**TRABAJO PRÁCTICO INTEGRADOR ADR 2021**

**Grupo 4**

**Entrega 3.0**

**Docente**: Rubén Sualdea

**Ayudante**: Cynthia Laura Skrzypek

**Curso**: K4052

**Integrantes**:

| Apellido, Nombre | Legajo |
| --- | --- |
| Dumont, Francisco | 159.030-3 |
| Guida, Diego | 146.616-1 |
| Oviedo, Facundo | 167.857-7 |
| Pardo, Matías | 153.872-0 |
| Valentín Víctor | 147.079-6 |

**Fecha de entrega**: 06/10/2021

**Historial**

| Fecha | Versión | Descripción | Autor |
| --- | --- | --- | --- |
| 26/05/2021 | 1.0 | Primera entrega del trabajo práctico | Grupo 4 |
| 21/07/2021 | 1.1 | Primera reentrega del trabajo práctico con correcciones | Grupo 4 |
| 25/08/2021 | 2.0 | Segunda Entrega del trabajo práctico | Grupo 4 |
| 06/10/2021 | 3.0 | Tercer entrega del trabajo práctico | Grupo 4 |
| 10/10/2021 | 3.1 | Primera reentrega de la segunda entrega | Grupo 4 |

**Tabla de contenidos**

[**Introducción**](#_heading=h.jz4mk9e8silj) **4**

[**Listado de requerimientos**](#_heading=h.ppcqlbmz03rb) **5**

[**EDT (Estructura de desglose de trabajo)**](#_heading=h.mv3jzhweq6yn) **7**

**R**[**iesgos**](#_heading=h.iz7kkxmzphns) **11**

[**D**](#_heading=h.14rqiyeh74he)**iagramas 14**

[**Arquitectura HW**](#_heading=h.q7kmdehgavrt) **14**

[**Virtualización**](#_heading=h.4jombqy0g3kp) **16**

[**Arquitectura SW**](#_heading=h.qul2dxj738qj) **16**

[**Módulos**](#_heading=h.mt9ph0tugd0i) **17**

[**Interacción de los módulos**](#_heading=h.p2hv03lt0ltf) **18**

[**Consideraciones y Cambios**](#_heading=h.y62j84sirlw6) **19**

**A**[**spectos a consultar y evaluar en la visita.**](#_heading=h.gmf19zr5k7rf) **20**

**F**[**alencias o fallas en seguridad que puede tener la Institución**](#_heading=h.6zjpc69l62ls) **22**

**R**[**iesgos identificados por los cambios recientes**](#_heading=h.pohk3gqujmw3) **23**

**C**[**ontroles o recomendaciones para cada riesgo**](#_heading=h.t96tl8nthcd2) **24**

Entrega 1

# Introducción

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

La red de Sanatorios Trisalud cuenta con tres sucursales. La principal, de alta complejidad, ubicada en la CABA y dos de media complejidad, una ubicada en zona sur de la provincia de Buenos Aires y otra en zona norte. Las tres instituciones cuentan con internación y atención ambulatoria tanto para pediatría como adultos y centros de vacunación.

La empresa requiere que el 80% de su personal pueda realizar trabajo remoto desde sus hogares y que a las sucursales asista el mínimo personal necesario para admisión de pacientes, personal de guardia y 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 ges ona 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).

Actualmente la institución cuenta con un datacenter principal y equipamiento en cada sucursal. El sistema cuenta con una arquitectura multi capa, es modular en su funcionalidad, implementada en una arquitectura monolítica. Utiliza como persistencia de datos una única base de datos relacional. El acceso a la aplicación se realiza mediante cliente liviano (navegador) y las reglas de negocio se ejecutan en los servidores.

La institución cuenta con vacunatorios en sus 3 sucursales, los ministerios de salud de CABA y provincia de Buenos Aires determinaron que en los mismos se vacunará a pacientes con la vacuna contra covid. Cada ministerio publicará mediante un servicio cuáles son los pacientes que deben vacunarse en un determinado período. Trisalud, deberá obtener información de los pacientes, realizar una planificación para la vacunación, asignar turnos a los pacientes y notificarlos del mismo. Una vez aplicada la vacuna, deberá informar a los ministerios DNI, Fecha, Tipo/Marca de vacuna y Número de Lote.

Los ministerios de salud cuentan con servicios de auditores informáticos externos para verificar los cumplimientos de seguridad en las instituciones de salud.

El objetivo de este documento es listar y detallar los requerimientos necesarios para permitir que los empleados puedan trabajar desde sus hogares teniendo en cuenta las características de implementación definidas, presentar una planificación para llevar a cabo el trabajo necesario y un plazo estimativo para su implementación. También serán planteados los cinco riesgos más relevantes asociados a los nuevos cambios, un plan de mitigación para cada uno y un plan de contingencia para los tres riesgos de mayor severidad. Así como detallar las modificaciones necesarias a la arquitectura de hardware y software necesarias para desarrollar la solución.

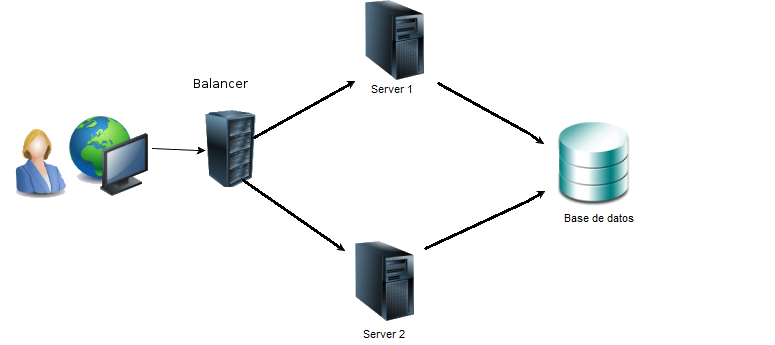
# Listar y detallar los requerimientos funcionales y no funcionales necesarios para permitir que los empleados puedan trabajar desde sus hogares teniendo en cuenta las siguientes características actuales de implementación:

Los empleados se van a conectar por VPN, con usuario y contraseña. El Hospital ya cuenta con un ABM de usuarios para crear los usuarios de los empleados del hospital.

