UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Implementación y soporte de servicio unificado de red en Banco

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Alberto Lorenzo León

ASESOR DE INFORME

Ing. Rodrigo Alejandro Gutiérrez Arenas

Ciudad Universitaria, Cd. Mx., 2021

Índice

Objetivos

En éste informe voy a desarrollar las principales actividades en las que he participado estando a cargo de la infraestructura que constituye el servicio unificado de red[1] que el Consorcio[2] ofrece al Banco[3].

En la primer parte del informe voy a resumir en un marco teórico los servicios y soluciones que se administran en la solución de servicio unificado de red.

A continuación, en la introducción voy a explicar las diferentes tecnologías que se han implementado en el Banco.

Considere cuatro actividades en mi reporte, donde voy a enunciar cada una de las tareas realizadas en ellas; para mostrar los retos presentados y la solución realizada para lograr mantener operativa la infraestructura del Banco y su crecimiento.

En la primer actividad voy a presentar un antes y después de migrar el centro de datos; las mejoras del mismo y el cumplimiento de los requerimientos planteados por Banxico[4].

En la segunda actividad voy a mencionar como se vivió y solventó un ciberataque[5] a la infraestructura de aplicativos del Banco, principalmente afectando a servidores de Active Directory[6], Microsoft Exchange[7], aplicativos financieros y equipos portátiles y de escritorio de los usuarios.

Para la tercer actividad, voy a describir como se llego al desarrollo de un tarificador de llamadas para Microsft Lync Server 2013[8], el proceso de análisis y desarrollo llevado a cabo; así como su implementación.

Por último, la cuarta actividad va a describir los componentes que conforman la solución de comunicaciones unificadas[9]. Presentar los diferentes escenarios en los que ha funcionado a lo largo de su tiempo de productividad y su viabilidad para dar el servicio de colaboración a los empleados del Banco antes y durante la pandemia de COVID 19.

1 Servicio unificado de red: comprende un conjunto de diferente infraestructura y aplicativos como son switches y routers de la marca HPE, así como servidores y controladoras de Wifi de la misma marca, aplicativos como ClearPass, DHCP's, tarificador de llamadas, un centro de monitoreo las 24 hrs., cableado estructurado y de fibra óptica, entre otros.

2 Consorcio: así llamare a la empresa donde laboro, ya que por temas de confidencialidad no me fue autorizado colocar el nombre de la misma.

3 Banco: así llamare a la institución financiera federal en la que el Consorcio licito y gano el proyecto de servicio unificado de red y que por temas de confidencialidad no es posible colocar su nombre.

4 Banxico: Banco de México

5 Ciberataque: es un intento malicioso y deliberado por parte de un individuo u organización para irrumpir en los sistemas informáticos de otro individuo u organización, buscando algún tipo de beneficio.

6 Active Directory: es una base de datos y conjunto se servicios que conectan a los usuarios de una red con diferentes recursos para que puedan realizar su trabajo.

7 Microsoft Exchange: es un software propietario de colaboración entre usuarios, desarrollado por Microsoft.

8 Microsft Lync Server 2013: software de comunicaciones que ofrece mensajería instantánea, presencia, conferencia y soluciones de telefonía empresarial.

9 Comunicaciones unificadas: se refiere a una solución formada por diferentes componentes y elementos, incluye correo electrónico, mensajería instantánea, voz, video, telefonía, conferencia, estado de presencia entre otras.

Marco teórico

Centro de datos o data center

Un centro de datos o data center es el instrumento de las empresas para computar, mantener registros, servicios y aplicativos para poder realizar sus tareas. Estos centros de datos deben proteger la información y los recursos más relevantes de las organizaciones.

La infraestructura existente en los centros de datos es muy importante para las organizaciones, por lo que debe cumplir con condiciones físicas y ambientales óptimas. De acuerdo con la American National Estándar Institute, los centros de datos poseen una norma de mejores prácticas llamada ANSI/TIA 942, donde su objetivo es certificar la disponibilidad de los componentes que albergan estos inmuebles, el tamaño de los mismo, el tiempo de respuesta y niveles de redundancia.

Existen cuatro niveles en los que se catalogan los centros de datos, actualmente denominados Tier, como se ilustra en la imagen 1, los cuales nos indican el nivel de fiabilidad y disponibilidad de un centro de datos.

- *Tier I*, centro de datos básico: lo constituyen las pequeñas y medianas empresas. El servicio queda comprometido y puedo sufrir interrupciones planificadas o no. Tiene la desventaja de qué sí se requiere aplicar un mantenimiento mayor tendrá que interrumpirse la actividad del centro de datos por completo.

- *Tier II*, centro de datos redundante: en este nivel, los centros de datos son menos susceptibles a interrupciones, ya sea planificadas o no. Tiene una sola conexión tanto a la línea de distribución eléctrica como a la de refrigeración, por lo que en un mantenimiento en estos campos implica una interrupción del servicio.

- *Tier III*, centro de datos concurrentemente mantenible: se enfoca a empresas que ofrecen sus servicios 24 horas los 7 días de la semana. Los centros de datos con estas características se conectan a múltiples líneas de distribución eléctricas y de refrigeración, lo cual ayuda a mantener la continuidad de las operaciones.

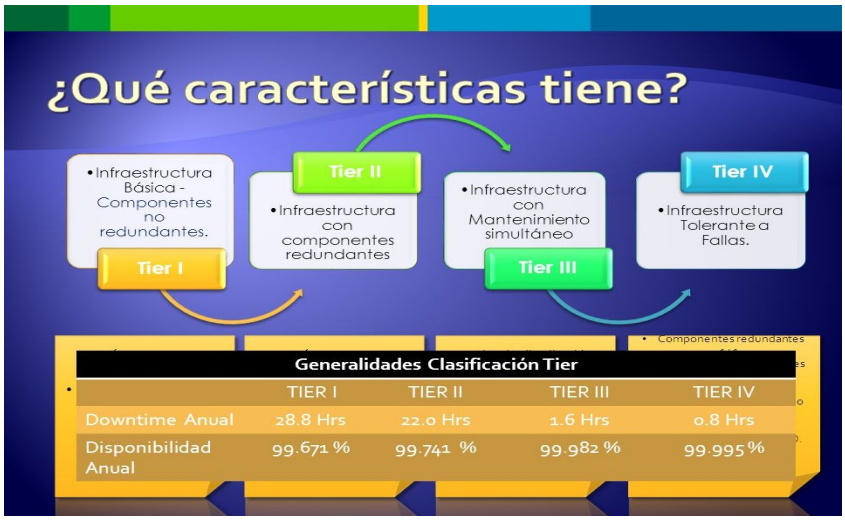


Imagen 1: Clasificación de centro de datos.

- *Tier IV*, centro de datos tolerante a fallos: está enfocado a empresas con presencia global, como bancos o empresas multinacionales, entro otras. De igual forma, los centros de datos están conectados a varias líneas de distribución eléctrica y de refrigeración, capaz de enfrentar eventos no planeados y deben cumplir con la disponibilidad más alta de los cuatro Tier, la cual es del 99.995%.

Si el centro de datos está ubicado en las propias instalaciones de la empresa, es responsabilidad de ésta, contar con expertos en los distintos campos de las aplicaciones que contenga, así como contar con contratos de mantenimiento de hardware y software. También se puede optar por un centro de datos por hosting, en donde la infraestructura de servidores vive en un sitio externo administrado por un tercero.

Aquí el proveedor proporciona el espacio para instalar los servidores, la energía eléctrica, la refrigeración para su óptimo desempeño, enlaces de comunicación dentro del mismo, entro otros servicios. Los principales beneficios de esta modalidad son la reducción de costos, mayor seguridad, mejor conectividad y flexibilidad en la gestión de servicios.

Microsoft Lync Server 2013 bajo arquitectura on-premises[10]

Microsoft Lync Server 2013 es un software de comunicaciones que ofrece soluciones de mensajería instantánea, presencia, conferencia, telefonía y movilidad para soportar las necesidades de colaboración a nivel empresarial que los usuarios demanden. Lync Server 2013 lo conforman una gran cantidad de componentes externos tales como sistemas operativos, sistemas de bases de datos, sistemas de red y sistemas telefónicos.

- *Mensajería instantánea y presencia*: permiten a los usuarios encontrarse y comunicarse entre sí de manera eficaz y eficiente. La mensajería instantánea permite a través del cliente de Lync 2013 o Skype empresarial comunicarse mediante chats. La presencia establece y muestra el uso de estados comunes como disponible, ocupado, vuelvo en seguida, en reunión o no molestar.

- *Conferencias*: Lync Server 2013 incluye el servicio de conferencias de mensajería instantánea, conferencias de audio, conferencias web, videoconferencias y uso compartido de aplicaciones, tanto para reuniones programadas como improvisadas. Adicionalmente, Lync Server 2013 admite conferencias de acceso telefónico local y vía PSTN[11].

- *Enterprise Voice*: Lync Server 2013 incluye el servicio de voice over internet protocol, VoIP[12], esto permite que los usuarios puedan llamarse internamente así como también llamar a números de la PSTN. Esta característica permite la funcionalidad de contestar, reenviar, transferir, hacer una conferencia, desviar, liberar y estacionar una llamada.

Bajo el esquema de arquitectura on-premises, Microsoft Lync Server 2013 permite implementarse en varios servidores para brindar tolerancia a fallas y alta disponibilidad. Dichos servidores se pueden agrupar en diferentes roles dependiendo de sus múltiples servicios, esta arquitectura fue aplicada en el Banco, como se muestra en la imagen 2.

10 Arquitectura on-premises: se refiere a que una empresa mantiene todos sus datos, servidores y todo su entorno de IT localmente. La empresa es responsable de ejecutar y mantener los datos en todo momento.

11 PSTN: Red telefónica pública conmutada (Public Switched Telephone Network), las llamadas locales y de larga distancia son posibles gracias a ella.

12 VoIP: se trata de un conjunto de recursos que hacen posible que la señal de voz viaje a través de internet empleando el protocolo IP (Protocolo de Internet)

Dentro de dichos roles tenemos:

- *Front End Pool:* proporciona los servicios de autenticación y registro de usuarios, información de presencia, servicio de carpeta de direcciones, mensajería instantánea, conferencias web, conferencias de acceso telefónico mediante la PSTN, conferencias audiovisuales y alojamiento de aplicaciones.
- *Edge Pool:* permite mediante la combinación de grupos que usuarios externos accedan a su implementación de Lync.
- *Wide Area Network (WAN):* es importante contar con una Red WAN cuando una implementación de Lync Server incluye sucursales.
- *Public Switched Telephone Network (PSTN):* red telefónica tradicional.
- *PSTN Gateway:* es un dispositivo que conecta a Lync Server a la PSTN.
- *Firewall:* dispositivo que realiza un filtrado especial para el tráfico de red.
- *Office Web Apps Server:* es un servidor que proporciona integración de Microsoft Office PowerPoint con conferencias.
- *Internet Information Server (IIS):* servidor web de Microsoft incluido con el sistema operativo Microsoft Windows Server.
- *SQL Server:* servidor de base de datos de Microsoft. Todos los servidores Front End de Lync utilizan SQL Server Express Edition.
- *Active Directory:* Lync Server 2013 requiere los servicios de domino de Active Directory para los grupos, usuarios y otra información de topología. Además, requiere una autoridad de certificación para la transferencia segura de datos cifrados y los servicios de certificado de Active Directory lo proporcionan.
- *File Share:* Lync Server 2013 requiere un directorio compartido para el almacenamiento de archivos.

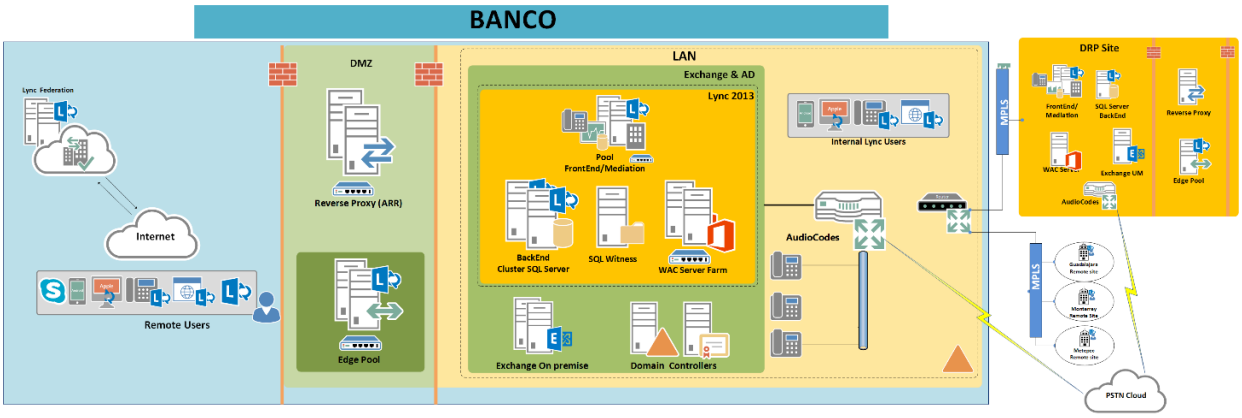


Imagen 2: Diagrama general de solución Microsoft Lync Server 2013 aplicada al Banco

Recursos open source aplicados a complementar la solución en Banco

El software open source es un código diseñado de manera que sea accesible al público: todos pueden ver, modificar y distribuir el código de la forma que consideren conveniente. El open source se ha convertido en un movimiento y una forma de trabajo que trasciende la producción del software. Este movimiento utiliza los valores y el modelo de producción descentralizada del software open source para hallar nuevas maneras de solucionar problemas en las comunidades y los sectores.

El modelo de desarrollo open source es el proceso que se utiliza en los proyectos de la comunidad open source para desarrollar sistemas de software de este tipo. El software se lanza bajo una licencia open source, la cual permite que cualquier persona pueda ver o modificar el código fuente.

- *PHP* (acrónimo recursivo de PHP: Hypertext Preprocessor) es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML. El código PHP es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente que era. PHP es altamente compatible para conexiones a bases de datos MySQL, PostgreSQL, Microsoft SQL Server entre otros.

- *MySQL-MariaDB:* MariaDB es la evolución de MySQL y es un sistema de gestión de base de datos con licencia GNU General Public License, utiliza como base el lenguaje de consultas estructurado SQL.

- *Python* es un lenguaje de programación de alto nivel, interpretado, orientado a objetos y ampliamente utilizado con semántica dinámica, utilizado para programación de propósito general.

Introducción

El Banco desde su fundación en 1937 a nuestros días tiene como objetivo principal apoyar la banca de desarrollo mexicana y financiar las exportaciones de bienes y servicios como agencia de crédito. Para poder llevar a cabo este objetivo, requiere contar con una solución de servicio unificado de red integrados que faciliten la realización de las tareas sustantivas de las diferentes áreas que lo conforman.

