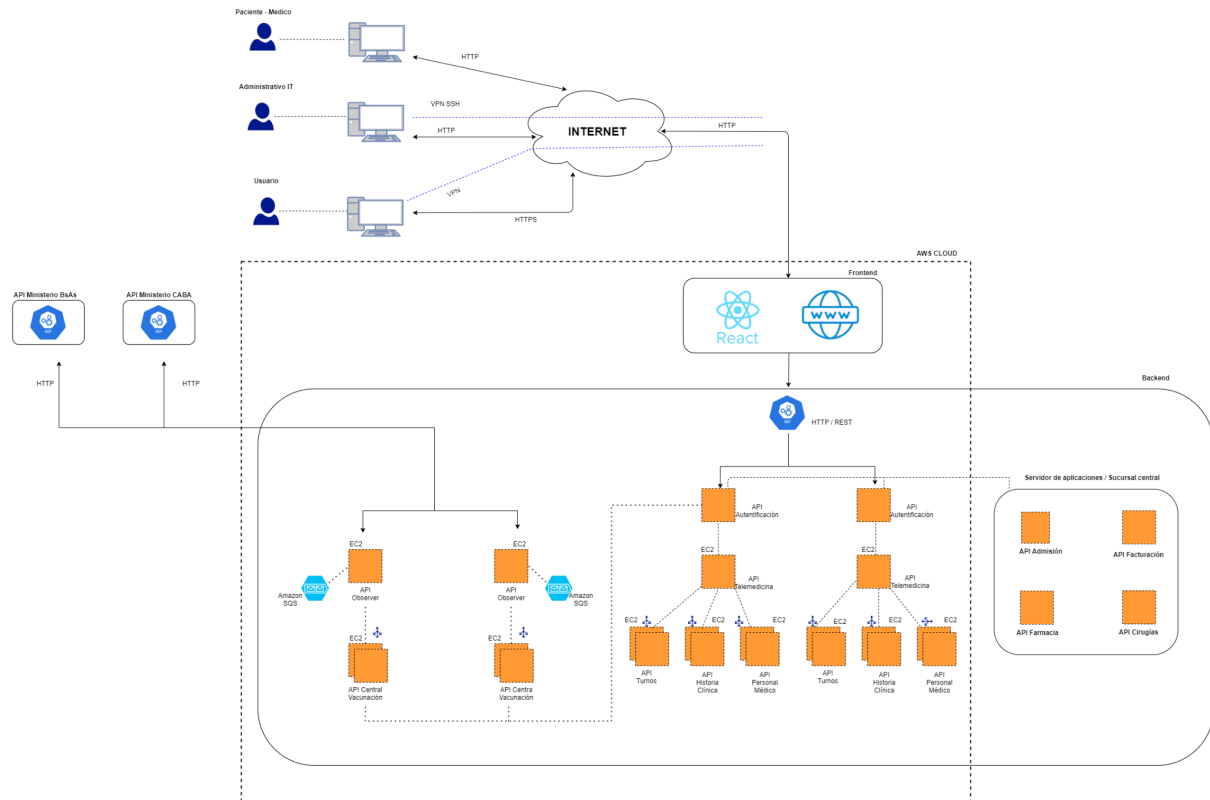


Diagrama de Arquitectura de SW Propuesta



<https://postimg.cc/rDnDsx6Q>

Después de realizar el relevamiento técnico se llegó a la conclusión de optar por una arquitectura de microservicios.

Para el módulo de telemedicina será necesario garantizar la máxima concurrencia que es de 15 mil afiliados.

Si bien aún no podemos estimar cómo será la recepción de los pacientes con la app web de telemedicina, tampoco podemos desestimar tener la máxima concurrencia.

Por tal motivo la mejor manera que encontramos es a través de un servidor cloud.

Esto nos garantiza la alta disponibilidad, la contratación de instancias a demanda. Ya que necesitamos desarrollar una solución escalable y flexible que cubran las demandas del trabajo y la atención de manera remota en la actual situación.