Requerimientos Funcionales:

* Adquisición de notebooks para el personal.
* Instalar los sistemas necesarios para que la computadora se pueda utilizar. Sistema   
  operativo, plugins necesarios para las aplicaciones Web Service.
* Gestionar los usuarios nuevos para los empleados que no poseían acceso a la VPN
* Desarrollar un nuevo módulo de telemedicina permitiendo un contacto a través de videollamada entre el médico y el paciente.
* Desarrollar un módulo que permita almacenar y gestionar la historia clínica del paciente.
* Implementar recetas digitales.
* Relacionar los módulos existentes con el nuevo módulo de telemedicina de forma tal que puedan interoperar entre ellos.
* Implementar sesiones de logeo para el nuevo módulo de telemedicina.
* Para los agentes externos a la organización, como lo son los pacientes, crear un ABM para sus usuarios.
* El módulo de telemedicina deberá contar con un mecanismo de cola de turnos, donde los usuarios no pierdan su puesto en la cola debido a problemas de conexión.

Requerimientos No Funcionales:

* **Capacitación**: Realizar instructivos para que los empleados se puedan conectar de forma remota.
* **Características del hardware para empleados:**
  + Computadoras con los siguientes **requerimientos mínimos**: procesador Intel i3 1115G4E, 8 GB de RAM DDR4, SSD de 240GB.
  + Un headset para cada empleado.
* **Cantidad**: Las computadoras a adquirir deben ser al menos 800. (De los 1000 empleados, 80% van a hacer home office)
* **Usabilidad:** El módulo de telemedicina debe tener una interfaz amigable para que la puedan utilizar personas de distintas edades sin dificultad. Para que esto pueda ser llevado a cabo de una mejor manera, se pueden hacer tests a los futuros usuarios (sean pacientes o los propios doctores) para poder ajustar el diseño de la UI. El sistema deberá contar con instructivos donde se explique de forma detallada y con imágenes el correcto uso del sistema.  
  El sistema debe contar con un diseño responsive garantizando la correcta visualización en múltiples dispositivos. Se deberá informar al usuario sobre los errores que surjan durante su operatoria, desplegando mensajes de errores informativos y orientados al usuario final, evitando revelar información destinada a desarrolladores.
* **Disponibilidad:** El módulo de telemedicina debe estar disponible 24/7 ya que se debe poder responder a la demanda covid que exista, debido a que el resto de los módulos se interrelacionan con éste, estos también van a tener que funcionar 24/7
* Debido al aumento de carga que va a haber (pues se busca que el sistema esté funcionando 24/7 y el nuevo módulo de telemedicina), se comprará otro servidor Dell poweredge t30 que funcionara como un espejo del servidor de aplicación, sobre este servidor además de estar corriendo los 4 módulos ya conocidos (admisión, facturación, cirugía y farmacia) va a correr el nuevo módulo de telemedicina , con el objetivo de balancear todas las solicitudes en ambos servidores, para ello se instalará un load balancer Linux Virtual Server corriendo sobre una computadora que tenga los siguientes requisitos: Intel I3 10100, 8 GB de RAM DDR4, HDD de 500GB.  
  
* **Aumento de concurrencia en la VPN**: Debido a que el firewall sufrirá más solicitudes concurrentes al tener la sucursal principal trabajando desde casa (estos pasarán a acceder por VPN)
  + Se puede aumentar las características de hardware del servidor presente actualmente, como lo sería un mejor procesador (del mismo socket) y un aumento de memoria RAM
  + Seguridad en los datos de las historias clínicas de los clientes, ya que solo deben ser accedidas por los médicos.
* **Seguridad**:
  + La conexión entre el paciente y el médico debe encontrarse cifrada, para garantizar la confidencialidad de la consulta.
  + El acceso o logeo a la plataforma de telemedicina debe autenticar y garantizar que la persona que ingresa a la plataforma es quien realmente debe ser. Para evitar el ingreso de personas no autorizadas a la videoconsulta.
* El nuevo módulo de telemedicina debe garantizar al menos 100 sesiones de forma concurrente.
* El nuevo módulo de telemedicina debe poder ejecutarse desde cualquier navegador (Google Chrome, Microsoft Edge, Safari, Opera, Firefox), en todas las versiones que tengan menos de 1 año de antigüedad.

# Diseñar la EDT (Estructura de desglose de trabajo) para el desarrollo del nuevo módulo de Telemedicina. Presente una planificación para llevar a cabo el trabajo necesario e indique en qué plazo podría implementarse (indicar los perfiles y la cantidad de recursos necesarios para realizarlo)

* 1. [**Antecedentes o Situación Actual**](#_heading=h.1fob9te)

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

Las tres instituciones cuentan con internación y atención ambulatoria tanto para pediatría como adultos y centros de vacunación.

Se cuenta con los servidores ubicados en 1 de las 3 sucursales y también existe un Firewall con VPN para el acceso a los servidores. Salvo la sucursal principal que es la única que está accediendo directamente (sin VPN)

* 1. **Justificación del proyecto**

La empresa Sanatorios Trisalud requiere que el 80% de su personal pueda realizar trabajo remoto desde sus hogares y que a las sucursales asista el mínimo personal necesario para admisión de pacientes, personal de guardia y de internación y el mínimo personal de IT para dar soporte a los usuarios que no pueda brindarse en forma remota.