El Consorcio ofertó al Banco los servicios unificados de red a fin de:

- Mantener día a día en óptimo funcionamiento la red de voz y datos institucional.
- Implementación de estándares y nuevas tecnologías para mantener a la vanguardia los servicios de comunicaciones y colaboración.
- Dar cumplimiento a los niveles de servicio comprometidos con las áreas sustantivas.

Dentro de dicha oferta se incluyen hardware, software, implementación, administración, monitoreo y mantenimiento, así como servicios operativos y administrativos asociados a las redes locales, con cobertura en la CDMX y en las oficinas donde el Banco tiene presencia en la República Mexicana.

El Consorcio para llevar a cabo el cumplimiento de las necesidades de su cliente, el Banco, provee sus servicios bajo el siguiente modelo de servicios administrados en demanda:

- Servicios de red de área local
- Servicios de red inalámbrica
- Servicios de comunicación unificada (telefonía empresarial, mensajería instantánea, web conferencing, movilidad desde Internet)

Servicio de red de área local

Los servicios de red de área local que fueron instalados y configurados en las instalaciones del Banco por parte de compañeros del Consorcio, con apoyo del fabricante HPE; se ubicaron en primer instancia, en:

- *Centro de datos:* en este espacio se localiza toda la infraestructura de TI[13] de diferentes proveedores que brindan sus servicios y soluciones al Banco. Por parte del Consorcio, aquí se ubica la infraestrucura que compone la solución llamada granja de servidores, Granja, core de aplicativos, Core, además de puntos de servicio perimetral. En la imagen 3 ilustra un poco como esta constituida la solución de Granja, Core y su interconectividad.

  Se nos asignaron cuatro racks en donde alojamos la mayor cantidad de la infraestructura que compone la solución ofertada al Banco. Granja esta implementada en dos racks[14], la constituyen dos equipos HPE FlexFabric 12910 Switch AC Chasis. Entre cada equipo de Granja se configuró un enlace IRF[15] de 20Gb para que se vean lógicamente como un sólo equipo. La misma arquitectura se aplicó para Core. Core y Granja se interconectan mediante cuatro fibras ópticas de 10Gb cada una, formando una agregación de 40Gb. Esta última configuración permite contar con un ancho de banda necesario para cumplir con la capacidad de procesamiento que requieren los servicios del Banco.

13 TI: Tecnologías de la Información.

14 Rack: es un gabinete que puede contener dispositivos de red, patchera desde donde salen cables de red de datos para conectar distintos servidores y equipos de TI.

15 IRF: Intelligent Resilient Framework, es una tecnología de virtualización de software orientada a conectar varios dispositivos de red a través de puertos IRF físicos, mediante la configuración necesaria para que estos se vean como un dispositivo distribuido.

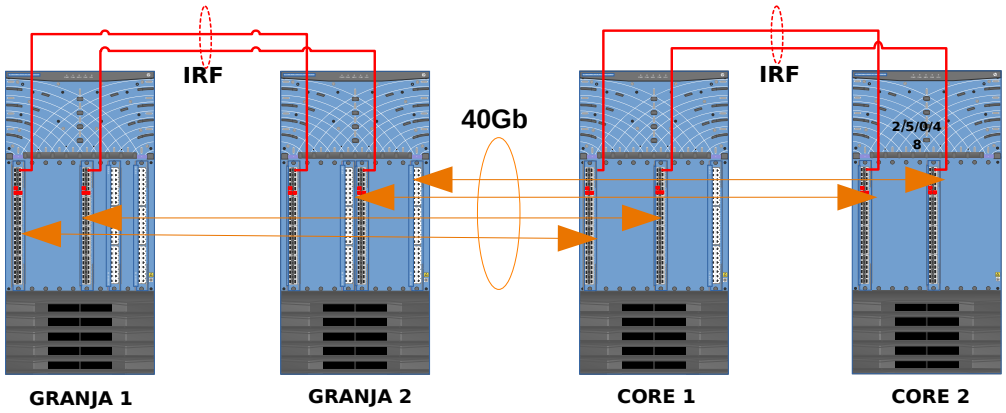


Imagen 3: Configuración de Granja y Core

- *IDFs*[16]*:* el inmueble donde se encuentra el banco cuenta con una planta baja y seis pisos. En cada uno de ellos, se asigna un área especifica para ubicar la infraestructura que brinda los servicios de red a los usuarios finales. Estas zonas se interconectan mediante fibra óptica a Core, el cual se ubica en el centro de datos, en la imagen 4 se representa la distribución de Core y los IDF's en en cada piso del Banco.

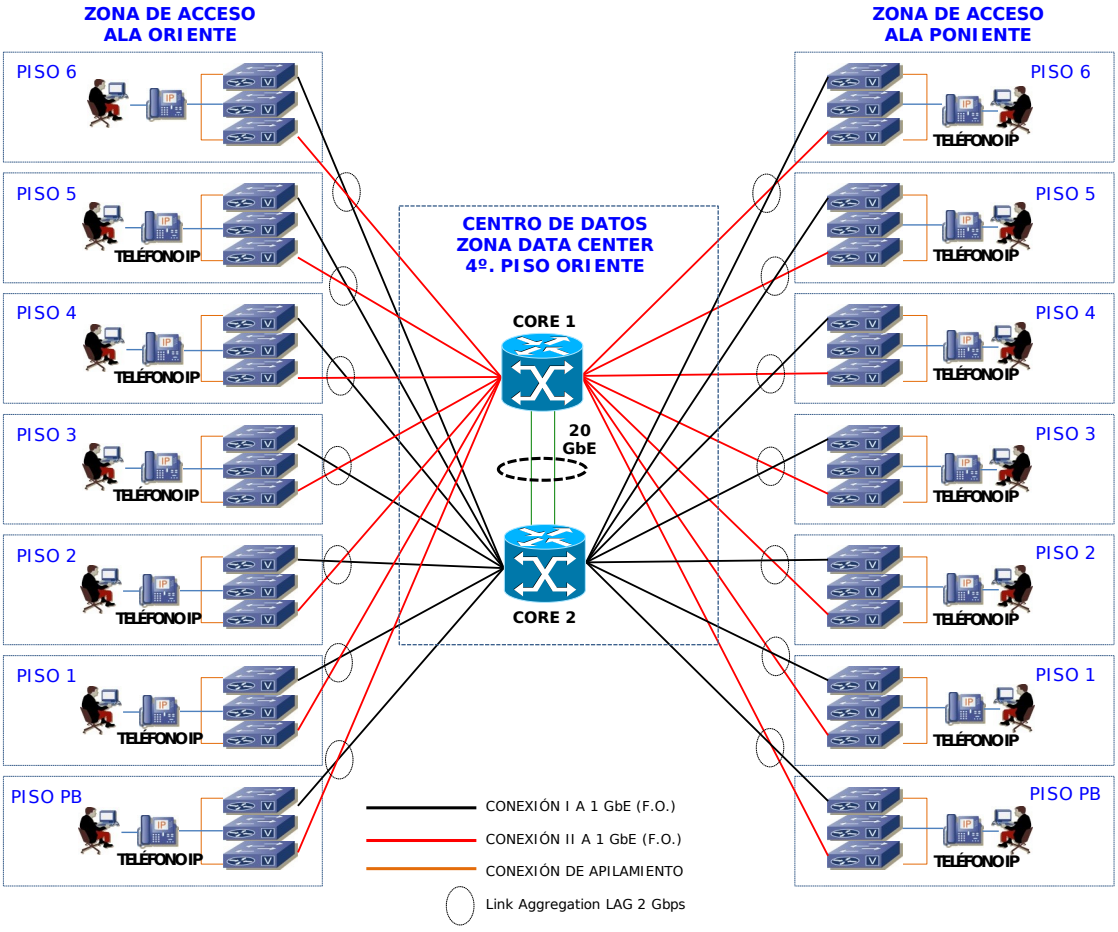


Imagen 4 : Configuración de Granja y Core

16 IDF: es un recinto de comunicación secundaria para un edificio que usa una topología de red en estrella.

- Infraestructura adicional en el centro de datos incluye los servicios de redes perimetrales, que en conjunto con compañeros del Consorcio, se implementó y entregó la solución de los siguientes servicios, como se ejemplifica en la imagen 5; los cuales fueron ubicados en racks de otros proveedores donde se contaba con espacio para instalarlos.

  - ✔ *DMZ:* es un switch configurado para prestar servicios públicos, zonas de acceso controladas por medio de firewalls del Banco.

  - ✔ *Red externa:* este equipo define la zona de acceso donde se localizan los enlaces de datos de internet del Banco.

  - ✔ *Red financiera:* son dos switches que aíslan la red local del Banco del la red destinada a proveedores de servicios de entidades normativas y financieras.

  - ✔ *Red WLAN:* es un switch destinado para brindar el servicio de movilidad en las instalaciones del Banco, siempre manteniendo la seguridad y restricciones para la conectividad a los diferentes tipos de redes y accesos a sistemas institucionales.

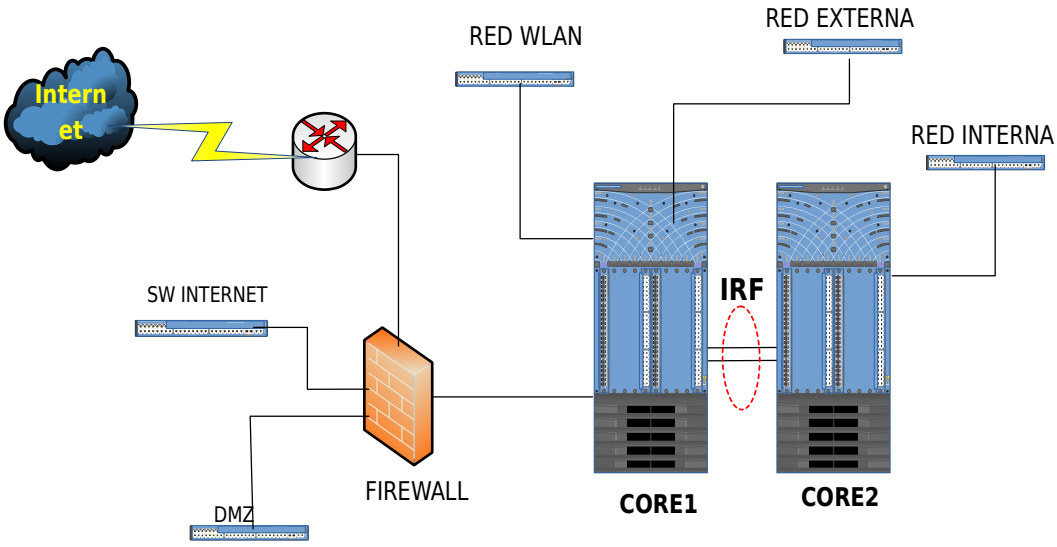


Imagen 5 : Infraestructura adicional en centro de datos

Servicio de red inalámbrico

La infraestructura que compone la solución de red inalámbrica, como se ilustra en la imagen 6, se instaló en los dos racks de Core, la cual esta constituida por dos equipos que contienen la solución Clearpass[17] del fabricante Aruba, dos servidores controladoras Cisco WLC[18] y un par más de servidores con la solución de monitoreo Aruba AirWave[19].

Los AP's[20] o puntos de acceso que se utilizaron para dar al inmueble la cobertura de red inalámbrica fueron equipos Aruba. Para cumplir con el requerimiento de la cobertura de red inálambrica, realizamos un site survey[21] con la herramienta Ekahau[22] en todo el edicficio del Banco. Lo cual nos dió como resultado la ubicación óptima de los AP's o puntos de acceso para la mejor cobertura.

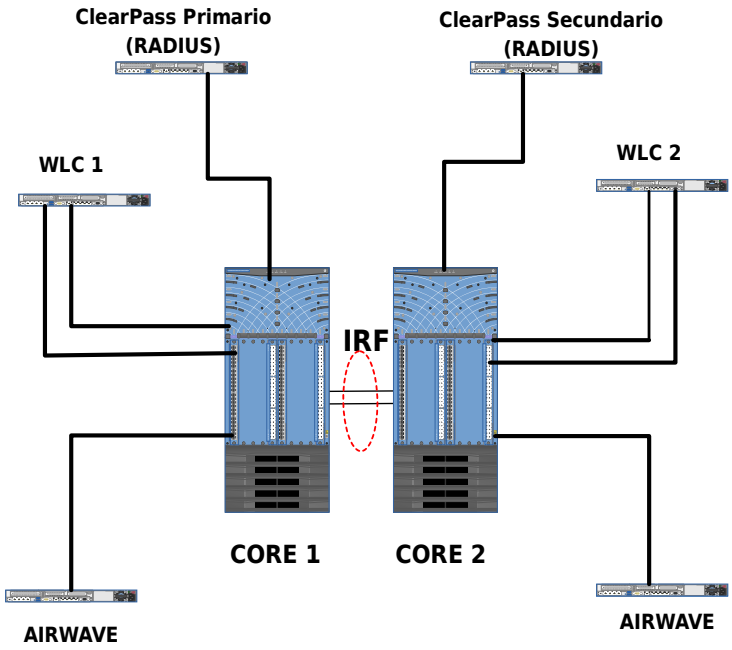


Imagen 6: Arquitectura de red inalámbrica

17 ClearPass: herramienta de control de acceso a la red.
18 WLC: Controladora de Red Inalámbrico, Wireless LAN Controller.
19 Aruba AirWave: es un sistema de operaciones de redes, además de permitir administrar la infraestructura inalámbrica de Aruba y o de otros fabricantes, también proporciona visibilidad granular de dispositivos, usuarios y aplicaciones en la red.
20 AP: Access Point o Punto de Acceso inalámbrico que proporcionan conectividad a grandes espacios públicos.
21 Site survey: análisis minucioso del entorno de red para identificar la capacidad de transmisión de datos que la infraestructura soporta y lo que esta obstruyendo el perfecto funcionamiento de la conexión inalámbrica
22 Ekahua: software para diseño y solución de problemas de redes inalámbricas.

Servicio de comunicación unificada

La solución de Microsoft Lync Server 2013 que se implementó en el Banco bajo el esquema on premises está compuesta por 12 servidores físicos ubicados en los dos racks de Granja. La siguiente tabla, 1, muestra la infraestructura que la conforma y su rol dentro de la solución.

