UNIVERSIDAD GALILEO

FACULTAD DE INGENIERÍA DE SISTEMAS, INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN



**Reporte**

ALEJANDRA RUBIO 1700

FREDY HANÍBAL MARROQUÍN PALENCIA 1700

KEVIN JOSÉ HERNÁNDEZ MARROQUÍN 17001095

INSTALACIONES ESTRUCTURADAS

SEXTO SEMESTRE

GUATEMALA, 18 DE NOVIEMBRE DE 2019

**Índice**

**1. Índice de Figuras** 3

**2.** **Índice de Tablas** 5

**3.** **Introducción** 6

**4.** **Objetivos** 7

**4.1.** Objetivo General 7

**4.2.** Objetivos Específicos 7

**5.** **Estudio de Factibilidad**  8

**5.1.** Investigación Preliminar 9

**6.** **Plan de Trabajo**  25

**6.1.** Restricciones 26

**Introducción**

El Hospital John Hopkins necesita de una estructura de red robusta de tal forma que pueda proveerle conexión a internet y las redes locales a todas las personas que se encuentran dentro del establecimiento.

El objetivo de este documento es informar, especificar y detallar el diseño de la propuesta de red que se presentará a continuación.

**Objetivos**

**Objetivo General**

Proporcionar al Hospital John Hopkins una propuesta de red robusta y eficaz, que cumpla con todos los requerimientos especificados y cumpla las expectativas.

**Objetivos Específicos**

* Investigar y cotizar dispositivos de red, líneas dedicadas de conexión y servicios proporcionados por un ISP.
* Realizar diagramas topológicos físicos y lógicos.
* Diseñar un esquema de direccionamiento considerando crecimiento de la red.
* Investigar y seleccionar los protocolos necesarios para que la red funcione correctamente.
* Investigar y cotizar servidores que sean capaces de soportar mucha concurrencia y paralelismo.
* Investigar y aplicar estándares de red.
* Investigar y cotizar materiales utilizados para el cableado del edificio: tanto la adquisición como la instalación.
* Proporcionar políticas de seguridad.

**Requerimientos**

**Requerimientos Funcionales:**

1. Acceso a la base de datos del CDC en Atlanta Georgia.
2. Cotizar precios de ISP locales de Guatemala.
3. Es necesario un mínimo de 45MB de ancho de banda redundante y dedicado.
4. Proveer a todas las universidades y hospitales del país a la base de datos CDC y a otras bases de datos médicas.
5. Seleccionar qué AWS es el mejor para disponer de un servicio de almacenamiento y acceso a imágenes de alta resolución. Es necesario que el servicio provea una gran cantidad de espacio de almacenamiento y una transferencia rápida.
6. Red inalámbrica robusta para dar acceso a los registros médicos desde cualquier dispositivo (Laptop, Tablet o teléfonos inteligentes)
7. Dispositivos alimentados con PoE con administración centralizada.
8. Definir las políticas de seguridad correspondientes a la red.
9. Diseñar, implementar e instalar un datacenter en el primer nivel.
10. Los doctores y enfermeras podrán consultar expedientes médicos, radiografías, ultrasonidos, prescripciones médicas y demás información en cualquier momento desde sus clínicas. Dicha información está guardada en el datacenter del hospital.
11. Conexión con las principales aseguradoras del país y con CIGNA global.
12. Conexión directa con MEDLINE.
13. Implementar VPN para incrementar la seguridad de la red.
14. Para cada recepción de cada piso, se debe otorgar acceso a las recepcionistas al data center.
15. Cada sala de operaciones debe contar con cámaras de alta resolución que permita conexión desde las universidades.
16. Instalar equipo de telepresencia en las salas de operaciones y de conferencias.
17. Utilizar switches de 1GB de cobre o 10GB de fibra.
18. Diseñar un esquema de direccionamiento IPv4 pero considerar un esquema IPv6.
19. Cotizar equipos e instalación

**Requerimientos No Funcionales:**

1. Utilizar como mínimo el estándar IEEE 801.11 AC (o uno más reciente)
2. Cableado estructurado categoría 6.
3. Utilizar estándares ANSI/EIA/TIA 569, 606 o 607.
4. Utilizar las siguientes marcas para los equipos activos: CISCO, JUNIPER, HUAWEI, MIKROTIK, ALCATEL o NOKIA.
5. Utilizar las siguientes marcas de equipos pasivos: ANIXTER, SIEMON, PANDUIT, BELDEN, LEGRAND o LEVITON.
6. Utilizar las siguientes marcas de servidores: HP, DELL, LENOVO, QUANTA, INVETEC o WISTRON.
7. No hay límite de precio.
8. Certificar puntos.