* 1. [**Determinación del Alcance**](#_heading=h.2et92p0)
     1. **Objetivos del Proyecto**

El primer objetivo de este proyecto es montar una plataforma para que los doctores de la institución puedan hacer videollamadas, la misma debe poder soportar un registro de atenciones que se lleven a cabo. Debe poder conectarse con el módulo de admisión para obtener los datos del paciente, y tener un cliente para que el usuario se registre y conecte.

También deberá conectarse con el módulo de farmacia y facturación para poder permitir hacer algunas funciones relevantes para la mejora de procesos automáticos.

El paciente podrá registrarse en una página validando estos datos con los del sistema de admisión, para posteriormente ingresar con un usuario para realizar la tele-consulta

* + 1. **Alcance del Proyecto**

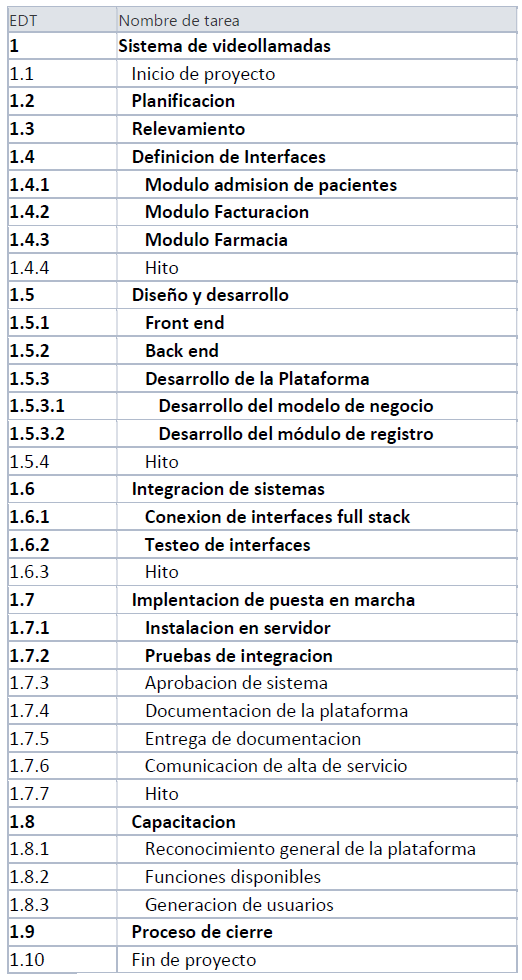
El sistema a realizar deberá estar disponible para los empleados que requieran y que pertenezcan a cualquiera de las 3 sucursales.   
También podrá contemplar la conexión para los pacientes sin importar su ubicación.

* 1. **Estructura de desglose de trabajo (EDT)**

EDT haciendo [click aquí](https://drive.google.com/file/d/1ej05MugX9r3nxVH_YIBZovTUGY_oarE_/view?usp=sharing)

Diagrama de Gantt hecho en MS Project haciendo [click aqui](https://drive.google.com/file/d/1CRZljizTMyr507-FgtmMu5YV1Nh1HMcJ/view?usp=sharing)

Gantt resumido:



* 1. **Recursos del proyecto:**
     1. **Consideraciones**

Todos los empleados están disponibles 5 días de la semana durante 8 hs.

Además de los recursos detallados se va a necesitar realizar entrevistas con:

* Un usuario funcional de la clínica que utilice los módulos actuales
* El administrador de servidores para que nos brinde acceso a los servidores.
* Un jefe de informática para ir informando las actividades y el estado del proyecto, el mismo será el interlocutor principal entre la clínica y “nosotros”
* Un responsable legal para aprobar los procesos y los protocolos a implementar
  + 1. **Recursos:**
* 1 Project Manager
* 1 Desarrollador Front end
* 1 Desarrollador Back end
* 1 Desarrollador full stack
* 1 Tester
* 1 Administrador de servidores
* 1 Administrador de base de datos
* 1 Jefe de Desarrollo

* 1. **Estrategia de solución**
     1. Comenzaremos la realización del proyecto con la etapa de planificación para realizar el armado de los equipos de trabajos, metodologías a utilizar, estimar costos y definir los riesgos a alcanzar.
     2. Terminada la etapa de planificación, comenzaremos con el relevamiento, basado principalmente en entrevistas, lo cual nos dará una una idea de cuáles son las necesidades específicas de los empleados para la aplicación.
     3. A partir de los resultados obtenidos, el equipo va a definir de qué manera se va a conectar el nuevo módulo con los otros sistemas del hospital, es decir, qué información va a requerir, cómo ser consistente con ella y cómo se la va a utilizar.
     4. Definidas las interfaces de conexión, se arranca el diseño y desarrollo de la plataforma, integrando el back-end con el front-end y junto a ello, la conexión de ambas partes, con un constante testeo en la medida que se avanza con cada parte.
     5. Finalizado el desarrollo de los módulos, se realizará la implementación en servidor, donde se harán todas las pruebas necesarias para asegurarse de que todo está listo para ser puesto en marcha.
     6. Tras ello, se hará un proceso de cierre donde se harán encuestas y se las analiza para detectar puntos de mejora en el proyecto. Con los datos obtenidos se generará la documentación de cierre y se adjuntará a la misma los instructivos de la aplicación.

# Describa los 5 riesgos más relevantes asociados a los nuevos cambios a implementar y plantee un plan de mitigación para cada uno de ellos. Además para los 3 riesgos de mayor severidad elabore un plan de contingencia.