#	Nombre	Ubicación	Descripción
1	Front End 1	Granja 1	Servidores primario y secundario, respectivamente, que contienen la aplicación de Microsoft Lync Server 2013 la cual nos permite usar mensajería instantánea (MI), presencia, conferencias y telefonía IP empresarial.
2	Fron End 2	Granja 2	
3	Edge 1	Granja 1	Servidor primario y secundario, respectivamente, que permite a los usuario comunicarse y colaborar con usuarios externos al firewall de la organización; que incluye usuarios de la propia organización que están trabajando remotamente, usuarios de organizaciones asociadas federadas y usuarios externos.
4	Edge 2	Granja 2	
5	Office Web Apps 1	Granja 1	Servidor primario y secundario, respectivamente, que contienen la aplicación Office Web Apps 2013 que proporciona la capacidad para compartir y presentar archivos de la paquetería de Microsoft Office durante una sesión de llamada o conferencia con el cliente de Lync 2013 o Skype for Business.
6	Office Web Apps 2	Granja 2	
7	Reverse Proxy 1	Granja 1	Servidor primario y secundario, respectivamente, que permiten la publicación de los servicios web de Lync fuera de la red empresarial. Estos servidores están implementados fuera de la red perimetral del Banco.
8	Reverse Proxy 2	Granja 2	
9	Back End 1	Granja 1	Servidor primario y secundario, respectivamente, de SQL Server, contiene las instancias de base de datos para la solución.
10	Back End 2	Granja 2	
11	SQL Witness	Granja 1	Servidor que provee el servicio de mirror y alta disponibilidad de las bases de datos en automático.
12	Exchange UM	Granja 1	El rol de mensajería unificada de Microsoft Exchange permite que los usuarios habilitados con buzón de correo, también puedan contar con buzón de voz para Lync Server; lo que permite que reciban notificaciones de llamadas perdidas, así como la posibilidad de revisar sus mensajes de correo de voz desde su cliente de correo Outlook.

Tabla 1: Arquitecura Microsoft Lync Server 2013 on premises en Banco

Actividad I
Migración de centro de datos o data center

Como se presentó anteriormente, la infraestructura que conforma la solución de servicios unificados de red para el Banco, esta distribuida en su mayor parte entre Core y Granja. Originalmente, la ubicación que nos fue asignada dentro del centro de datos se ilustra en la imagen 7.

Como resultado de las auditorias donde Banxico realiza a instituciones financieras que usan sus servicios, el Banco recibió las recomendación de mejorar sus instalaciones en el centro de datos. Debido a que éste presentaba algunas deficiencias en algunos rubros en los que Banxico es muy específico, por ejemplos no se contaba con un sistemas redundantes de energía y aire acondicionado; el sistema contra incendios presentaba algunas fallas, y no existía un sistema de video vigilancia y acceso controlado de usuarios.

El Banco desarrolló e implementá un nuevo centro de datos que solventa con dichas deficiencias y además, mantenga y amplíe la conectividad de servicios a Banxico, para poder llevar al cabo sus tareas con sus clientes finales. El nuevo centro de datos se implementó bajo los lineamientos de un Tier III, y el proceso de la migración se planeó y ejecutó en dos etapas controladas, para poder prevenir y evitar interrupciones y afectaciones a la operación financiera del Banco.

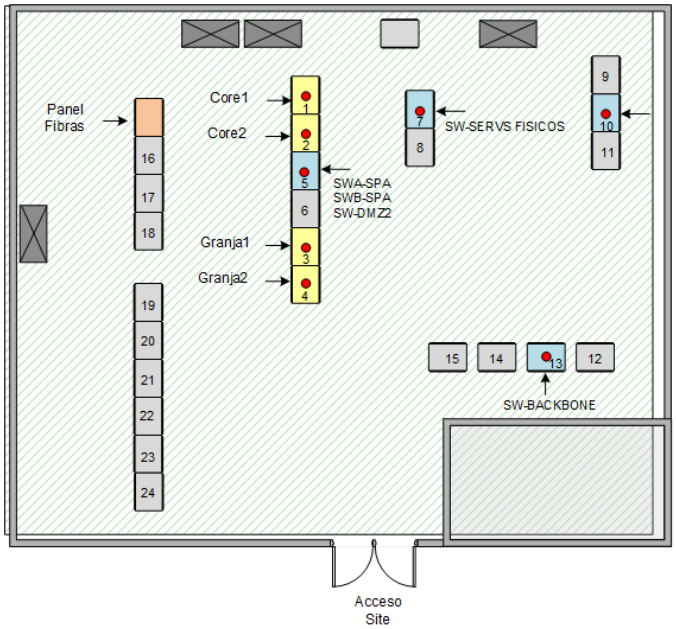


Imagen 7: Distribución original Core y Granja en centro de datos

Por parte de nuestra área, y como responsables de la infraestructura de Core, Granja y sistema de comunicaciones unificadas Microsoft Lync Server 2013; intervenimos en este proyecto, en conjunto con varias áreas del Banco, para trasladar de manera controlada y segura la infraestructura a nuestro cargo del centro de datos operativo al nuevo. Coordiné las labores de planeación, ejecución y validación de la migración de la infraestructura a cargo del Consorcio; así como de los servicios que proporcionamos al Banco.

El nuevo centro de datos, como se muestra en la imagen 8, está constituido por dos secciones: procesamiento y telecomunicaciones. En la sección de procesamiento se encuentran los racks con los servidores de SPA, Active Directory y aplicativos propios del Banco; también encontramos los dos racks de Granja y la solución de Lync Server 2013. En la sección de telecomunicaciones, se ubican los dos racks de Core y racks con servicios de Telmex y Axtel.

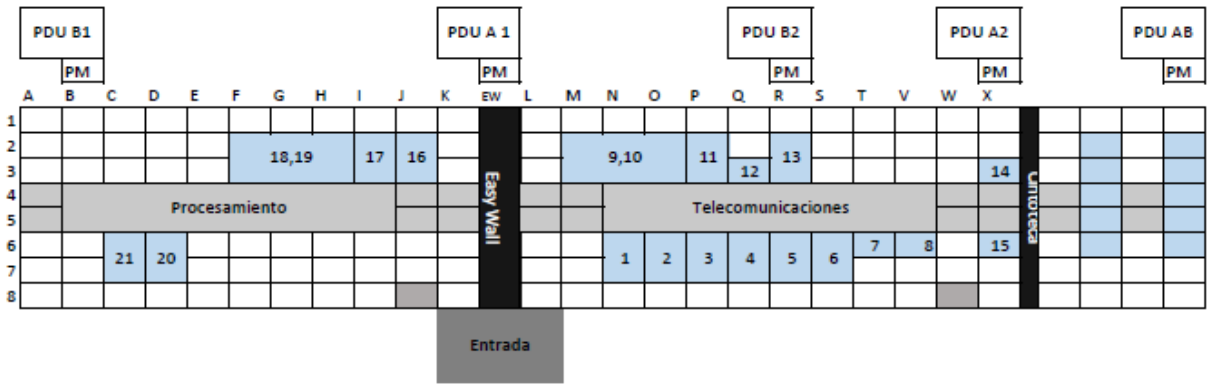


Imagen 8: Distribución de Core y Granja en el nuevo centro de datos

Primer Etapa

En un fin de semana, 9 y 10 de septiembre de 2017, como se muestra en el plan de trabajo de la imagen 9; se migra la primer etapa que comprende la solución SPA del Banco, la cual está a cargo de un tercero; y Granja, a nuestro cargo. Para la realización de esta etapa se lleva a cabo un inventario de interconexiones entre Core y Granja, previamente. De igual forma, se instalan fibras ópticas en el nuevo centro de datos; las cuales conectaran a Granja, en el nuevo centro de datos, con Core, en el centro de datos operativo; ademas de conectar a Granja con la solución SPA del Banco y con los equipos de Active Directory.

Cada empresa y/o área a cargo de infraestructura en el centro de datos, planeó y ejecutó acciones en conjunto con otras para llevar de manera exitosa la migración. Previo a la realización de la migración, se realizaron varias sesiones de trabajo en conjunto para planear e ir asignando tareas a las áreas involucradas. Durante la ejecución de la migración de Granja, se contó con el apoyo de personal capacitado para cargar los racks y montarlos en unas “tortugas” o “patines”, los cuales soportan el peso de dichos racks, dichos instrumentos nos facilitaron el traslado de los racks, del centro de datos operativo en ese momento, al nuevo.

El primer rack en migrar fue el que contiene los aplicativos SPA, Active Directory y Microsoft Exchange. Posteriormente, migramos el rack de Granja 2 y después Granja 1. Conforme se fue migrando cada rack, el equipo responsable de ellos trabajaba en las conexiones entre la infraestructura. Ya con los dos racks de Granja en el nuevo centro de datos, se realizaron las conexiones con Core, aún en el centro de datos operativo.

Con Granja en el nuevo centro de datos, se realizó y finalizó la actividad de conectar la infraestructura adicional contenida en dichos racks, por parte nuestra. Del lado de otros proveedores, se llevó a cabo las conexiones correspondientes. Finalizada esta parte de la migración, procedimos a encender y validar todo los servicios en conjunto.

En primer lugar se llevó a cabo el encendido de Granja por parte del Consorcio, después se continuó con el encendido de los servicios de SPA, Active Directory y Exchange. Se realizó las validaciones pertinentes de dichos aplicativos. Esta actividad estuvo a cargo de un tercero quien administra y gestiona dichos servicios. Cuando se concluyeron estas actividades, procedimos encender y a validar los servicios de Lync Server 2013.

Se realizaron varias pruebas por parte del Banco, quien después de no presentar algún tipo de falla en sus servicios, nos dio el VoBo de esta primer etapa y la dió por concluida exitosamente.

Id	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras	Nombres de los recursos
1	**Migración DataCenter V.3 -Banco**	**1700 mins**	**09/09/17 05:00 a. m.**	**13/09/17 09:20 a. m.**		
2	**Primer Bloque - Apagado Rack Granja 1 y 2**	**520 mins**	**09/09/17 05:00 a. m.**	**09/09/17 01:40 p. m.**		
3	Apagar – Solución SPA.	165 mins	16/09/17 05:00 a. m.	16/09/17 07:45 a. m.		BANCO
4	Apagar – Servidores Microsoft Lync de Granja 1 y 2.	40 mins	09/09/17 05:00 a. m.	09/09/17 05:40 a. m.		Alberto Lorenzo,Carlos Téllez
5	Apagar – Balanceadores Radware Alteon de Granja 1 y 2.	40 mins	09/09/17 05:40 a. m.	09/09/17 06:20 a. m.		Aldo Delgado
6	Apagar – Switches HP 12910 Granja de Servidores de Granja 1 y 2.	40 mins	09/09/17 07:00 a. m.	09/09/17 07:40 a. m.		Edgar García
7	**PUNTO DE CONTROL – Encendio y Apagado de Switch HP 12910 Granja 1 y 2 y SPA.**	**250 mins**	**09/09/17 07:45 a. m.**	**09/09/17 11:55 a. m.**		
8	Encender– Switch HP 12910 Granja 1 y 2.	30 mins	09/09/17 07:45 a. m.	09/09/17 08:15 a. m.		Edgar García
9	Encender– Solución SPA.	120 mins	09/09/17 08:15 a. m.	09/09/17 10:15 a. m.		BANCO
10	Apagar– Solución SPA.	60 mins	09/09/17 10:15 a. m.	09/09/17 11:15 a. m.		BANCO
11	Apagar – Switches HP 12910 Granja de Servidores de Granja 1 y 2.	40 mins	09/09/17 11:15 a. m.	09/09/17 11:55 a. m.		Edgar García
12	**Segundo Bloque de actividades. - Desconexión**	**130 mins**	**09/09/17 10:15 a. m.**	**09/09/17 12:25 p. m.**		
13	Desconectar (red y alimentación eléctrica) – Servidores Microsoft Lync de Granja 1 y 2.	30 mins	09/09/17 10:15 a. m.	09/09/17 10:45 a. m.		Alberto Lorenzo,Carlos Téllez,Jocelyn Corona,Rodolfo Álvarez
14	Desconectar (red y alimentación eléctrica) – Balanceadores Radware Alteon de Granja 1 y 2.	30 mins	09/09/17 10:45 a. m.	09/09/17 11:15 a. m.		Aldo Delgado,Edgar García,Emmanuel González
15	Desconectar (cables general) – KVM Granja 1 y 2.	30 mins	09/09/17 11:15 a. m.	09/09/17 11:45 a. m.		Rodolfo Álvarez
16	Desconectar (red y alimentación eléctrica) – Switch HP 12910 Granja 1 y 2.	30 mins	09/09/17 11:15 a. m.	09/09/17 11:45 a. m.		Aldo Delgado,Edgar García,Emmanuel González
17	Desconectar – PDUs y tierra física de rack Granja 1 y 2.	30 mins	09/09/17 11:45 a. m.	09/09/17 12:15 p. m.		INTCOMRED
18	PUNTO DE CONTROL -confirmación de desconexión de equipos.	10 mins	09/09/17 12:15 p. m.	09/09/17 12:25 p. m.		Emmanuel González
19	**Tercer Bloque de actividades. - Desmontaje de equipos de Rack Granja 2**	**140 mins**	**09/09/17 12:25 p. m.**	**09/09/17 02:45 p. m.**		
20	Desmontar – Servidores Microsoft Lync de Granja 2.	30 mins	09/09/17 12:25 p. m.	09/09/17 12:55 p. m.		Alberto Lorenzo,Carlos Téllez,Jocelyn Corona,Rodolfo Álvarez
21	Desmontar – Balanceadores Radware Alteon de Granja 2.	30 mins	09/09/17 12:55 p. m.	09/09/17 01:25 p. m.		Aldo Delgado
22	Desmontar – KVM.	20 mins	09/09/17 01:25 p. m.	09/09/17 01:45 p. m.		Rodolfo Álvarez
23	Desmontar – Desmontar – Switch HP 12910 Granja de 2.	40 mins	09/09/17 01:45 p. m.	09/09/17 02:25 p. m.		Edgar García
24	Desmontar – Tapas laterales y puertas del rack de Granaja 2.	10 mins	09/09/17 01:45 p. m.	09/09/17 01:55 p. m.		INTCOMRED
25	PUNTO DE CONTROL confirmar traslado de equipos exitoso a nuevo Data Center	20 mins	09/09/17 02:25 p.m.	09/09/17 02:45 p.m.		Emmanuel González
26	**Cuarto Bloque de actividades. - Traslado Rack Granja 2**	**60 mins**	**09/09/17 02:45 p. m.**	**09/09/17 03:45 p. m.**		
27	Traslado - Rack Granja 2 y equipos de la posición 4, hacia nuevo Data Center en la posición 19 (Sala Infraestructura).	60 mins	09/09/17 02:45 p. m.	09/09/17 03:45 p. m.		INTCOMRED
28	**Quinto Bloque de actividades. - Desmontaje de equipos de Rack Granja 1**	**140 mins**	**09/09/17 02:45 p. m.**	**09/09/17 05:05 p. m.**		
29	Desmontar – Servidores Microsoft Lync de Granja 1.	30 mins	09/09/17 02:45 p. m.	09/09/17 03:15 p. m.		Alberto Lorenzo,Carlos Téllez,Jocelyn Corona,Líder Técnico ,Rodolfo Álvarez
30	Desmontar – Balanceadores Radware Alteon de Granja 1.	30 mins	09/09/17 03:15 p. m.	09/09/17 03:45 p. m.		Aldo Delgado
31	Desmontar – KVM.	20 mins	09/09/17 03:45 p. m.	09/09/17 04:05 p. m.		Rodolfo Álvarez
32	Desmontar – Desmontar – Switch HP 12910 Granja de 1.	40 mins	09/09/17 04:05 p. m.	09/09/17 04:45 p. m.		Edgar García
33	Desmontar – Tapas laterales y puertas del rack de Granaja 1.	10 mins	09/09/17 04:05 p. m.	09/09/17 04:15 p. m.		INTCOMRED
34	PUNTO DE CONTROL confirmar traslado de equipos exitoso a nuevo Data Center	20 mins	09/09/17 04:45 p.m.	09/09/17 05:05 p.m.		Emmanuel González
35	**Sexto Bloque de actividades. - Montaje Rack Granja 2**	**170 mins**	**09/09/17 03:45 p. m.**	**09/09/17 06:35 p. m.**		
36	Montaje – Rack en posición 19 (sala Infraestructura).	30 mins	09/09/17 03:45 p. m.	09/09/17 04:15 p. m.		INTCOMRED
37	Montaje – Tapas laterales y puertas del rack de Granaja 2.	10 mins	09/09/17 04:15 p. m.	09/09/17 04:25 p. m.		INTCOMRED
38	Montaje – Switch HP 12910 Granja de 2.	40 mins	09/09/17 04:25 p. m.	09/09/17 05:05 p. m.		Edgar García
39	Montaje – KVM dentro del rack de Granja 2.	20 mins	09/09/17 05:05 p. m.	09/09/17 05:25 p. m.		Rodolfo Álvarez
40	Montaje - Balanceador Radware Alteon.	20 mins	09/09/17 05:25 p. m.	09/09/17 05:45 p. m.		Aldo Delgado
41	Montaje - Servidores Microsoft Lync de rack de Granja 2.	30 mins	09/09/17 05:45 p. m.	09/09/17 06:15 p. m.		Alberto Lorenzo,Carlos Téllez,Jocelyn Corona,Rodolfo Álvarez
42	PUNTO DE CONTROL (Tiempo considerado para alimentos)	20 mins	09/09/17 06:15 p. m.	09/09/17 06:35 p. m.		Emmanuel González
43	**Septimo Bloque de actividades. - Conexión de equipos Rack Granja 2**	**230 mins**	**09/09/17 06:35 p. m.**	**09/09/17 10:25 p. m.**		
44	Conectar - PDUs y tierra física del rack Granja 2.	30 mins	09/09/17 06:35 p. m.	09/09/17 07:05 p. m.		INTCOMRED
45	**Encender y validación– Switch HP 12910 Granja 2.**	**30 mins**	**09/09/17 07:05 p. m.**	**09/09/17 07:35 p. m.**		**Edgar García,Emmanuel**
46	Conectar - KVM.	20 mins	09/09/17 07:35 p. m.	09/09/17 07:55 p. m.		Rodolfo Álvarez
47	Conectar - Balanceador Radware Alteon.	10 mins	09/09/17 07:55 p. m.	09/09/17 08:05 p. m.		Aldo Delgado