Se propone desarrollar y alojar los nuevos módulos (Telemedicina y Vacunación) en la nube, Amazon Web Services (AWS), contratando el servicio de Amazon Elastic Compute Cloud (Amazon EC2). Esto nos permitirá el escalamiento vertical y horizontal de nuestra aplicación, pudiendo contratar instancias bajo demanda (On-Demand) que nos permitan soportar el aumento de solicitudes a nuestra aplicación.

Autenticación de Usuarios

El nuevo front-end se desarrollará en React, se accederá a nivel de usuario por el módulo de autenticación. Los microservicios se comunicarán entre sí, pero previamente se validarán las credenciales de los usuarios, para verificar que estén habilitados a las funcionalidades, para la autenticación a nivel de aplicación se utilizará el servicio de AWS Identity and Access Management (IAM) para la gestión de credenciales, permisos y accesos a los módulos de la aplicación.

Los empleados de la clínica tendrán que solicitar al área IT, la creación de un usuario y contraseña. Cuando ingresen por primera vez, tendrán que modificar su contraseña y también se les solicitará que acepten las políticas de privacidad de la información de la clínica.

Los pacientes podrán crear su usuario a través del app web, se le desplegará un formulario para que ingrese sus datos personales y la contraseña.

Luego se validan las credenciales y se habilitarán las funcionalidades correspondientes al tipo de usuario que se haya ingresado.

También se obtendrá un certificado SSL para nuestra página web, y la comunicación entre los microservicios será a través del protocolo HTTPS.

Lógica de negocio para la vacunación COVID:

El módulo de vacunación será desarrollado como un microservicio y alojado en un servidor cloud. Se espera que los listados de vacunación sean brindados por una API dada por los ministerios de salud de CABA y provincia.

Teniendo en cuenta que algunos de nuestros módulos existentes como factura, farmacia y admisión interactúan con el de telemedicina, realizaremos algunas modificaciones en estos para mantener la comunicación entre ambas arquitecturas.

Se tendrá un módulo llamado **API Observer** que se va a encargar de consultar estos servicios (Ministerio de salud de CABA y provincia) cada x cantidad de tiempo a través de un proceso **cron**.

En el caso de obtener la lista de pacientes, este módulo armará una petición por cada uno de los pacientes habilitados y delegará su procesamiento a la **API Central de Vacunación**.

Si este último, no logró procesarlo, la **API Observer** encolará esa petición para su posterior procesamiento.

En caso de que se pueda procesar, devolverá un Http Status entre 200 y 300 para que no se vuelva a encolar.

El procesamiento de la petición consta en los siguientes pasos:

- Se accederá al submódulo de Historial clínico para validar la identidad del paciente
- Accede al submódulo de Turnos
- Con la disponibilidad del paciente se determinan turnos disponibles
- Mediante los diferentes medios disponibles (email o teléfono) que tenga el paciente se le notificará sobre los turnos disponibles
- Se guardará en una DB el registro de este suceso

Respecto a la DB recientemente mencionada se contará con un MongoDB el cuál contendrá dos colecciones, uno para los pacientes de CABA y otro para los pacientes de provincia. El mismo contará con la siguiente estructura:

```
{
  numero_de_paciente: int,
  dni: int,
  vacunas: [
    {
      fecha: date,
      tipo_de_vacuna: string,
      numero_de_lote: int,
      estado: string
    },...
  ]
}
```

Las razones por las cuales se decidió usar MongoDB son las siguientes:

- **Flexibilidad:** Al ser Schema Less, es mucho más simple poder variar los campos sin tener que ejecutar scripts que crean campos con valores por defecto cada vez que se quiera agregar un campo nuevo en los registros.
- **Poderosa sintaxis para hacer consultas:** Tenemos múltiples operadores que nos permiten crear consultas poderosas con poco código, además que contamos con las Agregaciones que son un mecanismo que nos permite realizar operaciones entre múltiples colecciones.
- Es ideal para entornos con pocos recursos de computación
- Mejor **performance**, las consultas son más rápidas

La información enviada desde la API Central Vacunación hacia el servicio de almacenamiento (Amazon S3) donde se encuentran almacenadas las colecciones con los turnos disponibles una Mongo DB viajarán de manera encriptada (HTTPS). Antes del envío del request con la información del turno disponible se realizarán las siguientes validaciones:

- **Validación de parámetros:** Se comprobará la validez de todos los datos como ser el formato y validez.
- **Validación contra cyber-ataques:** Protección contra los ataques de inyección SQL, utilizando formatos específicos de datos incluso rangos y/o conjuntos de posibles valores y tamaño de campos.
- **Validar los tipos de contenido (Content-Type):** Siempre se debe validar el Content-Type por parte del cliente y validar primero que contenga ese tipo de dato.
- **Validar los tipos de contenido de salida(Accept):** No se debe admitir este header vacío o sin un valor en específico.
- **Validación de las URL:** Esto es necesario para la inserción de comandos, desbordamiento del búfer, manipulación de datos ocultos, ataques de cadenas de formato.
- **Codificación JSON:** Esto es principalmente para evitar la ejecución arbitraria de código javascript.

Para informar la aplicación de las vacunas aplicadas se correrá un proceso diario desde la API Observer, recorriendo la MongoDB filtrando por estado y fecha en forma de batch tratándolas de forma atómica, haciendo uso de la queue en caso de que falle el POST a las respectivas APIs de los Ministerios.

Backup and Recovery con MongoDB en la nube

Para esta DB se usará Amazon Simple Storage Service (**Amazon S3**) para mantener una copia de los datos en MongoDB. Esto es porque Amazon S3 almacena objetos de datos de forma redundante en varios dispositivos y en varias instalaciones y permite el acceso simultáneo de lectura y escritura por parte de muchos clientes independientes o subprocesos de aplicación. De esta forma podremos recuperarnos más rápido ante fallas o caídas de la DB.

Para las copias de seguridad usaremos MongoDB Cloud Manager, este es un servicio alojado de respaldo, monitoreo y automatización para MongoDB. Este servicio admite la realización de copias de seguridad y la restauración de conjuntos de réplicas y clústeres fragmentados desde una interfaz gráfica de usuario. Además con esta herramienta podremos crear instantánea de los datos a intervalos preestablecidos.

Seguridad de datos sensibles

Para resguardar la seguridad de los datos sensibles en la nube se tuvo en cuenta la contratación de un especialista con certificación en AWS.

Según el informe de CSA (Cloud security Alliance) la filtración de datos sensibles se produce por errores del cliente en la configuración y gestión de los servicios en la nube.

En cuanto a la **seguridad** en la nube para MongoDB por parte de AWS, ellos protegerán la infraestructura que ejecuta todos los servicios provistos en la nube de AWS. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube de AWS.