1. **Quedarse sin conexión de Internet en la sucursal donde se encuentran físicamente los servidores**.***Probabilidad: 6 - Impacto: 8***

Ya que el 80% de los empleados se van a conectar desde sus casas a los servicios ubicados en la sucursal principal, deberíamos tener en cuenta que la conexión de internet es un punto único de fallo por lo tanto definimos lo siguiente:

* 1. Plan de mitigación: Medir los microcortes que tenga el isp actual y en base a eso contratar un segundo ISP para tener redundancia. En el firewall se configura este segundo ISP y queda conectado y preparado para que en el caso de un corte del del servicio de internet de manera automática el tráfico salga por este segundo ISP, logrando así que nadie se entere que hubo un fallo en el servicio.
  2. Plan de contingencia: En caso de quedarse sin internet se deberá reprogramar todas las citas afectadas para las videollamadas en el horario sin servicio o tiempo que lleve la restauración del servicio. La reprogramación de las citas se llevará posteriormente al restablecimiento del servicio, el personal encargado de dar turnos deberá comunicarse con las personas que tenían un cita y concretar un nuevo día y horario para el turno.

1. **Un corte de electricidad en el Data Center.**

Nuestros servidores están conectados a la electricidad de la institución, en caso de haber un corte de luz, nos veríamos afectados para poder seguir brindando continuidad en nuestros servicios. ***Probabilidad: 7 - Impacto: 8***

* 1. Plan de mitigación: Implementar un sistema distribuido en las demás sucursales, instalando un un Data Center mínimo para poder soportar los servicios que se ejecutan en los servidores actuales, brindando un esquema de espejo, pero con data center con menos redundancia. Utilizando el ISP de las sucursales e instalando un servidor con requerimientos mínimos para todos los módulos, en una habitación con piso técnico, aire acondicionado, control de acceso y seguridad física.
  2. Plan de contingencia: Contamos con una UPS que podrá soportar hasta 20 min de autonomía brindando continuidad en nuestros servicios, en paralelo se activa el grupo electrógeno, y tardando menos de 1 min en prenderse, se realiza el cambio a este suministro para no seguir utilizando la UPS y en caso de que el corte dure varias horas el grupo podrá soportar esta demanda.Logrando de esta forma que el servicio siga funcionando.

1. **Filtrado de información sensible de los servidores**. ***Probabilidad: 2 - Impacto: 4***

Si bien estamos contemplando varios métodos de seguridad para nuestros servidores, todo sistema que tenga internet o algún tipo de conexión es hackeable.

* 1. Plan de mitigación: Realizar un cambio de contraseña mensual obligatorio, y brindando robustez indicando que deben tener caracteres especiales, números, mayúsculas, no pueden repetirse a las últimas 12 generadas, no puede ser una palabra conocida. Realizar la deshabilitación de los puertos que no se utilicen.
  2. Plan de contingencia: Realizar un cambio de contraseña para los usuarios con privilegios de admin y de forma masiva también para los usuarios. Realizar un análisis en la red para identificar los posibles dispositivos que realizaron el ataque y bloquearlos, identificar el origen de las fallas de seguridad que tuvimos y reforzar las con nuevas medidas de seguridad, en caso de existir un comité de seguridad informática, ejecutar las medidas que se planificaron.

1. **Rotura o problema con un disco de los servidores**. ***Probabilidad: 4 - Impacto: 9***

Nuestros servidores cuentan con un sistema operativo (basado en linux) montado en 1 disco. En caso de una falla se verían afectados los servicios que este posee, planificamos las siguientes soluciones:

* 1. Plan de mitigación: Implementar un sistema RAID 1 con 2 discos. Se utilizará el software de RAID que tienen los servidores para realizar la configuración de espejo con 2 discos.

1. **Falta de almacenamiento para la base de datos**. ***Probabilidad: 7 - Impacto: 7***

A día de hoy se tiene libres 500GB en la base de datos, debido a que se ve probable que la cantidad de espacio de almacenamiento por día que se use sea mayor debido a la información nueva que va a usar el módulo de telemedicina y que eventualmente el espacio se acabe, se deberá evitar esto

* 1. Plan de mitigación: Comprar discos adicionales para aumentar el espacio de almacenamiento o usar almacenamiento en la nube.

Entrega 2

1. **Presente las modificaciones necesarias a la arquitectura de HW y/o SW que considere necesarias para desarrollar e implementar la solución (presentar esquema implementación y explicación del mismo)**

# DIAGRAMAS

* + 1. [**Diagrama Software**](https://drive.google.com/file/d/13RMOfF-xxayPisg0aXAdVxZmng-6j15l/view?usp=sharing)
    2. [**Diagrama Hardware**](https://drive.google.com/file/d/1eRCIfhlkhcWUIchIedIST5Lr-lDTV-8e/view?usp=sharing)
    3. [**Diagrama de Virtualización**](https://drive.google.com/file/d/1vGAUmPTqH2kJSTSikAsahYgjz_R0wSTZ/view?usp=sharing)

# **INTRODUCCIÓN**

Planteamos cambiar nuestra solución inicial, para tener una arquitectura que permita una factibilidad más escalable y más tolerante a fallas con las ventajas que trae la virtualización.

Los 2 servidores de aplicaciones se virtualizarán instalando un cliente de virtualización, los mismos serán etiquetados a partir de ahora como **ISCX1** y **ISCX2** (VMware o similar) con clientes web y un Hipervisor para la administración, en el mismo se instalará un software de sincronización para brindar disponibilidad ante algún fallo de aplicación o de hw se instalará 1 SO en cada servidor (**ISCX**) sincronizados y así redireccionar a los usuarios a la instancia que está funcionando.