**Restricciones del Proyecto**

* Marca de equipos a utilizar.
* Fecha límite de propuesta: 18/11/2019.

**Cotización de Equipos**

**Propuesta de Equipos**

**Cotización**

**Cotización de Cable y Otros Componentes**

**Cables y Largo Estimado**

**Cotización**

**Certificación**

**Topología**

**Diagrama Topológico Físico**

* **Primer Piso:**

**Diagrama Topológico Lógico**

**Colocación y Conectividad**

El diseño del esquema de direccionamiento se diseñó de tal forma que se tenía pensado la tolerancia de fallos y escalabilidad. Las redes locales de cada piso tienen el mismo diseño que en otros pisos. Esto permite también que el mantenimiento sea fácil.

**Routers**

* En el piso 1 se encuentra el Router principal que le proporciona conexión a Internet a cada piso en la oficina de IT. Es el Router que tiene conectada la línea proporcionada por el ISP.

Nombre del Router: Núcleo.

* Para cada piso, existe un Router principal que centraliza la conexión de todas las redes locales que se ubican en el respectivo piso. Se tomó esta decisión para identificar de dónde provienen los dispositivos según su dirección IP.

Nombres de los Routers: Central\_1, Central\_2, Central\_3, Central\_4, Central\_5, Central\_6 y Central\_7.

* En el piso 1, se encuentra un Router que conecta la red servidores del Datacenter con el Router Central\_1.

Nombre del Router: Datacenter\_R.

* En cada piso, se encuentra un Router que conecta la red del departamento de IT con el Router que centraliza las redes del respectivo piso.

Nombres de los Routers: DIT1, DIT2, DIT3, DIT4, DIT5, DIT6 y DIT7.

* En el piso 1, 2 y 3 se encuentran Routers que conectan la red de las cámaras ubicadas en los salones de operaciones con el Router central del respectivo piso.

Nombres de los Routers: Camaras1\_R, Camaras2\_R y Camaras3\_R.

* En cada piso hay un Router que conecta las redes del personal administrativo: red del banco, red de recepcionistas y red oficinas del respectivo piso.

Nombres de los Routers: Per\_Adm\_1, Per\_Adm\_2, Per\_Adm\_3, Per\_Adm\_4, Per\_Adm\_5, Per\_Adm\_6 y Per\_Adm\_7.

* En cada piso hay un Router que conecta la red del banco con el Router Per\_Adm del respectivo piso.

Nombres de los Routers: Banco1, Banco2, Banco3, Banco4, Banco5, Banco6 y Banco7.

* En cada piso hay un Router que conecta la red de las recepcionistas con el Router Per\_Adm del respectivo piso.

Nombres de los Routers: Recep1, Recep2, Recep3, Recep4, Recep5, Recep6 y Recep7.

* En cada piso hay un Router que conecta la red de las oficinas con el Router Per\_Adm del respectivo piso.

Nombres de los Routers: Of1, Of2, Of3, Of4, Of5, Of6 y Of7.

* En cada piso hay un Router que conecta la red wireless pública con el Router central del respectivo piso.

Nombres de los Routers: WPublica1, WPublica2, WPublica3, WPublica4, WPublica5, WPublica6 y WPublica7.

* En cada piso hay un Router que conecta la red wireless de médicos con el Router central del respectivo piso.
* Nombres de los Routers: WMed1, WMed2, WMed3, WMed4, WMed5, WMed6 y WMed7.
* Para todo el hospital (en todos los pisos), se utilizan WAPs para proporcionar conectividad en todo momento. Se consideró utilizar repetidores pero eso afecta al throughput (lo reduce un 50% por cada repetidor) y esa opción se descartó inmediatamente.