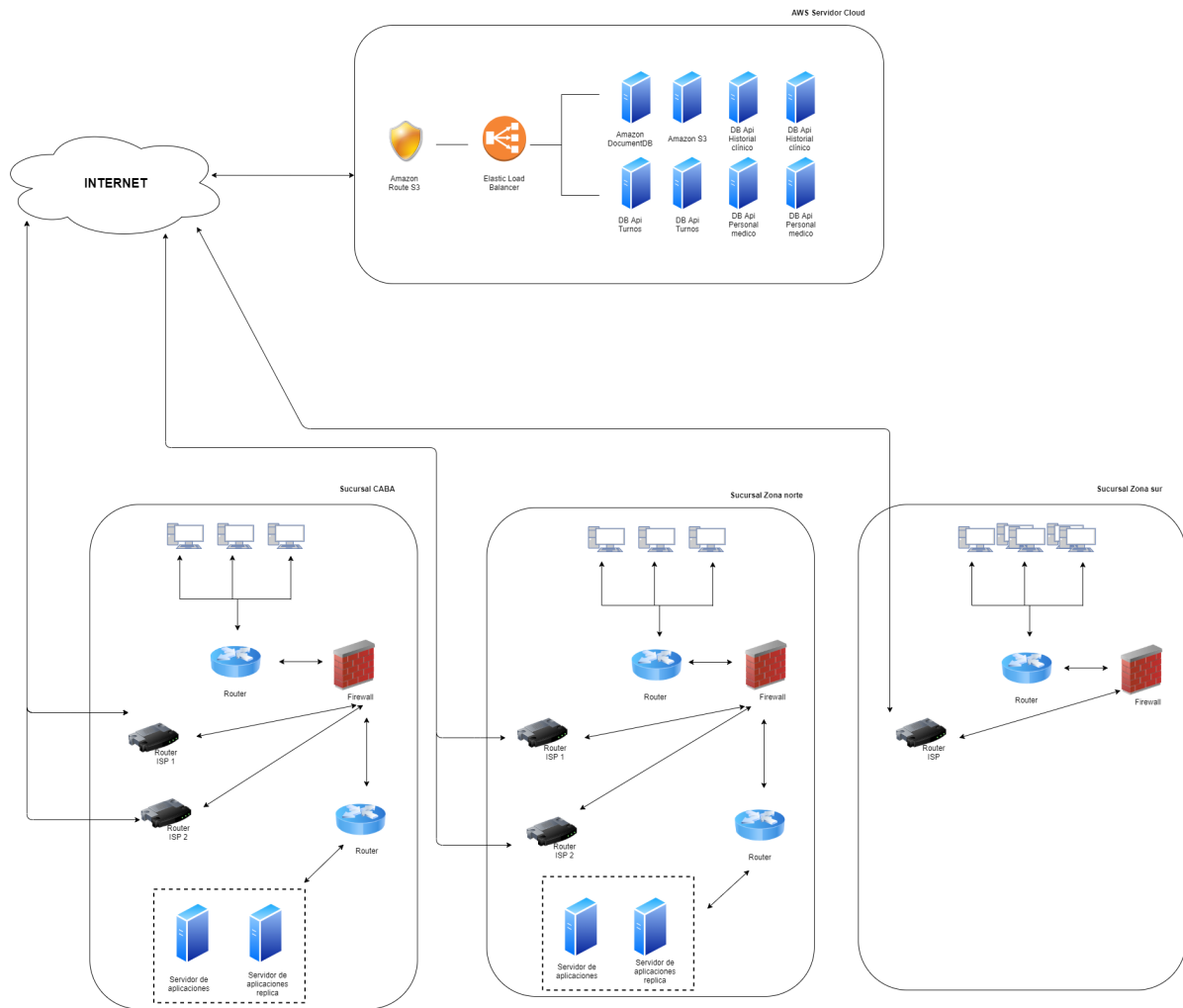
Por nuestra parte utilizaremos la herramienta de AWS Identity and Access Management (IAM) para administrar el acceso a los servicios y recursos de nuestra aplicación montada en AWS de manera segura.

Para el procesamiento de los datos sensibles se tendrá en cuenta **Ley 25326** de “Protección de Datos Personales” que incluye el Decreto Reglamentario N° 1558/2001 y normas complementarias (en adelante, “LPDP”) es una ley federal que aplica a la protección de los datos personales en Argentina y cuando los datos personales son transferidos internacionalmente para su procesamiento.

En el caso de los datos sensibles, la transferencia internacional, debe hacerse a países que revistan los mismos estándares de protección que nuestro país. Dentro de AWS se contratará servidores alojados en EU que tienen condiciones de licitud similares a la legislación argentina.

La Disposición No. 11/2016, derogada por la Agencia de Acceso a la Información Pública de Argentina (“Autoridad”) que emitió la Resolución 47/2018 (“Resolución 47”) bajo la LPDP. Esta Resolución describe nuevas medidas de seguridad recomendadas que están alineadas con las mejores prácticas y estándares internacionales, y están destinadas a proteger la confidencialidad e integridad de los datos personales durante su procesamiento, desde la recopilación de datos hasta la eliminación de datos. En particular, esta nueva resolución actualizó la lista de medidas y controles recomendados para administrar, planificar, controlar y mejorar la seguridad al procesar datos personales. Estas medidas de seguridad recomendadas se dividen en categorías de actividades relacionadas con el procesamiento, incluida la recopilación de datos, los controles de acceso, los controles de cambio, la copia de seguridad y la recuperación, la gestión de vulnerabilidades, la eliminación de datos, los incidentes de seguridad y los entornos de desarrollo. Además, la Resolución 47 incluye un listado de medidas de seguridad aplicables a los “datos sensibles” (según se define en la LPDP).