El tercer y cuarto servidor, de base de datos, también serán virtualizado y correrán el servicio de la base de datos etiquetado a partir de ahora como **ISCX3** e **ISCX4**, en los mismos se montaran 2 instancias de la base de datos respectivamente, para que ante la falla de 1 se redireccione la carga al otro (arquitectura master-slave), logrando una redundancia en instancias para que ante la falla de la base de datos o por algún error de aplicación sigue respondiendo consultas.

Se virtualiza el Load Balancer que actualmente lo tenemos en una PC, para brindar una mejor solución que contemple fallos de HW o SW, el mismo se instala en 2 instancias entre los **ISCX**, así podremos administrarlo con la virtualización y el software de sincronización y ante ese posible error, poder seguir distribuyendo la concurrencia entre las instancias funcionales del hospital.

# Arquitectura HW

**INTRODUCCIÓN**

Los 2 Servidores de Aplicaciones (ISCX 's) estarán conectados por medio de una patchera interack al switch principal, el cual también se encuentra conectado el firewall.

Al mismo switch estarán conectado el servidor Firewall y el de base de datos

* + 1. **Sucursales**  
       Las sucursales 1 y 2 estarán equipadas con 2 ISP para poder funcionar de manera constante y sin preocuparse de las caídas de un ISP, se conectarán a los servicios de la sucursal principal vía un VPN y con un browser con cliente liviano, ejecutando todas las reglas de negocio del lado del servidor en la sucursal principal..
    2. **Sucursal Principal**  
       La misma tendrá un Data Center con los 3 servidores que cuentan con virtualización, un load balancer y el firewall conectados al único switch (todo esto detallado en la sección de virtualización).
    3. **Base de datos**

La base de datos se encuentra virtualizada en un cluster de alta disponibilidad, dentro de este cluster, va a estar utilizando una solución SAN para la configuración de los discos (ISCX3 y ISCX4), proporcionando un alto throughput y una baja latencia, que será necesario debido a la alta tasa de querys que se requerirán con la virtualidad y el nuevo módulo de telemedicina. Se usará el protocolo Fibre Channel Protocol (FCP)

* + 1. **FIREWALL**Nuestros proveedores de ISP 's van a estar conectados directamente con el firewall y ahí se administra la redundancia de internet, que la misma se conecta por un cableado de red hasta el switch, el cual se conectará con el resto de los componentes.  
       El mismo también tendrá configurado una VPN para que los clientes que requieran conectarse a sus máquinas personales de la institución lo puedan hacer.
    2. **Nube: servidor de Telemedicina**Se realizará la utilización de la Nube con un servicio de tipo PaaS de Amazon Web Services. Aquí, se correrá nuestro módulo de telemedicina desarrollado para la pandemia, el motivo de usar la nube es que debido al posible aumento desmedido de demanda de este módulo, se tendrá la posibilidad de hacer escalar nuestro hardware de manera sencilla y contemplar así posible demanda espontánea que se puede disparar muy fácil por la situación de contagios y el desconocimiento de la enfermedad. Cosa que sería más difícil de poder llevar a cabo en una arquitectura on premise.
    3. **Médico homeoffice**

Los médicos que hacen uso de la nueva aplicación web de telemedicina se conectan desde su casa vía HTTPS al módulo que se encuentra en la nube.

* + 1. **Empleado homeoffice**

El empleado que hará su trabajo desde su casa, se conectará vía VPN a los servidores de aplicación que contienen los diferentes módulos para poder operarlos.

* + 1. **Servicio de vacunación externo**

Este servicio está corriendo sobre un servidor propio del ministerio, el cual se desconocen los detalles

* + 1. **Paciente de vacunación**

A este paciente, el módulo de vacunación le enviará un email y un mensaje vía whatsapp informando su turno para vacunarse. Lo cual se definirá a partir de la información que dé el servicio de vacunación externo de los ministerios.

# Virtualización

* + 1. **Configuración de la virtualización**En el ISCX1 se instalará 1 Instancias para los módulos del hospital y otra para el Load Balancer.  
       Paralelamente en el ISCX2 se instalará otra instancia para los mismos servicios del hospital y otro Load Balancer.  
       En el ISCX3 se instalarán 1 Instancias de la base de datos configuradas también con el software de sincronización. Se usará la replicación que ya viene incluida en la base de datos de Oracle para poder sincronizar ambas bases de datos.  
       Análogamente en el ISCX4 se configura otra instancia de la base de datos.
    2. **Administración Virtualización**  
       En el Hypervisor se configuran las 2 instancias para los módulos del hospital sincronizados entre el ISCX1 y el ISCX2; Otras 2 instancias para la base de datos, entre el ISCX3 y el ISCX4.  
       Las instancias de los módulos del hospital están configuradas por el software de sincronización. De esta forma tendría un nodo para los sistemas del hospital y otro nodo para la DB, consiguiendo algo similar pero en menor escala a un cluster de HA gracias a un software de sincronización que ante una falla en la aplicación o en el sistema operativo puede redireccionar.  
       Lo mismo sucede para las instancias de base de datos pero sincronizadas por la misma base de Oracle.
    3. **Detalles de implementación**  
       Los Sistemas Operativos de los módulos del Hospital tendrán 24GB RAM, 3 núcleos y 500 GB de espacio en disco. (1 Sistema Operativo por Servidor)

El Sistema Operativo de los Load Balancer tendrá 8GB RAM, 1 núcleo y 100GB de espacio en disco. (1 Sistema Operativo por Servidor)

# **Arquitectura SW**

* + 1. **Load Balancer**El load balancer estará conectado como servicio de escucha para los módulos de Farmacia, Facturación, Admisión, Cirugía, Historia Clínica, Receta Digital, Vacunación; los cuales estarán corriendo en 2 instancias en paralelo con una única Base de Datos  
       Se van a instalar 2 instancias de load balancer en la virtualización para generar redundancia ante la falla de uno y poder seguir repartiendo la concurrencia y con el software de sincronización se podrá detectar esa falla y así seguir brindando la distribución de la concurrencia con la instancia funcionando.
    2. **Base de datos**La misma estará virtualizada en 2 instancias en paralelo sincronizadas para que ante una falla siga brindando el servicio de base de datos. La misma es de tipo Relacional Oracle. Al estar la base de datos original en MySQL, se hará una migración con el software SQL Developer.
    3. **Oracle Database Backup Cloud Service**

Para realizar una copia de seguridad utilizaremos Oracle Cloud Infrastructure Classic, el software para el backup es Oracle Database Cloud Backup Module para OCI Classic. Quedará configurado en la misma instancia de la base de datos la cual se encargará de realizar el backup.