**Switches**

* En el piso 1, 2 y 3 se encuentran salas de operaciones. Para cada piso se encuentra un Switch que maneja las IP Cameras instaladas dentro de las salas de operaciones. Esto permite que las universidades puedan ver en vivo y en directo las operaciones que se llevan a cabo.

Nombres de los Switches: Camaras1\_SW, Camaras2\_SW y Camaras3\_SW.

* En cada piso, hay un switch dedicado al departamento de IT. Para el caso del piso 1, ese switch alberga también personal del datacenter y los servidores locales del hospital.

Nombres de los Switches: IT1\_SW, IT2\_SW, IT3\_SW, IT4\_SW, IT5\_SW, IT6\_SW y IT7\_SW

* En cada piso, se colocó un switch que conecta los APs con el router que proporciona conexión a internet a los visitantes del piso.

Nombres de los Switches: Piso1\_Publico\_SW, Piso2\_Publico\_SW, Piso3\_Publico\_SW, Piso4\_Publico \_SW, Piso5\_Publico\_SW, Piso6\_Publico\_SW y Piso7\_Publico\_SW

* En cada piso, se colocó un switch que conecta los APs con el router que proporciona conexión a internet a los médicos del piso.

Nombres de los Switches: Piso1\_Med\_SW, Piso2\_Med\_SW, Piso3\_Med\_SW, Piso4\_Med\_SW, Piso5\_Med\_SW, Piso6\_Med\_SW y Piso7\_Med\_SW

* Para cada piso, se tiene un Switch dedicado al respectivo banco.

Nombres de los Switches: Banco1\_SW, Banco2\_SW, Banco3\_SW, Banco4\_SW, Banco5\_SW, Banco6\_SW y Banco7\_SW.

* Para cada piso, se tiene un Switch dedicado a las oficinas.

Nombre de los Switches: Oficinas1\_SW, Oficinas2\_SW, Oficinas3\_SW, Oficinas4\_SW, Oficinas5\_SW, Oficinas6\_SW y Oficinas7\_SW.

* Para cada piso, se tiene un Switch dedicado a las Recepcionistas.

Nombre de los Switches: Rec1\_SW, Rec2\_SW, Rec3\_SW, Rec4\_SW, Rec5\_SW, Rec6\_SW y Rec7\_SW.

**Servidores**

Además, el hospital cuenta con 2 servidores adicionales:

* 1 servidor con IP xxxx.xxxx.xxxx.xxxx que soporta alta concurrencia y paralelismo y proporciona los web services que le permite a los doctores y enfermeras extraer y subir información al datacenter y conectarse a la base de datos CDC.
* 1 servidor con IP xxxx.xxxx.xxxx.xxxx que soporta alta concurrencia y paralelismo y proporciona los web services que

**Protocolos**

**Políticas de Seguridad**

**Resumen**: Los dispositivos, equipo de red y la información que estos contengan deben ser protegidos, cualquiera que sea su forma de ser compartida, comunicada o almacenada. Esta política es de consideración por parte de todos los miembros de la organización.

**Objetivos**: Comprender y tratar los riesgos operacionales y estratégicos en seguridad de los equipos y la información para que permanezcan en niveles aceptables para la organización. Entender y dar cobertura a las necesidades de todas las partes interesadas.

**Políticas y Normas**

* Las presentes normas y políticas de seguridad son aplicables en todas las áreas, departamentos o secciones de la organización, y son de cumplimiento obligatorio por parte de todos los funcionarios y empleados en cualquier nivel jerarquico, sean temporales o permanentes, definidos como usuarios o administradores de la información y equipos de red, asi como cualquier otro usuario que haga uso del sistema.
* El administrador del sistema es el responsable técnicamente de la administración, disponibilidad, seguridad y operación de la red de la organización al igual que de la información almacenada en esta.
* Un usuario es aquel que crea, lee, introduce, cambia o actualiza la

información almacenada en los sistemas de información de acuerdo a los

privilegios otorgados.