Imagen 9: Plan de actividades de migración de Granja al nuevo centro de datos – primer etapa

Segunda Etapa

La segunda etapa contempló la migración de Core, así como de aplicativos y servicios de terceros. Dicha etapa se realizó los días 23 y 24 de septiembre 2017. Para poder llevarla a cabo, se replicaron las acciones realizadas en la migración de Granja, las cuales se plasmaron en un plan de trabajo que se ejecutó el día de la migración, como se ilustra en la imagen 10.

Se contratan nuevamente personal que nos apoyan a trasladar los racks del entonces actual centro de datos al nuevo; se emplean los “patines” para facilitar el traslado de los racks contemplados en esta etapa. Previo a este traslado, se realiza la desconexión de las fibras ópticas que se habían colocado provisionalmente del actual al nuevo centro de datos y que conectaban a Core y Granja.

Con Core y Granja en sus ubicaciones asignadas en el nuevo centro de datos, se realizan las conexiones entre ellos y con la demás infraestructura. Las tareas previamente planeadas en varias sesiones de trabajo resultan exitosas y se logra minimizar tiempos y tareas. Se realiza la conexión vía fibras ópticas entre los Core y entre Core y Granja. Los equipos a nuestro cargo que se conectan nuevamente a Core son los que se alojan en dichos rack; estos son aplicativos como controladoras Aruba, servidores de DHCP, servidor tarificador de llamadas, servidores de monitoreo AirWave e iMC, entre otros.

	Nombre de tarea	Duration	Start	Finish	Predecessors	Resource Names
1	**Migración DataCenter V.1 -Bancc ıt - Core**	**1,120 mins**	**Sat 9/23/17**	**Mon 9/25/17**		
2	**Primer Bloque - Apagado Rack Core 1 y 2**	**190 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
3	Apagar – Servidores AudioCode Core 1.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
4	Apagar – Servidores Aruba Core 1 y 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
5	Apagar – Servidor Storage Core 1	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
6	Apagar – Servidor Tarificador Core 2	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
7	Apagar – Servidor Grabaciones Core 2	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
8	Apagar – Servidores iMC Core 2	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
9	Apagar – Servidores Microsoft Lync de Granja 1 y 2.	40 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
10	Apagar – Servidores DHCP Core 2	40 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
11	Apagar – Switches HP 12910 Core 1 y 2.	40 mins	Sat 9/23/17	Sat 9/23/17		Edgar García
12	**PUNTO DE CONTROL – Encendio y Apagado de Switch HP 12910 Core 1 y 2.**	**80 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
13	Encender– Switch HP 12910 Granja 1 y 2.	40 mins	Sat 9/23/17	Sat 9/23/17		Edgar García
14	Apagar – Switches HP 12910 Granja de Servidores de Granja 1 y 2.	40 mins	Sat 9/23/17	Sat 9/23/17		Edgar García
15	**Segundo Bloque de actividades. - Desconexión**	**70 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
16	Desconectar (red y alimentación eléctrica) – Servidores AudioCode Core 1.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
17	Desconectar (red y alimentación eléctrica) – Servidores Aruba de Core 1 y 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
18	Desconectar (red y alimentación eléctrica) – Servidores Storage Core 1.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
19	Desconectar (red y alimntación eléctrica) – Servidor Tarificador Core 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Rodolfo Álvarez,
20	Desconectar (red y alimntación eléctrica) – Servidores de Grabaciones Core 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Rodolfo Álvarez,
21	Desconectar (red y alimentación eléctrica) – Servidores iMC de Core 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
22	Desconectar (red y alimentación eléctrica) – Servidores DHCP Core 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
23	Desconectar (red y alimentación eléctrica) – Switch HP 12910 Core 1 y 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
24	Desconectar – PDUs y tierra física de rack Core 1 y 2.	30 mins	Sat 9/23/17	Sat 9/23/17		INTCOMRED
25	PUNTO DE CONTROL -confirmación de desconexión de equipos.	10 mins	Sat 9/23/17	Sat 9/23/17		Emmanuel Gonz
26	**Tercer Bloque de actividades. - Desmontaje de equipos de Rack Core 1 y 2**	**70 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
27	Desmontar – Servidores Aruba Core 1 y 2.	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
28	Desmontar – Servidore Storage Core 1	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,
29	Desmontar – Servidores AudioCode Core 1.	30 mins	Sat 9/23/17	Sat 9/23/17		Rodolfo Álvarez,
30	Desmontar – Servidores iMC Core 2	30 mins	Sat 9/9/17	Sat 9/9/17		Rodolfo Álvarez,
31	Desmontar – Servidores DHCP Core 2.	30 mins	Sat 9/9/17	Sat 9/9/17		Rodolfo Álvarez,
32	Desmontar – Servidor Tarificador Core 2.	30 mins	Sat 9/9/17	Sat 9/9/17		Rodolfo Álvarez,
33	Desmontar – Servidor Grabador Core 2.	30 mins	Sat 9/9/17	Sat 9/9/17		Rodolfo Álvarez,
34	PUNTO DE CONTROL – Validar desmotaje de servidores y alistamiento de rack para	10 mins	Sat 9/9/17	Sat 9/9/17		Emmanuel Gonz
35	**Cuarto Bloque de actividades. - Traslado Rack Core 1**	**0.13 days**	**Sat 9/23/17**	**Sat 9/23/17**		
36	Traslado - Rack Core 1 y equipos de la posición 1, hacia nuevo Data Center en la pos	60 mins	Sat 9/23/17	Sat 9/23/17		INTCOMRED
37	**Quinto Bloque de actividades. - Traslado Rack Core 2**	**0.13 days**	**Sat 9/23/17**	**Sat 9/23/17**		
38	Traslado - Rack Core 2 y equipos de la posición 2, hacia nuevo Data Center en la pos	60 mins	Sat 9/23/17	Sat 9/23/17		INTCOMRED
39	**Sexto Bloque de actividades. - Apagado de Switches Verticales**	**120 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
40	Apagado - Switches de verticales	120 mins	Sat 9/23/17	Sat 9/23/17		Aldo Delgado,Ed
41	**Septimo Bloque de actividades. - Montaje Rack Core 1 y 2**	**70 mins**	**Sat 9/23/17**	**Sat 9/23/17**		
42	Montaje – Servidores Aruba Core 1	30 mins	Sat 9/23/17	Sat 9/23/17		Alberto Lorenzo,

Imagen 10: Plan de actividades de migración de Core al nuevo centro de datos – segunda etapa

En esta segunda etapa también se contempló las conexiones vía fibra óptica de Core a los IDF's y las validaciones de servicios a los usuarios finales. Adicional, igual que en la primer etapa, se migraron los servicios restantes de otros proveedores.

Los servicios de redes perimetrales a nuestro cargo, fueron reubicados en un nuevo rack que nos fue asignado, para contar con una mejor administración de toda la infraestrucura a nuestro cargo dentro del nuevo centro de datos. En la imagen 11 se ilustra como quedó al final la distribución en el nuevo centro de datos, la cual corresponde al área de red financiera.

El nuevo centro de datos permite al Banco contar con un mejor sistema redundante de corriente eléctrica, con un sistema eficiente de aire acondicionado para mantener en óptimas condiciones la infraestructura que ahí se aloja, un sistema contra incendios adecuado al tipo de equipos, un sistema de video vigilancia y un sistema de control de accesos por medio de validación biométrica. Todas estas mejoras en conjunto con el cumplimiento de las observaciones hechas en auditorias por Banxico, le permiten al Banco seguir creciendo y ampliando sus servicios para con sus clientes y como con el propio Banxico. En el ambito técnico, permite un mejor control para la realización de algún tipo de mantenimineto preventivo o correctivo sin afectar la operación del Banco.

	Rack	Descripción	Cuadrante	PDU	Cantidad
TELECOMUNICACIONES	1	LIBRE			
	2	MPLS	O6,O7	A-B	1
	3	Reuters	P6,P7	A2	1
	3	Reuters	P6,P7	B2	1
	3	Reuters	P6,P7	A-B	1
	4	Red Financiera	Q6,Q7	A2	1
	4	Red Financiera	Q6,Q7	B2	1
	4	Red Financiera	Q6,Q7	A-B	1
	5	Multiplexor GDC	R6,R7	A2	1
	5	Multiplexor GDC	R6,R7	B2	1
	5	Multiplexor GDC	R6,R7	A-B	1
	6	MetroRed, Metronet y Red Presidencial	S6,S7	A-B	2
	7	Telmex 1	T6	A-B	0
	7	Telmex 1	T6	A2	1
	7	Telmex 1	T6	B2	1
	8	Telmex 2	V6	A-B	0
	8	Telmex 2	V6	A2	1
	8	Telmex 2	V6	B2	1
	9	Core 1	M3,M2	N/A	0
	9	Core 1	M3,M2	A2	2
	9	Core 1	M3,M2	B2	2
	10	Core 2	O3,O2	A-B	1
	10	Core 2	O3,O2	A2	2
	10	Core 2	O3,O2	B2	2
	11	F.O. Verticales	P3,P2	A-B	1
	12	Telmex Cobre	Q3	N/A	0
	13	Otros Servicios	R3,R2	A2	1
	13	Otros Servicios	R3,R2	B2	1
	13	Otros Servicios	R3,R2	A-B	1
	14	Acometida Alestra Voz	X3	A-B	1
	15	Acometida Alestra Datos	X6	A-B	1
PROCESAMIENTO	16	SPA 1	J3,J2	A-B	1
	16	SPA 1	J3,J2	A1	1
	16	SPA 1	J3,J2	B1	1
	17	SPA 2	I3,I2	A1	6
	17	SPA 2	I3,I2	B1	6
	17	SPA 2	I3,I2	A-B	3
	18	Granja 1	F3,F2	A1	2
	18	Granja 1	F3,F2	B1	2
	18	Granja 1	F3,F2	A-B	1
	19	Granja 2	H3,H2	A1	2
	19	Granja 2	H3,H2	B1	2
	19	Granja 2	H3,H2	A-B	1
	20	Seguridad 1	D6,D7	A1	1
	20	Seguridad 1	D6,D7	B1	1
	20	Seguridad 1	D6,D7	A-B	1
	21	Seguridad 2	C6,C7	A1	1
	21	Seguridad 2	C6,C7	B1	1
	21	Seguridad 2	C6,C7	A-B	1

Imagen 11: Distribución final de toda la infrestrucura en el nuevo centro de datos

Actividad II
Ciberataque a servicios financieros de Banco

La infraestructura de servicio unificado de red que implementó el Consorcio, en un inicio, sólo contaba con la configuración que heredamos de la solución previa, la cual sólo tenía la configuración de las diferentes VLAN[23]s que segmentan los diversos servicios financieros para los usuarios del Banco. Se contaba con la configuración de VLAN's para el segmento de voz por piso y de datos por servicios. Adicionalmente, se tenía el monitoreo de los estados de salud tanto de procesador, memoria y consumo de disco duro de los equipos de la red LAN; de igual forma, el consumo de ancho de banda de la red internet. Dentro de la configuración de la infraestrucutura global, se tenía un segmento especifico que brindaba el servicio de internet inalámbrico a usuarios externos del Banco. Para conectar a usuarios externos a la red de invitados, no se tenía alguna política o restircción por parte del Banco.

Inicialmente, nuestra solución en producción fue configurada con éstas características, pero con el paso del tiempo, y debido a las diversas necesidades operativas del Banco; la configuración de toda la infraestructura fue evolucionando poco a poco. Se incorporaron métodos como autenticación MAC[24] de los dispositivos de red, teléfonos IP y equipos de cómputo de escritorio y portatiles.

Los dispositivos de red se actualizaban mínimo una vez al año ya que por su operatividad, es crítico actualizar sin afectar la operación del Banco. Los teléfonos IP de igual forma se actualizaban una vez al año, ya que el firware que utilizan; es específico para uso del Banco. Servidores y equpos de escritorio y portatiles se actulizaban cada dos o tres meses, contando adicionamente con su antivirus; aplicativos de terceros también se procuraba que contaran con las últimas actulizaciones.

En enero de 2018, el Banco vivió un ciberataque en toda su infraestructura de dominio y aplicativos financieros, que comprendió sus servicios de Active Directory, Microsoft Exchange, sistemas conectados a Banxico y equipos portátiles y de escritorio de sus usuarios.