El módulo de Oracle Database realizará un backup incremental. Es un servicio provisto por Oracle configurado en las mismas instancias de la base de datos que permite guardar el backup en la nube de Oracle. Este proceso se configura para ejecutarse todos los días de la semana a las 03:00.

**Backup incremental**

Los días domingo se realizará un backup completo y en los días de la semana solo se realizará un backup de la información que se haya actualizado o agregado.

# Módulos

* + - 1. **Módulo de Facturación**

Los empleados podrán conectarse a este módulo para cargar la prestación realizada para la posterior presentación a las obras sociales o para el cobro a particulares.  
Se conectará con AFIP vía HTTPS para realizar la facturación electrónica

* + - 1. **Módulo de Cirugía**

Los empleados se conectarán al módulo para gestionar el uso de quirófanos y de instrumentación.

* + - 1. **Módulo de Admisión**

Se encarga de recepcionar pacientes ambulatorios y admitir los pacientes para la internación.

* + - 1. **Módulo de Farmacia**

Se registra la compra y consumo de medicación e insumos.

* + - 1. **Módulo Historia Clínica**

Módulo que permite gestionar, cargar y consultar la historia clínica de los pacientes.

* + - 1. **Módulo Receta Digital**

El módulo se encarga de permitir la implementación de receta digital en las teleconsultas.

* + - 1. **Módulo de Vacunación**

El módulo de vacunación se encarga de consultar la información sobre los pacientes que deben ser vacunados, además de realizar la correspondiente planificación y registro de la información.

# Interacción de los módulos

* + - 1. **Módulo de Vacunación**Se encarga de conectarse vía HTTPS a los servicios API Rest ofrecidos por los ministerios de CABA y Provincia de Buenos Aires, para consultar y enviar la información necesaria.

**Implementación del módulo de Vacunación**Se realiza una planificación para el plan de vacunación, el mismo se le informará a los pacientes vía mail y whatsapp el día y la sucursal a la cual debe asistir. También se le avisará a las sucursales el detalle de la planificación, grabando la nueva información de los pacientes que deben vacunarse en la base de datos.   
El paciente luego de recibir alguna dosis de la vacuna un empleado de Trisalud deberá cargar la información pertinente dentro del mismo módulo para que luego se envíe a los servicios del ministerio.

Un servicio programado todas las noches verificará nuevos pacientes vacunados y envía toda la información vía HTTPS a los servicios del ministerio (API Rest)

* + - 1. **Módulo Telemedicina**

El módulo de Telemedicina se encuentra instalado dentro de una instancia contratada en la nube. El mismo se encarga de ofrecer una aplicación Web Service para utilizar como plataforma al momento de realizar la videoconsulta, además permitiéndole al paciente registrar o cancelar turnos. El módulo se conectará con la Base de Datos para obtener los turnos disponibles y ofrecer al paciente un calendario para elegir el turno deseado. Todos los días el módulo de telemedicina le enviará a los pacientes y a los médicos un recordatorio sobre el turno y el link para conectarse a la videollamada. Al momento de finalizar la consulta, el médico se conectará con el perfil del empleado para cargar la documentación necesaria en la historia clínica del paciente y generar la receta digital en caso de ser necesaria.   
Para garantizar la conexión entre el módulo de telemedicina y los módulos existentes, la sucursal principal cuenta con dos ISP.

# Consideraciones y Cambios

Decidimos virtualizar nuestros servidores para poder tener una administración más fácil, poder lograr algo similar a una clusterización de HA, entendemos que por ahi se requieren más instancias corriendo en paralelo, pero dado nuestro esquema creemos que es redundante y con el software de sincronización podemos redireccionar a los usuarios que estén usando la aplicación que falló a la instancia que no tuvo errores. Algo que también está dentro de nuestro abanico de posibilidades, es que fallen las 2 instancias que están corriendo, de ser así, tendríamos un problema para seguir brindando disponibilidad, este es un riesgo que pensamos asumir.

Una posible opción de software para la virtualización es VMware vSphere Enterprise si bien se necesita una licencia paga también existen otras opciones libres quizás no con el mismo soporte pero también se podría llevar a cabo la solución con Virtual Box o KVM.

Se requiere agregar 16GB RAM DDR3 a cada Servidor de aplicación para poder soportar la solución que estamos llevando a cabo, en principio habrán 2 instancias por servidor, y los recursos que se van requerir de los mismos son los puertos de red, memoria ram y procesamiento, nuestra solución logra dejar el camino abierto para seguir creciendo en caso de una gran demanda por tema COVID, ya que al tener una virtualización de base, en caso de necesitar escalabilidad, al adquirir nuevos servidores, estos se pueden virtualizar y así lograr ampliar nuestra solución.

El código fuente del sistema de telemedicina estará resguardado en un sistema de versiones en la nube, como por ejemplo Git o SVN.

Se procederá a adquirir un servidor más igual o similar al servidor de base de datos actual, que será usado para poder garantizar la alta disponibilidad de la base de datos

Se hará una migración de la base de datos original MySQL a Oracle, esto debería ser considerado en la EDT.