* El administrador del sistema deberá dirigir las investigaciones y auditorias sobre incidentes y problemas relacionados con la seguridad de la información y equipo de red, así como recomendar las medidas de control pertinentes.
* El administrador debe velar por la protección de la propiedad intelectual.
* El administrador del sistema debe proponer y gestionar la implementación de medidas de prevención de ataques a la red de la organización.
* Los usuarios deben conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la Información, Hardware y Software.
* Un usuario no puede divulgar por cualquier medio, información confidencial a personas no autorizadas, de no cumplir esta normativa se accionara de manera legal contra el responsable de divulgar dicha información.
* Los usuarios no pueden compartir o revelar su contraseña a otras personas

empleados o ajenos a la organización.

* Es responsabilidad del usuario seleccionar una contraseña segura que no

tenga relación obvia con el usuario, sus familiares, el Instituto de trabajo y

otras relaciones parecidas.

* Ante algún inconveniente o problema, se debe reportar inmediatamente a su jefe inmediato, al Administrador del sistema cualquier evento que pueda comprometer la seguridad y sus recursos informáticos, como por ejemplo: contagio de virus informáticos, intrusos, modificación o pérdida de datos y otras actividades poco usuales.
* La información estará protegida contra cualquier acceso no autorizado.
* Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que acceda o maneje directamente, especialmente si dicha información ha sido clasificada como sensible.
* Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral en la organización, no podrán facilitarla más que a aquellos otros empleados que necesiten conocerla para la misma finalidad y se abstendrá de usarla en beneficio propio o de terceros.
* La integridad de la información se mantendrá en relación a la clasificación de la información.
* La información relativa a los empleados, funcionarios y miembros de Junta Directiva, incluida, en su caso, la relativa a remuneraciones, evaluaciones y revisiones médicas debe ser tratada con especial cuidado como información confidencial sensible del recurso humano.
* El Usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario.
* Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales.
* Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera sin el Visto Bueno del titular de la Oficina que lo tiene asignado y la debida autorización escrita extendida por el departamento de red y el traslado debe estar motivado por los intereses y objetivos de la organizacion.
* Está prohibido modificar la configuración de hardware y software establecida por la Unidad Técnica de Informática. Tampoco está permitido hacer copias del software para fines personales.
* El Usuario es responsable de salvar periódicamente la información de su equipo personal cuando esté utilizando el hardware para evitar que un corte de energía u otra falla del equipo, le haga perder la información de manera permanente.
* El Usuario es responsable de apagar el hardware que tenga asignado cuando tenga que abandonar su estación de trabajo por períodos de tiempo superiores a una (1) hora. Deberá además bloquear su estación de trabajo durante cualquier ausencia temporal de su puesto de trabajo.
* Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:
* No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
* No colocar objetos pesados encima del Hardware.
* Mantener alejado del Hardware cualquier elemento electromagnético como imanes, teléfonos, radios, etc.
* No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.
* No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el Área de Soporte Técnico de la Unidad Técnica de Informática.
* Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
* Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.
* Ningún usuario o programa debe utilizar las contraseñas de administrador de sistemas, salvo personal autorizado.
* Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona. El usuario que viole esta normativa será responsable directo por todos los daños y perjuicios que resulten de tal violación.
* Es responsabilidad del Usuario no usar contraseñas que sean idénticas o sustancialmente similares a contraseñas previamente empleadas.
* Utilizar el Antivirus autorizado por el área de administración de red o IT, el cual tendrá disponible automáticamente cada vez que se conecte al dominio de la red.
* Mantener el Antivirus permanentemente activo para que vigile constantemente todas las operaciones realizadas en el Sistema. Está terminantemente prohibido al Usuario desactivar el Antivirus.