El ciberataque comenzó afectando los equipos portátiles y de escritorio, impidiendo su uso y forzando su reinicio. Se presento de manera aislada en un par de equipos, pero en cuestión de minutos, ya eran aproximadamente todos los equipos con el mismo comportamiento. Los equipos que de forma similar comenzaron a presentar este comportamiento fueron los servidores de dominio y aplicativos financieros que brindan servicios críticos al Banco.

La primer tarea en la que participamos como parte del Consorcio mientras los equipos estaban siendo afectados, fue interrumpir la conexión hacia internet de todo el Banco, posteriormente, dimos de baja los servicios de comunicaciones unificadas como son correo electrónico, mensajería instantánea y telefonía.

La comunicación con Banxico se dió de baja de igual forma, pero antes de dicha acción, se validaron las operaciones financieras realizadas hasta ese momento, las cuales requieren de varios factores de autorización por diferentes áreas del Banco. Fue en ese instante cuando se identificaron algunas transacciones bancarias por cientos de dolares listas para ser realizadas, pero gracias a las medidas de validación en el proceso de ejecución de cada operación, fueron detectadas y denegadas.

23 VLAN: red de área local virtual, divide una red física en segmentos de redes lógicas.
24 Autenticación MAC: permite limitar que dispositivos pueden conectarse a una red WiFi o LAN, mediante la autorización o denegación de servicios por su dirección de control de acceso al medio.

De igual forma, se solicitó el apoyo a Banxico para validar y cancelar operaciones dudosas e interrumpir temporalmente la conexión entre ambas instituciones.

Para poder continuar con los servicios del Banco, se acondicionaron líneas telefónicas análogas de contingencia y se configuró una red privada exclusivamente para que las áreas críticas pudieran trabajar y finalizar sus operaciones del día con Banxico. Los equipos habilitados se monitorearon en todo momento.

Dentro de la solución unificada de red, se contempló un sitio alterno, DRP[25], el cual se encuentra ubicado físicamente en Metepec, Estado de México; en las instalaciones de una empresa externa que ofrece este servicio, se representa en la imagen 12; el cual fue pensado para tener los servicios básicos y esenciales para la continuidad del negocio del Banco.

La conectividad e infraestructura en el DRP estan a cargo del Consorcio, dicho sitio alterno tiene dependías de servicios centralizados en el Banco, como por ejemplo información de dominio mediante Active Directory, Exchange y aplicaciones financieras; por lo que al intentar poner en operación, se identificó que no era posible y se descartó esta opción para la continuidad de operaciones financieras.

Imagen 12: Banco - DRP

Bajo este escenario, se laboró varios días en lo que las áreas como seguridad informática, soporte técnico de equipos de cómputo y de tecnología trabajaban para recuperar los servidores, servicios de domino y equipos de computo afectados.

Por nuestra parte iniciamos a rediseñar y a realizar nuevas configuraciones a toda la red. Dentro de las mejoras realizadas inicialmente, fue aplicar nueva configuración en Core, Granja y switches de servicios financieros; se configuraron ACLs[26], como se ejemplifica la imagen 13, para delimitar el tráfico en la red entre equipos financieron y el resto de los equipos. Además se definieron rutas estáticas[27] entre equipos de red y equipos de usuarios.

25 DRP: Disaster Recovery Plan o Plan de Recuperación de Desastres, es un sistema con el cual las organizaciones se preparan contra posibles desastres de diversos índoles que puedan dañar su infraestructura tecnológica y poner fin a sus actividades.
26 ACL: Listas de control de acceso, permiten controlar el flujo del tráfico en los equipos de redes, tales como enrutadores y conmutadores.
27 Rutas estáticas: define una ruta explícita entre dos dispositivos de red.

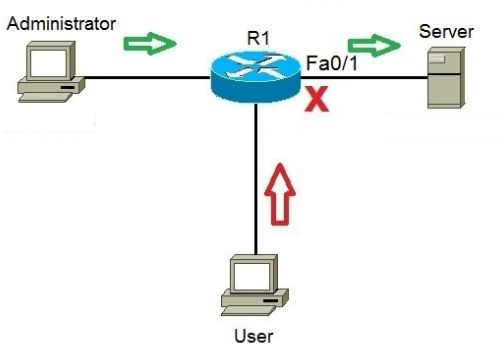


Imagen 13: Ejemplo de ACL aplicado en nueva configuración de Banco

Se configuró en la solución de ClearPass de Aruba el protocolo RADIUS[28] para aplicar tripe autenticación en equipos de red y equipos de cómputo. En el mismo ClearPass se crearon usuarios y perfiles, los cuales fueron habilitados para la administración de los equipos de red y se eliminaron los usuarios locales de los mismos, como se ejemplifica en la imagen 14.

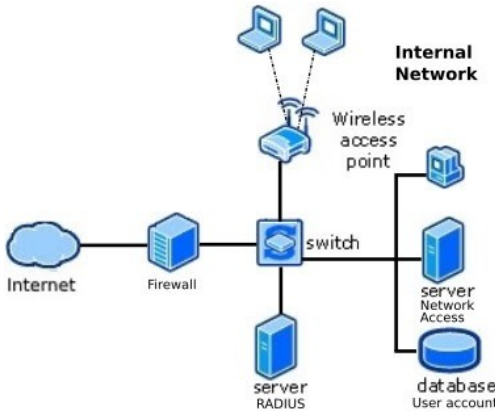


Imagen 14: Ejemplo de operación de protocolo RADIUS aplicado a dispositivos de red de Banco

Estos fueron algunos requerimientos iniciales solicitados y validados por parte del área de seguiridad informatica de Banxico para poder conectarnos nuevamente a sus servicios, pero en modo contingencia; en lo que recuperabamos los servidores de dominio aplicativos financieron afectados y los equipos de cómputo afectados.

Después de varias semanas de trabajos en la infraestructura afectada, comenzamos a probar e integrar los servidores de dominio a la red, realizamos validaciones y pruebas de funcionalidad individual y en conjunto con otras integraciones. En un inicio la problemática que enfrentamos fue contar con respaldos actualizados de los equipos afectados, se contaba con políticas de respaldos institucional pero no se llevaban a cabo eficientemente. Realizamos varios intentos, tuvimos diferencias en la información de usuarios de dominio y cuentas de Lync Server 2013. Dichas dificultades se fueron superando hasta llegar a un punto en donde se logró recuperar en su totalidad la información a como estaba operando antes del ciberataque.

28 RADIUS: Proviene del acrónimo Remote Access Dial in User Service y se trata de un protocolo cliente-servidor AAA (Authentication, Authorization and Accounting) que se encarga de gestionar el acceso de los usuarios a las redes a través de un dispositivo NAS

En el ámbito de los equipos de computo afectados se logró recuperar poca información de los usuarios y al final se remplazaron los discos duros de los equipos para llevar a cabo nuevos hardening[29] en la configuración de los mismos.

El Banco contrató los servicios de una empresa extranjera para que llevara a cabo la ingeniería forense del ciberataque, se le proporcionaron evidencia tanto de servidores afectados como equipos de cómputo. También se les proporcionó la configuración de toda la red LAN y wireless para su revisión. Después de varias sesiones de trabajo y entrevistas en conjunto con los forenses y con los diferentes coordinares de la infraestructura operativa en el Banco; se entregó el resultado de su análisis a los directivos del institución, con toda la información resultado de su estudio. También los forenses entregaron un manual de procesos y recomendaciones de mejora para aplicar en el Banco y contar con una mejor ciberseguridad en la infraestructura.

Para poder recuperar los servicios financieros en su totalidad con Banxico ejecutó una gran cantidad de auditorias y recomendaciones a solucionar en toda la infraestructura del Banco para poder habilitar los servicios nuevamente. El Banco adquirió tanto software y hardware que les fue recomendado para fortalecer la seguridad en los equipos que se conectan al Banxico.

Por parte del Consorcio, se mejoro la configuración de conexión a la infraestructura de red, la propia configuración de Core, Granja, switches de acceso y de red financiera y AP’s contaron con protocolo RADIUS y autenticación MAC.

Invirtió en su personal para capacitarlo en temas de ciberseguridad, tomando cursos para poder hacer uso de recursos open source como son el sistema Kali Linux, el cual cuenta con una amplia gama de herramientas para hacer análisis de vulnerabilidades a sistemas operativos, aplicativos como son bases de datos SQL Server, Active Directory, Microsoft Exchange, permite la ejecución de script en Python, exploit, para validar en maqueta algunas de las vulnerabilidades en sistemas o aplicativos reportados por paginas especializadas en seguridad informática.

Después de esta experiencia, el Banco mejoró sus procesos de protección de la información crítica:

- Fortaleció sus políticas de respaldo de información y configuración de servidores.

- Invirtió en la adquisición de antivirus, recomendado por los ingenieros forenses y por Banxico, el cual fue instalado en todos los servidores de los proveedores que conforman las diferentes soluciones implementadas, así como de igual forma en equipos de cómputo de usuarios del Banco.

- Se mejoro la política de aplicación de actualizaciones de seguridad en sistemas operativos, tanto para servidores como para equipos de cómputo. Estas se realizan cada mes y primero se aplican en servidores de dominio y después en servidores de aplicativos, finalmente en equipos de cómputo de usuarios finales; todo esto mediante un sistema centralizado llamado WSUS[30].

- Se adquirió nueva infraestructura y se implemento una red de invitados nueva para separar físicamente la red de usuarios invitados del Banco de la red institucional.

29 Hardening: en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

30 WSUS: Windows Server Update Services es un rol disponible en Windows Server, que permite disponer de un sistema centralizado de actualizaciones para equipos de puestos de trabajo Windows a través de la red local de nuestra empresa. Mediante WSUS se gestiona completamente la distribución de las últimas actualizaciones publicadas por Microsoft Windows a través de Windows Update así como de parches de seguridad más recientes.

- Se reconfiguró la solución de Granja y Core aplicando mejoras como nuevos ACLś, rutas estáticas, se actualizo al último firware recomendado por el fabricante. De igual forma los switches de acceso y de red financiera fueron actualizados a la última versión recomendada.

- Se rediseñó el concepto de DRP, en un inicio se migraron nuevos servicios financieros en los equipos que ahí se alojan, pasando previamente por varias auditorias y recomendaciones de Banxico. Después de superar dicho proceso, se diseñó e implementó una parte del propio DRP en la nube, mediante servicios de AWS. Sólo se migraron aquellos servicios que el propio Banxico, por políticas, permite estén alojados en servicios de nube. Se eliminaron ciertas dependencias centrales de aplicativos bancarios para poder hacer uso de ellos en caso de cualquier contingencia.

- Cada determinado tiempo, se simula una contingencia en sede del Banco y se habilitan los servicios de DRP, desde ahí las áreas financieras realizan sus operaciones y trabajan con normalidad sus actividades.

- Se realizan y aplican políticas de acceso de equipo de cómputo portátil externo a las instalaciones del Banco, tanto de usuarios como de proveedores. Se aplica un hardening a los equipos previos a su ingreso, si el personal va a estar varios días ingresando al Banco. Si el proveedor o visitante va por un corto tiempo, se deshabilitan puertos con unas etiquetas las cuales sólo pueden ser colocadas y retiras por personal de vigilancia del mismo Banco.

- El acceso a la red de invitados es sólo con solicitud al área involucrada. Dicha red es monitoreada para prevenir un uso inadecuado del recurso.

- Puertos de red sin uso en Granja, Core y switches se habilitan y deshabilitan administrativamente cada que hay cambios en la arquitectura de la propia red o se da un cambio de ubicación de usuarios por motivos operativos del Banco.

- Se adquiere y hace uso de software especializado para realizar análisis de vulnerabilidades en infraestructura nueva que se adiciona a la ya existente en el Banco. También se realizan análisis de vulnerabilidades a servidores y equipos de cómputo conectados a la red institucional cada determinado tiempo o cuando por parte de algunos plataformas llega algún boletín informativo con algunas recomendaciones a revisar y/o aplicar en caso de contar con software identificado.

- Se implementa un sistema automatizado de respaldo de configuración de toda la infraestructura de red mediante un script en Python, dicho recomendación fue hecha por el propio Banxico.

Entre algunas otras acciones el Banco a la fecha, mediante su área de seguridad informática y del Consorcio como administradores de la infraestructura de la red, ha trabajado arduamente para mantener lo más segura y libre su infraestructura de afectaciones por ciberataques. Durante procesos electorales en el país a recibido algunos tipos de ciberamenazas y también cuando han sido afectados otras instituciones financieras. Por suerte no se ha vuelto a vivir otro caso como el anteriormente comentado. Día a día van cambiando los requerimientos del Banco, dichos cambios siempre conllevan un análisis de seguridad informática.

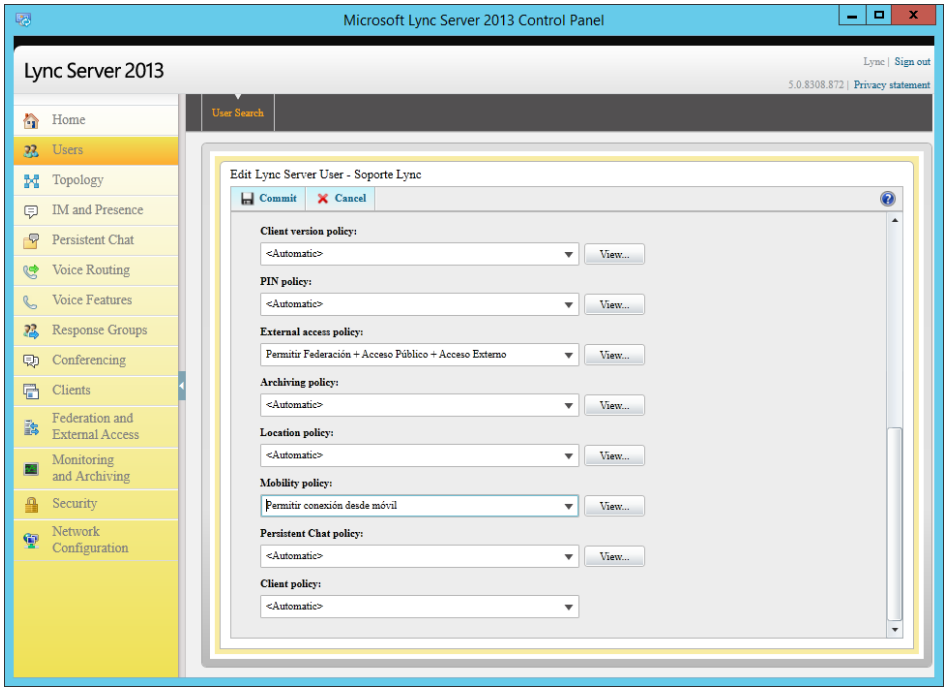
Actividad III
Tarificador complementario para Lync Server 2013

Como parte de la solución integral de servicios que ofertó el Consorcio, se tiene la aplicación de tarificación de llamadas. Microsoft Lync Server 2013 tiene una forma muy particular de como llevar a cabo el registro de llamadas, conferencias y transferencias internas y/o externas, su mensajería instantanea y la presentación de contenido mediante videollamadas.