Solución SAN, para poder cumplir con la conexión de Fibre Channel Protocol (FCP) vamos a necesitar adquirir 2 placas de red PCI-e 10 Gb Marca tipo Hewlett Packard de dos puertos (Dual Port) Conectores SFP+ Server.

Entrega 3

1. **Los ministerios de salud cuentan con servicios de auditores informáticos externos para verificar los cumplimientos de seguridad en las instituciones de Salud**

# Desarrolle los aspectos que consultará y evaluará en su visita.

Aspectos y/o puntos a evaluar en nuestra auditoría:

* Evaluación de la seguridad.
  + Deberá haber un especialista en seguridad informática en la organización
  + Se realizará una evaluación de la seguridad de fisica
    - Documentación que indique la seguridad física que poseen los sectores de IT y la sala de servidores. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
    - Consideraciones para Diseño y Construcción de Data Center en base al estándar IEEE-587
  + Se realizará una evaluación de la seguridad de lógica
    - La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.
    - Software de protección contra amenazas
    - Verificar una política de protección contra amenazas, deployada en todas las terminales y servidores.
      * Monitoreo contra amenazas.
      * Actualización de Antivirus
    - Procedimientos para la gestión de usuarios, donde se incluya el cambio de contraseña, frecuencia y complejidad.
    - Políticas de prevención de fraude y de fuga de datos
* Evaluación de los planes de contingencia y mitigación ante la presencia de fallas o incidentes de seguridad.
* Revisión de los sistemas operativos
  + Verificar la existencia de una política de instalación y actualización, tanto para las terminales como para los servidores u otro componente.
  + Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante. Deben revisarse los parámetros variables de las Librerías más importantes de los Sistemas, por si difieren de los valores habituales aconsejados por el fabricante.
* Revisión de los software
  + Revisión de software de terceros
    - Política de instalación y actualización de los software instalados en la organización.
  + Revisión de software propios
    - Control de versiones del código fuente.
    - Trazabilidad de las incidencias que ocasionan las modificaciones en el sistema.
    - Documentación de las versiones.
    - Estudio del soporte lógico de los equipos
      * Es deseable conocer cómo se adquiere, distribuye y usa el soporte lógico del software para localizar posibles vulnerabilidades.
    - Seguimiento y actualización constante
    - Verificar que los sistemas se comporten conforme fueron definidos.
    - La existencia de condiciones y procedimientos de seguridad que protejan los datos de la organización.
    - Manejo adecuado de las excepciones y rechazos.
* Revisión de los siguientes aspectos para Cloud computing
  + Configuración independiente
    - Las áreas de tecnología configuran sus propios entornos tecnológicos a través de la nube y evitan los protocolos y controles de TI de la organización, pueden presentarse riesgos no abordados o sin mitigación.
  + Afectación de datos sensibles
    - La pérdida, robo o corrupción de datos sensibles puede causar daños reputacionales graves y posibles procesos penales o acciones civiles, lo que se constituye en un gran riesgo operativo.
  + Acceso inapropiado de usuarios
    - Puede presentarse el riesgo de que los proveedores de los servicios en la nube no restrinjan adecuadamente el acceso a los datos, con las consecuencias que ello implica.
  + Incumplimiento normativo
    - El riesgo de que la organización sujeta a supervisión regulatoria obtenga no conformidades, glosas y observaciones por parte de las entidades que ejercen supervisión y control. Por ejemplo, incumplimientos en el uso y protección de datos personales
  + Uso inapropiado de los datos personales
  + Evaluación del proveedor
    - También pueden verificar la existencia de políticas de seguridad, resultados de pruebas de vulnerabilidad y penetración y resultados de evaluaciones independientes de su entorno de control.
  + Evaluar la arquitectura implementada
* Métricas de funcionamiento
  + Detalle de las métricas existentes, su utilización y monitoreo.
  + Procedimientos ante la recepción de eventos originados por alertas en el sistema debido a alto consumo de recursos.
  + Cambios realizados para mejorar la eficiencia de los sistemas.
* Administración de Base de Datos
  + Política de instalación y actualización del software instalado en la base de datos.
  + Procedimientos para la realización de backups y recuperación de la información.
  + Documentación del esquema utilizado y los campos a guardar en la base de datos.
  + Encontrar evidencia de campos de auditoría en las principales tablas.
  + Consistencia, integridad y no redundancia en los datos de la base de datos.
* Entorno organizacional
  + Organigrama de la organización.
  + Examen de organigrama del departamento de informática e identificación de las grandes unidades organizativas
  + Revisión de la documentación existente para conocer la descripción de las funciones y responsabilidades
  + Realización de entrevistas a los directores de cada una de las áreas para determinar su conocimiento de la responsabilidades y que éstas respondan a las descripciones existentes en la documentación correspondiente.
* Flujos de Información
  + Organizacional y datos lógicos
* Inventario de Hardware y Software
  + Comprobar el correcto registro, flujo y valuación de los inventarios
  + Comprobar la correcta aplicación de los métodos y técnicas de administración de inventarios definidas por la compañía
  + Se necesita conocer todos los programas informáticos con los que cuenta la empresa.

# Conociendo el contexto y los desarrollos realizados anteriormente, ¿Qué falencias o fallas en seguridad considera que puede tener la Institución?