* Dar aviso inmediato a la Unidad Técnica de Informática y apagar el Hardware asignado inmediatamente que detecte la presencia de un virus electrónico que no es eliminado por el Antivirus. Por motivo de seguridad, los mensajes o archivos adjuntos que contengan virus serán inmediatamente eliminados sin posibilidad de recuperación.
* Está terminantemente prohibido al Usuario ejecutar los archivos anexos a su correo electrónico si no provienen de una fuente reconocida y segura.
* Queda terminantemente prohibido al Usuario compartir el disco duro del Hardware que tenga asignado, si necesita compartir alguna carpeta debe obtener la autorización correspondiente y sólo hacerlo al usuario destino.
* Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros.
* Está terminantemente prohibido el uso de correo electrónico para cualquier tema ajeno a la organización.
* Es responsabilidad del Usuario utilizar Internet únicamente con propósitos laborales. Queda terminantemente prohibido a los Usuarios el acceso, la transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, dato o material que viole estas Políticas, la Ley o los protocolos electrónicos.
* Es responsabilidad de los Usuarios desconectarse inmediatamente de páginas de Internet que tengan contenido ofensivo, ya sea sexual, pornográfico, político, racista o de cualquier otro tipo.
* La adquisición de Hardware y Software, o el desarrollo de programas, sólo se gestionará a través de la Jefatura de IT.
* Es responsabilidad del usuario, realizar un respaldo periódico de la información contenida en los dispositivos móviles o portátiles asignados, para evitar la pérdida de dicha información por robo, extravío, daño del aparato o cualquier otra circunstancia.
* Todos los sitios donde se encuentren sistemas de procesamiento informático o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.
* Es responsabilidad del Administrador de red, asignar a todos los servidores internos instalados en la organizacion, un responsable por la administración del sistema de cada uno y contar como mínimo con la siguiente información relacionada:
  + Nombre del Servidor.
  + Localización del Servidor.
  + Nombre del administrador responsable y localización al igual que su suplente.
  + Detalle especifico del Hardware.
  + Sistema operativo y su versión.
  + Aplicaciones y bases de datos.
  + Función principal y/o uso.
  + Acuerdos de mantenimiento.
* Es responsabilidad de cada administrador del sistema, que todos los servidores, así como su sistema operativo, tengan estándares de configuración de seguridad documentados y aplicados de acuerdo con el rol del servidor en la organización.
* Es responsabilidad del Administrador de Sistemas, que las actualizaciones más recientes de seguridad sean instaladas en los servidores tan pronto como sea posible, validando previamente en ambientes de prueba, considerando el menor impacto en la continuidad de los servicios de negocio.
* Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, video seguridad y cómputo deben ser tratadas como Información Confidencial.
* Queda terminantemente prohibido que los empleados y funcionarios lleven a cabo algún tipo de instalación de líneas telefónicas digitales o análogas, canales de transmisión de datos, módems o cambiar su configuración, esto es responsabilidad exclusiva del área de Informática o de cualquier empresa que se haya contratado para tal fin.
* Es responsabilidad del Administrador de red que, en los enlaces de comunicaciones establecidos con terceros, se depure el enrutamiento de tal manera que se publiquen únicamente las redes necesarias para el buen funcionamiento de las aplicaciones que utiliza este enlace.
* Los Centros de Cómputo y Data Center están clasificadas como áreas de acceso restringido.
* Es responsabilidad del Administrador de red, asegurar que todos los recursos de computación y Telecomunicaciones del Instituto cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados.

**Estas políticas deben ser comunicadas y cumplidas en su totalidad por parte de los empleados y partes externas interesadas.**

**Referencias Bibliográficas**

* [1] "Stuxnet", En.wikipedia.org, 2019. [Online]. Disponible en: https://en.wikipedia.org/wiki/Stuxnet. [Accesado: 27 Oct. 2019].
* [2] S. code, "Stuxnet code : Free Download, Borrow, and Streaming : Internet Archive", Internet Archive, 2019. [Online]. Disponible en: https://archive.org/details/Stuxnet. [Accesado: 27 Oct. 2019].
* [3] "Flame (malware)", En.wikipedia.org, 2019. [Online]. Disponible en: https://en.wikipedia.org/wiki/Flame\_(malware). [Accesado: 27 Oct. 2019].
* [4] "phoenixlzx/flame-sourcecode", GitHub, 2019. [Online]. Disponible en: https://github.com/phoenixlzx/flame-sourcecode. [Accesado: 27 Oct. 2019].