Infraestructura de Hardware y Redes Propuesta



<https://postimg.cc/GTvHM55p>

Para redirigir las peticiones de nuestros usuarios resguardando la escalabilidad y la alta disponibilidad, usaremos el servicio Amazon Route 53, este servicio termina redirigiendo las mismas a nuestras instancias EC2 mediante la traducción de nombres legibles para las personas. Este servicio conecta de forma efectiva las solicitudes de los usuarios con nuestra infraestructura en ejecución en AWS.

Nuestras aplicaciones en la nube de AWS serán máquinas virtuales EC2. De esta manera eliminamos la necesidad de invertir en el hardware, de manera que se pueda desarrollar en un tiempo menor. Podremos lanzar tantos servidores como se necesite, configurar la seguridad y las redes, además de administrar el almacenamiento. También podremos escalar hacia arriba o hacia abajo de acuerdo a la demanda que vaya surgiendo, se estima que habrá meses en los cuales se contará con una buena cantidad de stock y otros meses en los cuales no abundarán las vacunas. En cuanto a lo que respecta de la disponibilidad, estas instancias estarán ubicadas en diferentes regiones de alguna zona de disponibilidad.

Para distribuir automáticamente el tráfico entrante a la aplicación entre las varias instancias utilizaremos Elastic Load Balancing (ELB). De esta manera aumentamos la disponibilidad y mejoramos la tolerancia a fallas.

Nuestras instancias para las API Observer además de ir a buscar la info para planificar los turnos de vacunación también cuenta con una cola de mensajes, esto lo logramos haciendo uso del servicio Amazon SQS, de esta manera podemos desacoplar y ajustar la escala entre nuestros microservicios. De esta manera SQS nos abstrae bastante sobre la complejidad de tener a la API Observable y API Central Vacunación (esta API tendría la responsabilidad en lo que respecta a las reglas de negocio) sincronizadas, permitiendo a nuestros desarrolladores enfocarse más en lo que respecta el modelo de negocio y darle ese valor agregado correspondiente. El tipo de cola de mensajes que usaremos sería la estándar, en el cual permite una capacidad de procesamiento máximo, un ordenamiento de menor esfuerzo y una entrega de al menos una vez.

En lo que respecta a la persistencia de la información de los ciudadanos con sus respectivas vacunas se hará uso del servicio Amazon DocumentDB, el mismo está diseñado para cargas de trabajo escalables y permite que los procesos informáticos y el almacenamiento escalen de forma independiente. Además de que puede escalar la capacidad de lectura a millones de solicitudes por segundo. Gracias a este servicio ya no tendremos que preocuparnos por tareas de administración de la base de datos tales como el aprovisionamiento del hardware, la aplicación de parches, las instalaciones, las configuraciones, las copias de seguridad o el ajuste de escala.

Este servicio es compatible con la flexibilidad y el tipo de información que necesitábamos guardar.

En cuanto a la API de Telemedicina, esta se comunicará vía API REST con las demás APIs para lograr satisfacer con los requerimientos que tengan que ver con la nueva modalidad de trabajo y las funcionalidades correspondientes al nuevo contexto de pandemia.

Tanto la API de Historia Clínica como la de Personal Médico contarán con una db aprovechando todas las ventajas por tenerlas alojadas en la nube, flexibilidad, tolerancia a fallos, disponibilidad, backup and recovery, robustez, entre otros. En el caso de la db de la API de Historia Clínica, contaremos con un servicio llamado AWS Directory Service, donde podremos almacenar información sobre nuestros pacientes en directorios.

Redes

La comunicación entrante con nuestros servicios en la nube pasarán por routers ISP, estos son provistos por un Proveedor de Servicios de Internet de fibra óptica. El modelo de distribución interna que se va a utilizar es la Traditional 3-Tier en el que vamos a tener Routers Core que se van a conectar a equipos de acceso para después conectarse con las terminales.

Para mantener la seguridad de nuestra red local, utilizaremos un Firewall. En el cuál también podemos integrarle un antivirus. De esta manera podemos filtrar las comunicaciones que entran y salen de nuestro sistema de acuerdo a ciertos criterios que van cambiando con el tiempo para mantenerse actualizados frente a ataques que están también en una evolución constante.