Por esta situación la solución originalmente entregada al Banco no contemplo varios puntos de como Lync Server 2013 registra las llamadas en las bases de datos y tablas que contiene en SQL Server. Adicionalmente su proveedor de telefonía e internet, Axtel, tiene una forma especial de realizar el cobro de cada llamada, tanto para llamadas locales, celulares, larga distancia nacional e internacional (Estados Unidos y Canada), Centroamérica y el Caribe, Sudamérica, Europa y resto del mundo.

La solución no cumplió con los requerimientos en éste rubro al Banco, por más que sus desarrolladores trabajaron para lograrlo. Por último, el Banco planteo un requerimiento poco realizado por los tarificadores convencionales; el cual consistía en realizar sistemáticamente la cobranza de llamadas a sus usuarios, diferenciando cuales llamadas eran de uso personal y cuales eran de uso laboral.

Todos el personal empleado, servicios sociales, preveedores en sitio y otros que laboran de fijo en el Banco y cuentan con un equipo de cómputo y correo electrónico de la institución, estan dados de alta en Active Directory y Exchange. Estas plataformas proveeen de información elemental para la configuración de extensiones en Lync Server 2013. Cuando se da de alta una extensión en Lync Server 2013, previamente debe de existir un correo electrónico asignado a una persona en los servidores de dominio del Banco, como se muestra en la imagen 15.



Imagne 15: Ejemplo de la consola de administración de usuarios y extensiones de Lync Server 2013

Cumpliendo con los requerimientos anteriores, la extensión es habilitada en Lync Server 2013 con los parámetros de cobertura y de dominio, se configura en equipos telefónicos IP de marca Yealink T48G o Polycom VVX601, se ilustran en la imagen 16, los cuales cumplen en hardware y software recomendado por Microsoft.

Imagne 16: Modelos Yealink T48G y Polycom VVX 601 usados en Banco

Ya configurado el equipo telefónico la extensión correspondiente, el usuario ya puede hacer uso de los servicios que Lync 2013 ofrece. En el teléfono puede realizar:

- Llamadas internas hacia extensiones y/o externas hacia la PSTN.
- Realizar transferencias de llamadas internas o externas, ya sea asistida o a ciegas.
- Poner en espera llamadas.
- Realizar o participar en conferencias.
- Tomar llamadas de otras extensiones mientras estas esten configuradas en un grupo específico.
- Configurar números favoritos para un rápido marcado.
- Marcar a su buzón de voz en caso de estar habilitado mediante Exchange.
- Configurar desvio de llamadas

Adicional a estas funcionalidades, el cliente de Lync Server 2013, ahora Skype for Business, instalado en los equipos de cómputo institucional, permiten las mismas funciones y además:

- Videollamadas y videoconferencias.
- Mensajería instantánea.
- Compartir presentaciones de archivos o el escritorio de equipo de cómputo de usuarios.
- Permite configurar un arreglo jefe secretaria en extensiones de gerentes y directores del Banco, dicha función permite que cuando un jefe recibe una llamada, su asistente también la reciba, ya sea al mismo tiempo o después de algunos rings previos en la extensión del jefe.

Todas estas interacciones quedan registradas en las bases de datos SQL Server que utiliza Lync Server 2013 en los servidores Back End. De las bases de datos que utiliza el sistema, sólo emplearemos la base LcsCDR que es donde se registran todas las llamadas, ya sean entre extensiones y hacia la red pública y buzón de voz; desde el equipo telefónico o desde el cliente de Lync o Skype for Business. Las interacciones de mensajería instantánea, videollamadas y compartir escritorio o archivos queda registrada en otras bases, las cuales para objetivos del tarificador no son contempladas.

Para el desarrollo del tarificador complementario en primer instancia, se validaron varias facturas del proveedor Axtel con consultas de registros de en las bases de datos del sistema. Se identificó dicha base de datos y tablas empleadas por Lync Server 2013 donde lleva a cabo el registro de llamadas, conferencias y transferencias realizadas por las extensiones. También se localizó la tabla donde estan todas las extensiones dadas de alta, así como la tabla que tiene el registro de las diferentes coberturas para asignar a las extensiones.

Por parte de la facturación del proveedor, se identificó el cómo realiza el cobro de cada tipo de llamada, llegando a la siguinte resolución:

- Locales: tiene una tárifa por evento independiente de la duración de la misma.
- Larga distancia nacional: tiene una tárifa por duración de la llamada, la cual es superior a una llamada local, se cobra por minuto.
- Celulares: tiene dos tárifas, el primer minuto se cobra como llamada local más la tárifa establecida para llamadas a celular; sí la llamada supera el minuto, se suma ya sólo la tárifa de llamada a celular por minuto subsecuente.
- Internacionales, Centroamérica y el Caribe, Sudamérica, Europa y resto del mundo tienen una tárifa distinta cada una y es única para cada tipo de llamadas, se cobra por minuto.

Identificada esta información, se desarrolló y implementó el tarificador complementario en una máquina virtual en VirtualBox, con sistema operativo Debian 9. Adicional se le instalaron Apache, PHP y MariaDB. En las bases de datos SQL Server de los Back End se creó un usuario local con permisos de consultas a la base de datos y tablas que se utilizaron para el tarificador, como se muestra en la imagen 17.

Se programaron los querys en la base de datos con las tablas y campos de las mismas para obtener la información de cdr’s, llamadas por usuaurios, por región, por rango de fechas y horas; contemplando horario de verano. Se desarrolló el ambiente web con HTML y hojas de estilo, así como los scripts en PHP para poder llevar a cabo la ejecución de consultas dinámicas a la base de datos con ciertos parámetros como filtros para obtener la información requerida, como son extensión, usuario de dominio, fechas y horario. Para la autenticación al nuevo sistema de tarificación, se desarrolló un script para validar la información de los usuarios con sus cuentas de domino, para ello se realizo una relación de confianza entre los servidores de dominio y el nuevo servidor virtual del tarificador.

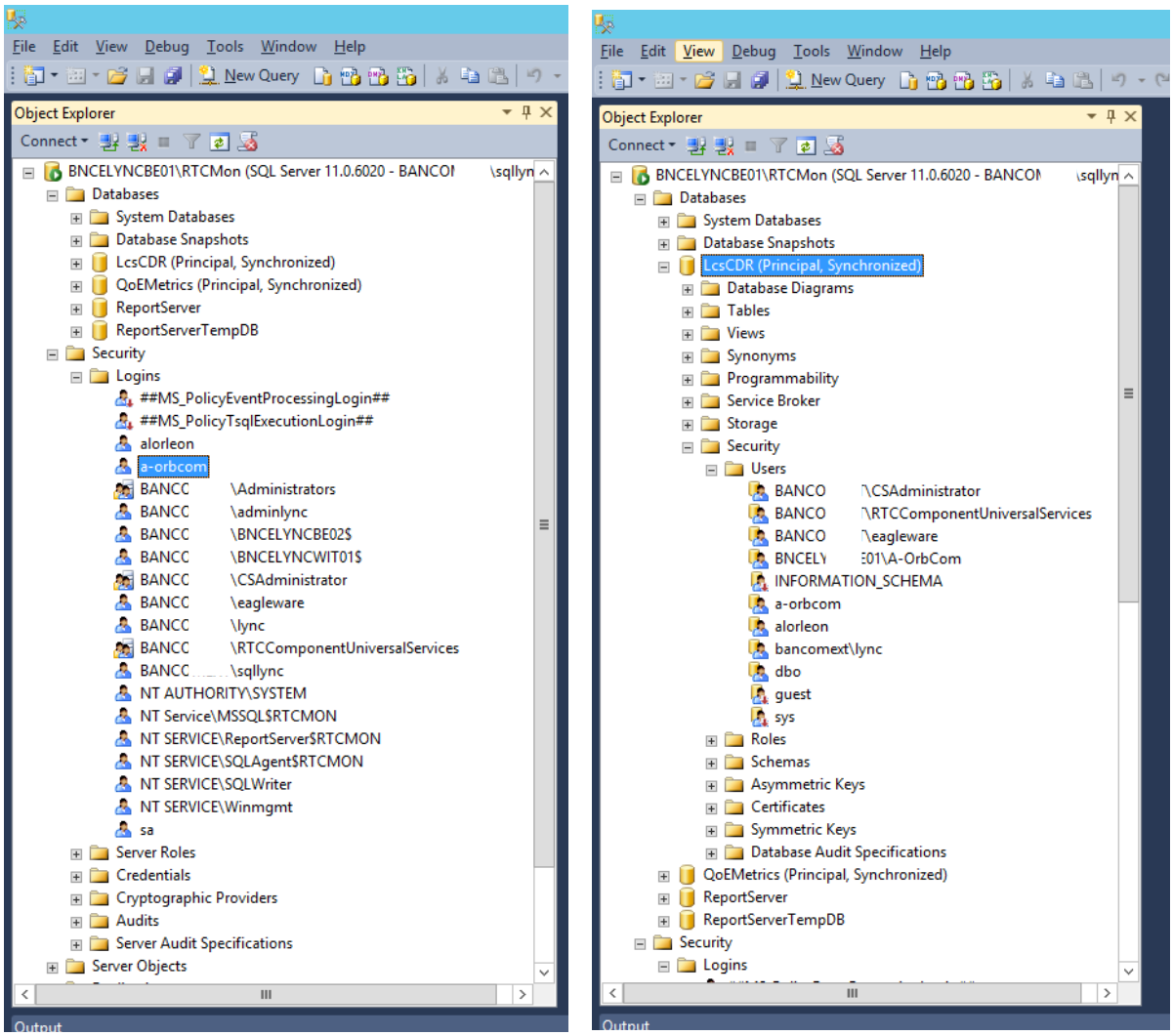
Para obtener la información de todos los tipos de llamadas que se presenta en el tarificador complementario, en sus diferentes reportes, llamadas entre extensiones y a la red telefónica, se contemplaron las tablas de la base LcsCDR como son:

- dbo.SessionDetails: en esta tabla estan todos los registros de llamadas y transferencias ya sean internas o externas que se realizan mediante un equipo telefónico o por el cliente de Lync o Skype for Business.

- dbo.Users: contiene información de las extensiones asignadas a los usuarios de dominio del Banco.

- dbo.TimeZoneConfiguration: contiene el inicio y fin del horario de verano por año y por país.

- dbo.Conferences: aquí se registran todas las llamadas, interna o externas que se unen a una conferencia.



Imagne 17: Configuración de usuario local para consultas a la base de datos SQL Server en los servidores Back End

Los usuarios del sistema de tarificación complementario, que son todos aquellos que tienen cuenta en los servidores del dominio del Banco, se tienen que autenticar con su cuenta de dominio institucional, la cual es validada con los servicios de dominio del Banco para permitir su ingreso. Posteriormente el sistema valida si el usuario que ingreso tiene permisos sólo para consultar sus llamadas o cuenta con permisos para consultar las llamadas de cualquier usuario. La interfaces de acceso al tarificador complementario se muestra en la imagen 18.

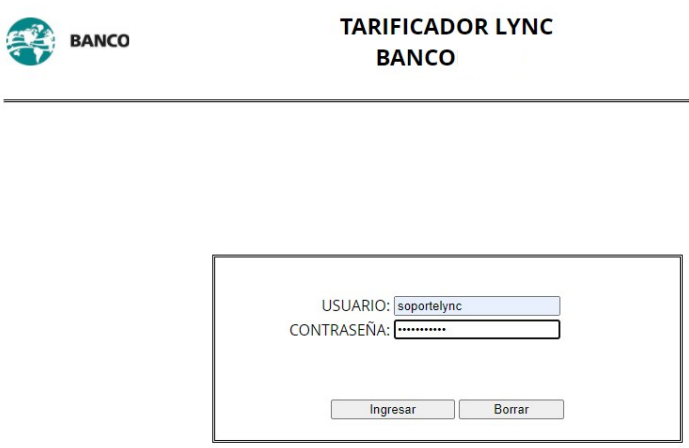


Imagen 18: Logeo de usuarios a sistema de tarificación complementario por medio de cuentas de dominio

Los reportes que entrega el sistema de tarificación complementario muestran los registros de llamadas de los usuarios correspondientes al día de consulta, incluye filtros para poder consultar información puntual de llamadas tanto por usuarios, extensión, fecha y hora, distintos al día de la consulta.

El primer módulo de consultas es un cdr con todas las llamadas realizadas del día en curso o de algún rango de fechas definido por el usuario. Este reporte contiene llamadas entre extensiones, llamadas de y hacia la red pública; con fecha y hora de inicio y fin de la misma, duración y estatus de las llamadas. Tiene la opción para exportar a formato pdf para su uso fuera del sistema, como se muestra en las imágenes 19a y 19b.