* Se encuentra que muchos riesgos principalmente respecto a incidentes de seguridad no están analizados. Por ejemplo, ante un acceso no autorizado. También encontramos una deficiencia en los planes de contingencia y mitigación de los riesgos ya analizados.
* Ausencia de un controlador de dominio para llevar a cabo la administración de las políticas de Windows en las PCs de usuario, como las actualizaciones de Windows y el login para tener los usuarios de windows centralizados y no de manera local en la computadora del usuario así como para cambiar las contraseñas personales cada un determinado tiempo.
* Ausencia de una administración integral para y hacia las posibles amenazas informáticas.
  + No hay un sistema de actualizaciones centralizado, lo cual puede llevar a que existan máquinas que no tengan las últimas actualizaciones de los antivirus y de los sistemas operativos.
* La sala técnica no tiene alarma contra temperatura, ante alguna falla en el sistema de refrigeración debería saltar una alarma contra temperatura para poder activar un plan de mitigación y así no sufrir consecuencias severas.
* No hay un control de acceso centralizado a la sala de servidores (algún tipo de control biométrico). Actualmente se utiliza un acceso con una llave, pero para garantizar un correcto acceso se debe ser un sistema que permita monitorear y controlar que personal puede ingresar.
* Falta de fuentes verificables de evidencia de auditoría, que son necesarias para probar los controles o para realizar procedimientos de pruebas de sustanciación. Por lo que puede haber evidencia adulterada, archivos de logs corrompidos, documentación modificada.   
  *Razón de diferencia*: En estos casos la organización puede desconocer que la evidencia tenga inconvenientes de seguridad debido a no tener una auditoría interna que lo verifique constantemente.

Si un elemento aparece en esta lista y no en la del punto 5.3, el motivo se aclara con el texto “Razón de diferencia”

# ¿Qué riesgos habría identificado por los cambios recientes?

Los riesgos respecto a la seguridad se encuentran detallados en esta sección

* Ante la falta del controlador de dominio, se genera el riesgo de que se aproveche una vulnerabilidad de seguridad en la computadora de un usuario para robar la clave local sin posibilidad de reiniciar remotamente.
  + Probabilidad de ocurrencia: 10%
  + Impacto: 90%
* Ataques o amenazas informáticas a la organización ante vulnerabilidades de software.
  + Debido a la pandemia, se han multiplicado los ataques informáticos a las empresas. Muchas actualizaciones de Antivirus y de seguridad de Windows, ocurren después de que una vulnerabilidad sea conocida y tal vez explotada, por lo que es muy importante tener las últimas actualizaciones.
  + Probabilidad de ocurrencia: 50%
  + Impacto: 70%
* Daños en el equipamiento ante la falta de una alarma por temperatura.
  + Una falla en el sistema de aire acondicionado podría ocasionar un aumento de temperatura en los servidores y posteriormente el apagado de los mismos.
  + Probabilidad de ocurrencia: 20%
  + Impacto: 90%
* Ingresos indebidos a la sala de servidores
  + La falta de un sistema de control de acceso para la sala de servidores hace que cualquier persona que llegue hasta esa sección del edificio, tenga la posibilidad de entrar allí y tener los servidores a su disposición.
  + Probabilidad de ocurrencia: 5%
  + Impacto: 95%
* Falta de personal responsable por la seguridad informática de la organización, pudiendo causar un fallo de seguridad informática debido a la ausencia de chequeos o de una auditoría interna.
  + Para garantizar un control adecuado de todos los flujos de información existentes entre diferentes áreas y siendo datos personales, se debería contar con un comité de seguridad informática con 1 responsable de cada área.
  + *Razón de diferencia*: Dentro de nuestra organización, consideramos que un especialista en seguridad informática nos daría un sistema mucho más robusto, no obstante esto no es un requisito para una auditoría de seguridad tradicional.
  + Probabilidad de ocurrencia: 5%
  + Impacto: 80%

Al igual que en el punto anterior, si un elemento aparece en esta lista y no en la del punto 5.2, el motivo se aclara con el texto “Razón de diferencia”

# ¿Qué controles o recomendaciones habría elaborado para cada riesgo?

* Instalar un servidor de controlador de dominio, este correrá un sistema Windows Server 2019 y llevará gestión de los usuarios de cada empleado del sistema, esto incluye un sistema para cambios de contraseña cada 6 meses. Este servidor estará on-premise y no será necesaria la alta disponibilidad ni un RTO bajo pues el login puede hacerse sin necesidad de que esté funcionando y las actualizaciones se pueden posponer.
* Poner un sistema de actualización integral.
  1. Para las computadoras de usuario que corran Windows se correrá dentro del servidor de dominio Windows Server Update Services(WSUS) que se asegurará que estas computadoras tengan siempre las últimas actualizaciones de seguridad de Windows.
  2. En el caso de los servidores Linux existen alternativas similares, como FOG Project o Red Hat Satellite, al haber Linux solamente en los servidores y no necesariamente en su misma versión, lo ideal es llevar a cabo las actualizaciones de forma manual
  3. Para el antivirus, se usará el ESET NOD32, para controlarlo se usarán ESET Remote Administrator Server, ESET Remote Administrator Console y ESET NOD32 Antivirus para Windows Server. Esto nos permitirá instalar de forma remota este antivirus a todas las computadoras del dominio y también mantenerlo actualizado.
* Se instalará un sensor de temperatura Sonoff Snzb-02 que se conecta a un sistema de domótica Sonoff Zb Bridge. Este a su vez estará conectado a una alarma y a una aplicación plataforma de domótica Sonoff / eWeLink.
* Se instalará un control de acceso por huella digital “Prosoft modelo 672” para la sala de servidores, conectado a la red con un sistema integral instalado en el área de IT para verificar y monitorear el acceso a la sala técnica.
* Se recomienda contratar un especialista en seguridad informática que garantice la autenticación e identificación del cliente antes de cada video consulta. El mismo debe pertenecer a un comité de seguridad informática conformado por diferentes responsables para asegurar que la planeación, ejecución y desarrollo de proyectos informáticos son acordes a dichas prioridades y necesidades estratégicas.