Todas nuestras instancias EC2 contarán con un firewall para especificar los protocolos, los puertos y los rangos de direcciones IP que pueden alcanzar nuestras instancias mediante el uso de grupos de seguridad.

Auditoría

Aspectos a consultar y evaluar en la visita

El objetivo consiste en constatar a dicha fecha, lo siguiente:

- Corroborar que las cifras presentadas en los estados contables sean razonables.
- Determinar si este sistema produce resultados, es decir, planes, presupuestos, pronósticos, estados financieros, informes de control dignos de confianza, adecuados y suficientemente inteligibles por el usuario que lo revise.
- Informar precisa y oportunamente los desvíos producidos y aconsejar las medidas de acción correctivas necesarias.
- Análisis de red y cifrados
- Análisis de comunicaciones.
- Análisis de Hardware
- Análisis de Software
- Análisis de vulnerabilidades
- Comprobar y promover la eficiencia de los distintos procesos operativos.

Para llevar a cabo el cumplimiento de esta auditoría se recolectará la siguiente información:

- Estructura organizativa vigente en el período objeto de evaluación, indicando las personas que trabajaron en el proyecto a auditar.

- Documentos contables originales de las operaciones del proyecto: Recibos de Caja, Consignaciones, Egresos, Facturas y Notas Contables.
- Informes del proyecto, técnico y financiero, correspondiente al período a auditar.
- Carpetas de cada una de las personas que se encontraban vinculadas al proyecto, ya sea por contrato de trabajo o por prestación de servicios.
- Copia de los pagos por seguridad social de las personas vinculadas al proyecto.
- Relación de las cuentas por cobrar y las cuentas por pagar del proyecto, vigentes al corte del período a auditar, indicando fecha de la operación y el concepto.
- Libro Mayor y Balances y Caja Diario, debidamente registrados y foliados.
- Evidencias de la materialización de las sugerencias derivadas de la auditoría al período anterior.

Una vez recolectada toda esta información, se llevarán a cabo los siguientes procedimientos:

- Comparación de estados contables con registros, implica comparar las cifras de los estados contables con los saldos que arrojan los mayores, submayores y subdiarios.
- Entrevistas sobre actividades y procedimientos a diferentes miembros del equipo para de esta manera ampliar la información ya obtenida.
- Examen de documentos importantes
- Análisis de razonabilidad, este procedimiento tiende a brindar evidencia sobre la existencia de cosas no tangibles y de activos físicos en poder de terceros.
- Observación de actividades, este procedimiento nos proporcionará evidencias acerca del funcionamiento del sistema, evidencia de que los controles que no dejan constancia documentada de aplicación o existencia, estén en vigencia y evidencia de que los otros controles operan en la forma manifestada.

Falencias o fallas de seguridad consideradas

Las fallas de seguridad o falencias que puede tener la Institución son las siguientes:

- **Autenticación:** Si bien el Login de los usuarios del sistema cuenta con algunas validaciones para identificarse, hay otros ataques que podrían corromper el sistema, por ejemplo un ataque de SQL Injection o de fuerza bruta.
- **Wifi:** Los usuarios del módulo de Telemedicina se tienen que conectar mediante la red para ejecutar sus operaciones, esto puede ser peligroso porque la misma puede ser interceptada por personal ajeno a la Institución para conectarse a la red o interceptar transferencia de datos. Si un usuario no

cuenta con ciertas prácticas esenciales para la seguridad de su red, prácticamente está invitando a entidades maliciosas a atacar el sistema.

- **Predisposición al phishing:** En esta época de teletrabajo muchos de los usuarios quedan expuestos a ataques de phishing, ya sea desde los correos corporativos para los médicos y administrativos y desde los correos personales en el caso de los pacientes.
- **Uso de software pirata:** Si los usuarios utilizan este tipo de softwares en sus computadoras, pueden ser víctimas de troyanos y virus y dado que el software carece de respaldo porque es pirata, el usuario es privado de soporte técnico quedando a expensas del ataque sin ayuda.
- **Errores de configuración:** Este cambio en la arquitectura con servicios en la nube, si el personal encargado de implantar las políticas de seguridad no conoce el entorno, las políticas estarán mal configuradas y no serán seguras ni eficaces.
- **Desconocimiento de la localización de los datos:** Se pone en riesgo la seguridad de los datos guardados en la nube al desconocer la legalización de otros países.
- **Viabilidad a largo plazo:** Existe el riesgo de que las condiciones del contrato sufran alguna modificación y debido a esto tengamos que salir a realizar los cambios correspondientes con la posibilidad de que nos afecte negativamente según sea el caso.