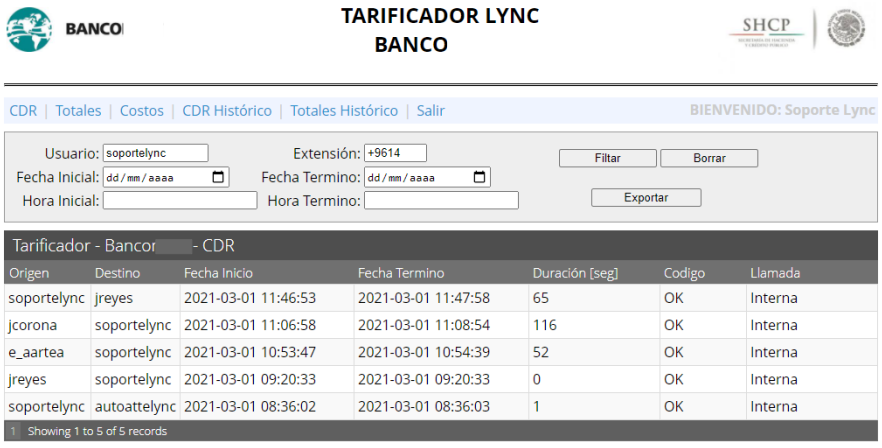
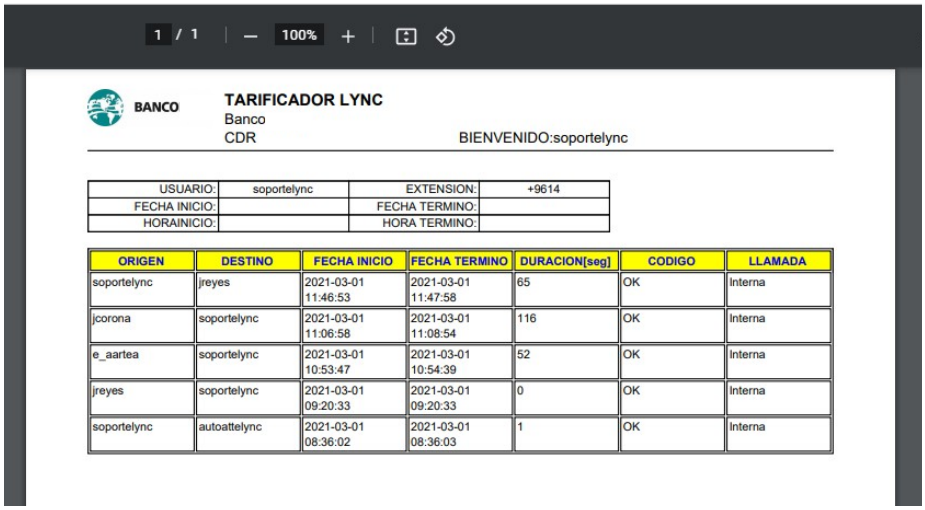


Imagen 19a: Reporte web de llamadas CDR



BANCO

TARIFICADOR LYNC
Banco
CDR

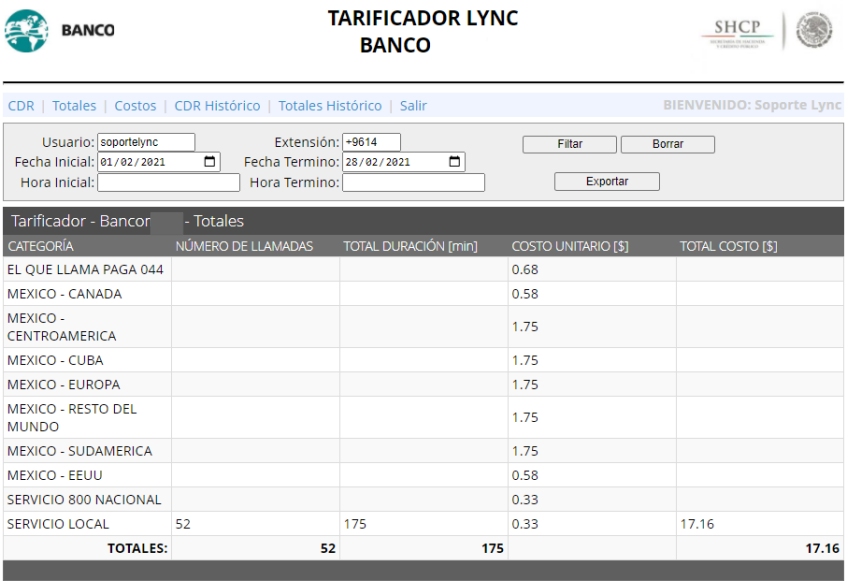
BIENVENIDO:soportelync

USUARIO:	soportelync	EXTENSION:	+9614
FECHA INICIO:		FECHA TERMINO:	
HORAINICIO:		HORA TERMINO:	

ORIGEN	DESTINO	FECHA INICIO	FECHA TERMINO	DURACION[seg]	CODIGO	LLAMADA
soportelync	jreyes	2021-03-01 11:46:53	2021-03-01 11:47:58	65	OK	Interna
jcorona	soportelync	2021-03-01 11:06:58	2021-03-01 11:08:54	116	OK	Interna
e_aartea	soportelync	2021-03-01 10:53:47	2021-03-01 10:54:39	52	OK	Interna
jreyes	soportelync	2021-03-01 09:20:33	2021-03-01 09:20:33	0	OK	Interna
soportelync	autoattelync	2021-03-01 08:36:02	2021-03-01 08:36:03	1	OK	Interna

Imagen 19b: Reporte pdf de llamadas CDR

En un segundo módulo, se tiene la sección de reporte totales, la cual presenta un reporte de todas las llamadas realizadas ya sea por usuarios o globalmente del Banco, agrupadas por región y tipo de llamada. Este reporte permite al área de finanzas validar la factura que su proveedor le entrega mensualmente por el cobro del servicio. Compara este reporte con la factura para poder realizar el pago correcto por el servicio, las discrepancias que llegaran a darse entre el reporte y la factura ya se resuelven entre las áreas correspondientes, el reporte que presenta el sistema se puede observar en la imagen 20a, su versión en pdf en la imagen 20b.



BANCO

TARIFICADOR LYNC
BANCO

SHCP

CDR | Totales | Costos | CDR Histórico | Totales Histórico | Salir

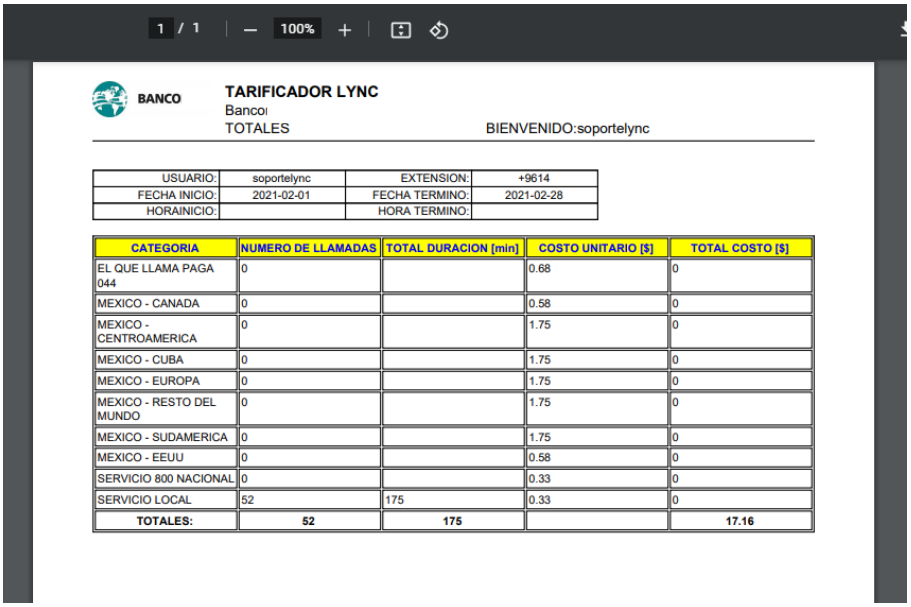
BIENVENIDO: Soporte Lync

Usuario: soportelync Extensión: +9614 Filtar Borrar
Fecha Inicial: 01/02/2021 Fecha Termino: 28/02/2021
Hora Inicial: Hora Termino: Exportar

Tarificador - Bancor - Totales

CATEGORÍA	NÚMERO DE LLAMADAS	TOTAL DURACIÓN [min]	COSTO UNITARIO [$]	TOTAL COSTO [$]
EL QUE LLAMA PAGA 044			0.68	
MEXICO - CANADA			0.58	
MEXICO - CENTROAMERICA			1.75	
MEXICO - CUBA			1.75	
MEXICO - EUROPA			1.75	
MEXICO - RESTO DEL MUNDO			1.75	
MEXICO - SUDAMERICA			1.75	
MEXICO - EEUU			0.58	
SERVICIO 800 NACIONAL			0.33	
SERVICIO LOCAL	52	175	0.33	17.16
TOTALES:	**52**	**175**		**17.16**

Imagen 20a: Reporte web de totales llamadas



BANCO

TARIFICADOR LYNC
Banco
TOTALES BIENVENIDO:soportelync

USUARIO:	soportelync	EXTENSIÓN:	+9614
FECHA INICIO:	2021-02-01	FECHA TERMINO:	2021-02-28
HORAINICIO:		HORA TERMINO:	

CATEGORIA	NUMERO DE LLAMADAS	TOTAL DURACION [min]	COSTO UNITARIO [$]	TOTAL COSTO [$]
EL QUE LLAMA PAGA 044	0		0.68	0
MEXICO - CANADA	0		0.58	0
MEXICO - CENTROAMERICA	0		1.75	0
MEXICO - CUBA	0		1.75	0
MEXICO - EUROPA	0		1.75	0
MEXICO - RESTO DEL MUNDO	0		1.75	0
MEXICO - SUDAMERICA	0		1.75	0
MEXICO - EEUU	0		0.58	0
SERVICIO 800 NACIONAL	0		0.33	0
SERVICIO LOCAL	52	175	0.33	0
TOTALES:	**52**	**175**		**17.16**

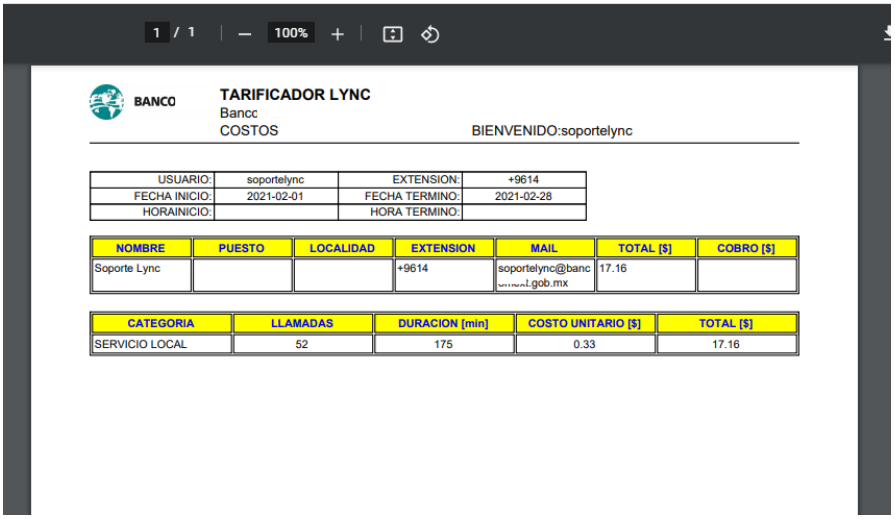
Imagen 20b: Reporte pdf de total de llamadas

En un tercer módulo se tiene la opción de consultar el detalle de llamadas por usuario y por rubro de llamadas, esta opción permite al área de recursos humanos contabilizar las llamadas de los usuarios y catalogarlas como de trabajo o personales para posteriormente realizar un posible cobro, por el área de finanzas, a los usuarios por el uso del servicio.

Para poder llevar a cabo el cobro, el área de finanzas estableció con base en un análisis, un tope en pesos por el consumo de servicio telefónico por usuario. Si el usuario rebasa ese margen, entonces en el reporte presenta un mensaje indicando que el usuario a sobrepasado el tope de saldo para llamadas y debe de catalogarlas por llamadas personales o de trabajo.

El área de recursos humanos envía una notificación vía mail al usuario para que ingrese al sistema y valué sus llamadas. Cuando el usuario ingresa y valida el periodo indicado por recursos humanos, el sistema le presenta una primer opción de posible categoría, la cual el usuario puede ir modificando con base al conocimiento de dichas llamadas. El reporte que el sistema entrega se muestra en las imágenes 21a y 21b.

Imagen 21a: Reporte web de costo de llamadas



BANCO

TARIFICADOR LYNC
Bancc
COSTOS

BIENVENIDO:soportelync

USUARIO:	soportelync	EXTENSION:	+9614
FECHA INICIO:	2021-02-01	FECHA TERMINO:	2021-02-28
HORAINICIO:		HORA TERMINO:	

NOMBRE	PUESTO	LOCALIDAD	EXTENSION	MAIL	TOTAL [$]	COBRO [$]
Soporte Lync			+9614	soportelync@banc	17.16	

CATEGORIA	LLAMADAS	DURACION [min]	COSTO UNITARIO [$]	TOTAL [$]
SERVICIO LOCAL	52	175	0.33	17.16

Imagen 21b: Reporte pdf de costo de llamadas

Para cumplir completamente con el tarificador, dentro de la licitación que ganó el Consorcio, éste debe ser capas de almacenar y poder reportar cdr's históricos del 2011 al 2015 que contenía la solución previa a la nuestra. Se analiza la información contenida en dichos cdr's y la mejor forma de cumplir con este punto es desarrollar dentro del tarificador complementario, una pequeña base de datos con sólo una tabla que contenga toda la información de los archivos proporcionados por el Banco.

En la máquina virtual del tarificador complementario se instala e implementa una base de datos en MaríaDB, con una tabla con varios campos; se crean sus respectivos índices y llaves para una optima funcionalidad. De dicha tabla se genera una vista, se muestra en la imagen 22, con los campos que se utilizaran en los diferentes tipos de consulta. Se replica las opciones de consulta con ésta información, se desarrollan los reportes de cdr geneneral, totales y de costos similares a los reportes entregados con la información que se almacena en Lync Server 2013, se presenta un ejemplo de los reportes históricos en la imagen 23a y 23b.

```
MariaDB [cdr_backup]> describe cdr_historico;
+--------------+-------------+------+-----+---------+-------+
| Field        | Type        | Null | Key | Default | Extra |
+--------------+-------------+------+-----+---------+-------+
| PhoneOrigen  | varchar(50) | YES  |     | NULL    |       |
| PhoneDestino | varchar(50) | YES  |     | NULL    |       |
| DateInicio   | datetime    | YES  |     | NULL    |       |
| DateTermino  | datetime    | YES  |     | NULL    |       |
| Duracion     | int(11)     | YES  |     | NULL    |       |
| Codigo       | varchar(9)  | YES  |     | NULL    |       |
| TypeCall     | varchar(11) | YES  |     | NULL    |       |
+--------------+-------------+------+-----+---------+-------+
7 rows in set (0.00 sec)

MariaDB [cdr_backup]>
```

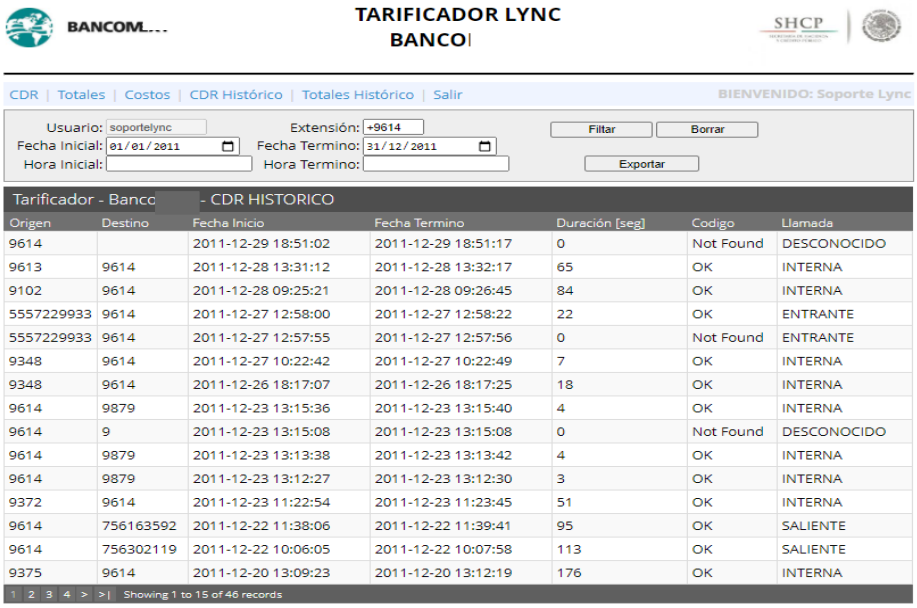
Imagen 22: Vista de tabla global con campos usados para reportes de históricos

Con este desarrollo, el Consorcio logró cumplir en tiempo y forma con lo requerido en la licitación y evitarse penalizaciones económicas fuertes. Afianzando la confianza y relación con su cliente, el Banco, y abriendo la puerta a posibles requeriminetos nuevos para continuar su relación de negocios.