Auditoría Interna

INFORME DE AUDITORÍA	
FECHA INFORME: 12/10/2020	SISTEMA AUDITADO: Sistema de gestión de sanatorios de Trisalud
AUDITOR LIDER:	Duración: 20hs
TIPO DE AUDITORIA: Interna	FECHA DE AUDITORÍA: 27,28,29 y 30 de septiembre

OBJETIVO DE LA AUDITORÍA
<p>Evaluar los nuevos riesgos potenciales del Sistema de gestión de sanatorios de Trisalud luego de la actualización del sistema que se realizó debido a la pandemia, teniendo en cuenta los requisitos de seguridad anteriormente establecidos en los procesos que hacen parte del sistema.</p>
ALCANCE DE LA AUDITORÍA
<p>Controlar los accesos no autorizados al software, así también como el cuidado y mantenimiento del hardware. Manejar el acceso de la red de tal manera que se utilice solo para uso de trabajo.</p>
CRITERIOS DE AUDITORÍA
<ul style="list-style-type: none"> - Normas de calidad de la información ISO 9001:2015 - Requisitos legales aplicables - Documentación interna de los procesos - Ley 1845 - Protección de Datos Personales
HALLAZGOS DE LA AUDITORÍA
<ul style="list-style-type: none"> - Cambios en la gestión - Control de la seguridad a la red corporativa - Ingreso de malware a la red corporativa - Ataques a contraseñas - Riesgo de acceso privilegiado

Informe de las debilidades detectadas		
Situación actual	Recomendaciones/Control	Nivel de Riesgo
Solo se cuenta con personal en el área IT que solo cumplen el rol de gestores de infraestructura	Contratar empleados con certificación en AWS o realizar un reskilling de los empleados en esa área.	Alto
El empleado ya no se conecta desde la oficina donde tenían las barreras de seguridad ahora lo hace por su propia cuenta y con sus propios dispositivos, controlar estos accesos se convierte en un serio desafío ya que la VPN utiliza un proceso de autenticación de una sola vez y asume que todo está bien si el usuario está dentro de la red.	Evaluar el cambio de un nuevo modelo de seguridad para disminuir los posibles ataques a la red interna. Se debe contemplar el modelo de seguridad de Zero Trust Network Access	Medio
La gran parte de los ataques se producen por una combinación de vulnerabilidades en el área de HW, SW y usuario, pero principalmente, debido al error humano.	Actualización de SW, antivirus, antispyware y antimalware.. Como el error es predominantemente humano, el control se debe hacer manteniendo constantemente informado a los usuarios de medidas de seguridad pertinentes.	Alto

<p>Las contraseñas se encuentran encriptadas pero no fueron encriptadas con una criptografía recomendada para contraseñas.</p>	<p>Utilizar buenas prácticas para el resguardo de contraseñas ante ataques (ataques de diccionario o fuerza bruta), por ejemplo normas para la actualización o vencimiento de contraseñas, bloqueo de cuentas, delay incremental, captchas, utilización de criptografía confiable como hash con salt</p>	<p>Alto</p>
<p>Estas cuentas tienen acceso a los datos más confidenciales y los sistemas críticos de la organización. Pueden generar problemas por el mal uso del acceso privilegiado, aumento de los ciberataques, derecho a eludir los controles de seguridad establecidos y uso de acceso privilegiado en cuentas de aplicaciones / servicios.</p>	<p>Gestión de Accesos Privilegiados o PAM puede controlar, supervisar, proteger y auditar todas las identidades y actividades con privilegios humanos y no humanas en todo el entorno informático de la empresa.</p>	<p>Medio</p>

Conclusión: Se presentan faltas graves de seguridad al acceso de información sensible.