Por su parte el Banco logró contar con un sistema robusto en tema de tarificación de llamadas, tanto contando con los reportes básicos, con el sistema Eagleware inicial, que son cdr's, las 10 y 20 llamadas con mayor duración, los números más marcados entre otros.

Por parte del tarificador complementario cuenta con reportes tipo facturación idénticos como los entrega su proveedor de telefonía, que le permiten validar sus pagos correctamente. Evaluación y cobro de llamadas personales y de trabajo por parte de sus usuarios, así tanto el área de recursos humanos y finanzas como el propio usuario pueden estar de acuerdo al momento de llegar a algún tema de aclaración por el uso del servicio telefónico; además permite a dichas áreas realizar un último corte antes de que el usuario pierda su relación laboral con el Banco.

La recuperación económica por el concepto de catalogar y cobrar las llamadas personales es mínimo, pero esto a permitido reducir en un 10% el total del pago de la factura por servicios de telefonía


TARIFICADOR LYNC
BANCO

CDR | Totales | Costos | CDR Histórico | Totales Histórico | Salir — BIENVENIDO: Soporte Lync

Usuario: soportelync Extensión: +9614 Filtar Borrar
Fecha Inicial: 01/01/2011 Fecha Termino: 31/12/2011
Hora Inicial: Hora Termino: Exportar

Tarificador - Banco - CDR HISTORICO

Origen	Destino	Fecha Inicio	Fecha Termino	Duración [seg]	Codigo	Llamada
9614		2011-12-29 18:51:02	2011-12-29 18:51:17	0	Not Found	DESCONOCIDO
9613	9614	2011-12-28 13:31:12	2011-12-28 13:32:17	65	OK	INTERNA
9102	9614	2011-12-28 09:25:21	2011-12-28 09:26:45	84	OK	INTERNA
5557229933	9614	2011-12-27 12:58:00	2011-12-27 12:58:22	22	OK	ENTRANTE
5557229933	9614	2011-12-27 12:57:55	2011-12-27 12:57:56	0	Not Found	ENTRANTE
9348	9614	2011-12-27 10:22:42	2011-12-27 10:22:49	7	OK	INTERNA
9348	9614	2011-12-26 18:17:07	2011-12-26 18:17:25	18	OK	INTERNA
9614	9879	2011-12-23 13:15:36	2011-12-23 13:15:40	4	OK	INTERNA
9614	9	2011-12-23 13:15:08	2011-12-23 13:15:08	0	Not Found	DESCONOCIDO
9614	9879	2011-12-23 13:13:38	2011-12-23 13:13:42	4	OK	INTERNA
9614	9879	2011-12-23 13:12:27	2011-12-23 13:12:30	3	OK	INTERNA
9372	9614	2011-12-23 11:22:54	2011-12-23 11:23:45	51	OK	INTERNA
9614	756163592	2011-12-22 11:38:06	2011-12-22 11:39:41	95	OK	SALIENTE
9614	756302119	2011-12-22 10:06:05	2011-12-22 10:07:58	113	OK	SALIENTE
9375	9614	2011-12-20 13:09:23	2011-12-20 13:12:19	176	OK	INTERNA

1 2 3 4 > >| Showing 1 to 15 of 46 records

Imagen 23a: Reporte web de cdr histórico en tarificador complementario


TARIFICADOR LYNC
Banco
CDR HISTORICO BIENVENIDO:soportelync

USUARIO:		EXTENSION:	9614
FECHA INICIO:	2011-01-01	FECHA TERMINO:	2011-12-31
HORAINICIO:		HORA TERMINO:	

ORIGEN	DESTINO	FECHA INICIO	FECHA TERMINO	DURACION[seg]	CODIGO	LLAMADA
9614		2011-12-29 18:51:02	2011-12-29 18:51:17	0	Not Found	DESCONOCIDO
9613	9614	2011-12-28 13:31:12	2011-12-28 13:32:17	65	OK	INTERNA
9102	9614	2011-12-28 09:25:21	2011-12-28 09:26:45	84	OK	INTERNA
5557229933	9614	2011-12-27 12:58:00	2011-12-27 12:58:22	22	OK	ENTRANTE
5557229933	9614	2011-12-27 12:57:55	2011-12-27 12:57:56	0	Not Found	ENTRANTE
9348	9614	2011-12-27 10:22:42	2011-12-27 10:22:49	7	OK	INTERNA
9348	9614	2011-12-26 18:17:07	2011-12-26 18:17:25	18	OK	INTERNA
9614	9879	2011-12-23 13:15:36	2011-12-23 13:15:40	4	OK	INTERNA
9614	9	2011-12-23 13:15:08	2011-12-23 13:15:08	0	Not Found	DESCONOCIDO
9614	9879	2011-12-23 13:13:38	2011-12-23 13:13:42	4	OK	INTERNA
9614	9879	2011-12-23 13:12:27	2011-12-23 13:12:30	3	OK	INTERNA

Imagen 23b: Reporte pdf de cdr histórico en tarificador complementario

Actividad IV
Lync Server 2013 – Home Office

A finales de 2019 surge una nueva sepa de la COVID y se propaga por todo el mundo, en general, en el 2020, vivimos la pandemia más fuerte por la COVID-19 de los últimos tiempos y México no es la excepción; debido a esta situación y como todas las dependencias gubernamentales y privadas del país, los empleados son enviados a resguardarse en sus casas y trabajar desde ahí para tratar de minimizar el impacto de dicha pandemia y mantener las operaciones de las empresas.

Dos de las funcionalidades importantes de la solución on premises de Lync Server 2013 implementada en el Banco son el uso del servicio de redes externas a la institución y la movilidad de las extensiones dadas de alta en su platafoma; tanto en sus instalaciones como en sitios externos con conexión a internet, la casa de un usuario por ejemplo; un empleado puede hacer uso de todos los servcios de Lync Server 2013 como si estuviera en su lugar de trabajo. Esta característica de Lync fue considera cuando se optó por esta solución, pero únicamente se contempló un 20 a un 30 por ciento de la cantidad total de usuarios para que hicieran uso de ésta funcionalidad.

Cuando se puso en producción Lync Server 2013 se realizaron pruebas de:

- Red externa: al habilitar esta característica de la extensión en la consola de Lync Server 2013, imagen 24; el cliente de Lync o Skype for Bussines instalado en un equipo de cómputo institucional o personal (únicamente si se instala previamente un certificado de seguridad proporcionado por el Banco en el equipo), puede conectarse desde un servicio de internet externo a la red LAN del Banco; logeandose con su cuenta de dominio institucional pueden hacer uso de todas las funcionalidades disponibles. Se conservan todas la características de una extensión como si estuviera en el Banco, puede llamar a otras extensiones, recibir llamadas de la PSTN que entran al IVR del Banco y son desviadas a una extensión, puede el usuario hacer llamadas externas hacia la red pública con base en la cobertura asignada en su configuración.

- Movilidad: cuando se habilita esta característica de Lync Server 2013 en la extensión, imagen 24, el usuario puede tener instalado el cliente de Skype for Business en su celular o tablet de cualquier fabricante, como se muestra en la imagen 25, y con su cuenta de dominio del Banco, poder logearse y acceder a todas las funciones que Lync ofrece como si estuviera en su lugar de trabajo.

En un inicio sólo se contemplo al personal que podría estar en riesgo por al nueva enfermedad y se les habilito y configuro en sus equipos y dispositivos la funcionalidad de política externa y movilidad para que laboraran desde sus casas. Pero conforme fueron pasando los días, se requirió que más usuarios fueran habilitados con estas funcionalidades, lo cual nos llevo a tener un escenario con mas del 95 por ciento de los empleados del banco con estas opciones habilitadas, esto sucedió cuando se declaro en los mese de abril o mayo de 2020 el semaforo rojo en todo el país debido a la pandemia or COVID-19.

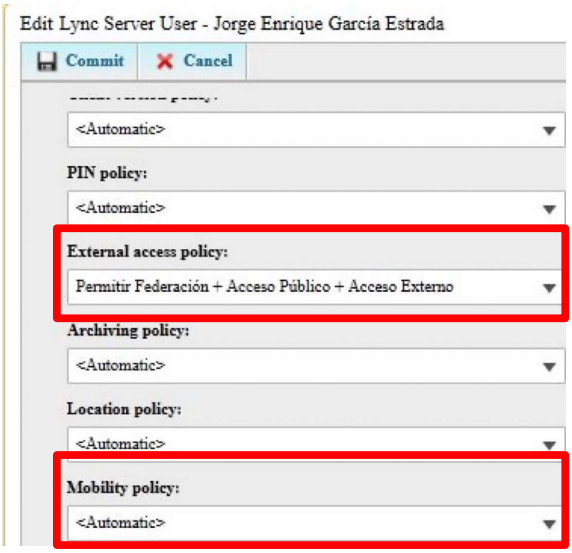


Imagen 24: Ejemplo de configuración de acceso externo y movilidad para extensión

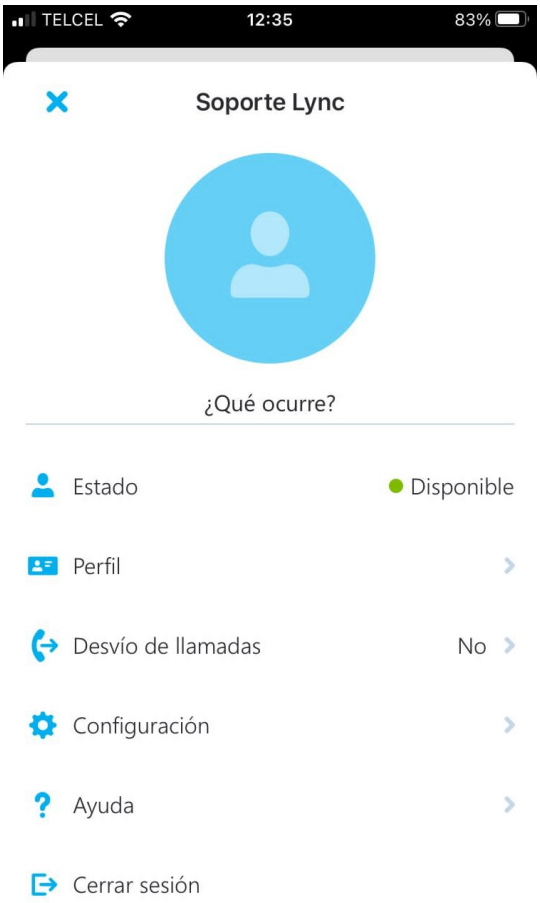


Imagen 25: Usuario Soporte Lync habilitado para conectarse mediante dispositivo móvil fuera de la red del Banco

Esto nos llevó a un escenario donde la conectividad al servicio de Lync Server comenzó a tener algunas dificultades, tanto por la capacidad de procesamiento de los servidores como por el ancho de banda del servicio de internet del propio Banco. Algunos servidores de la solución comenzaron a fallar debido a la alta demanda de recurso informáticos.

Dentro de las fallas que afrontamos fue que los servidores presentaron daños físicos de hardware tanto en baterías de alimentación de la tarjeta controladora de discos duros, así como daños fisicos de las tarjetas motherboard.

El Consorcio adquirió el hardware necesario para solventar las fallas que ibamos presentado y además adquirió refacciones para tener en stock en caso de futuras eventualidades. Además se renovó el soporte con los fabricantes de los servidores que conforman la solución de Lync Server 2013 para estar lo más respaldados en caso de una falla grave en días de mayor demanda de los servicios.

La respuesta ante estas problematicas operativas por nuestra parte fue correcta y el impacto en la afectación del servicio se minimizaron. Como área crítica del Banco, desde que inicio la pandemia a la fecha hemos laborado de manera normal; siempre siguiendo las recomendaciones de higiene establecidad por la Secretaria de Salud.

El soporte brindado para los usuarios ha sido tanto físicamente, en su mayoría cuando en Marzo de 2020 comendaron a enviar a laborar a casa a la población mas vulnerable, y remotamente ya con la contingencia sanitaria en su máximo nivel. En las fechas más recientes, inicios del año 2021, poco a poco se vuelven a retomar las labores presenciales, pero de manera controlada y escalonada, lo cual nos lleva a pensar en una nueva normalidad y modalidad de laborar en el Banco.

Hace ya algunos años, que el contrato que comprende la licitación hecha en 2015 finalizó y el Banco comenzó a buscar nuevas tecnologías tanto para su red corporativa como para los servicios unificados, lamentablente por el tema de la austeridad gubernamental; se han visto frenados para llevar a cabo dicha renovación de infraestructura.

Por lo que como parte del Consorcio continuamos manteniendo en operación toda la solución existente, pero ya los equipos estan llegando a su tiempo de vida útil, o ya lo superaron; tanto de software como hardware. Esto nos esta ocasionado varios retos en cuestión de refacciones o de cambio de equipos completos, debido a que los fabricantes ya no los producen. Por lo que se busca muchas veces equipos de segunda mano, ya sea para refacciones o para remplazo completo.

La pandemia ha traido varios retos al Banco, tanto de servicios de comunicaciones y conectividad para que sus empleados puedan laborar desde sus casas como la cultura del trabajo en casa. Al inicio se tenía la incertidumbre que los usuarios realmente cumplieran con sus labores, dado que el Banco invirtió en infraestructura para facilitar y brindar la conectividad remota a sus servicios financieros y además en robustecer su área de seguridad informática para previnir y evitar posibles ciberataques ya que varios sistemas que originalmente fueron pensados para estar de forma local, ahora estaban expuestos a internet o se tenía acceso a ellos mediante su VPN corporativa.

El personal del Banco a demostrado que puede realizar sus funciones y tareas labores desde sus casas o en la ubicación donde esten con acceso a internet, dejo a un lado el temor que los directivos tenían referente a este tema. Por su parte, en cuestión de infraestrucura y servicios de comunicaciones el Banco cumple y entrega a sus usuarios para que no interrumpan sus labores y puedan realizarlas como si estuvieran en su lugar de trabajo.

Conclusiones

Los retos a los que una institución financiera se enfrenta son varios, desde la selección de su infrestructura TI, la cual debe cubrir sus necesidades operativas y estar preparada para los retos que su entorne le presentan, hasta el contar con la mejor ciberseguridad para protegerse de las amenazas cibernéticas que día a día se presentan en el ambiente global.

El aprendizaje que me ha brindado el coordinar y estar involucrado en todo el proceso de la migración de un centro de datos fue enorme. Conocer la logística que conlleva la planeación y ejecución del mismo, así como los factores internos propios la institución y externos, sismos de 2017; que se van presentando durante el proceso; me permitió conocerme en ambientes no controlados y adaptarme a las circunstancias de la mejor forma para salir adelante.

Se cumplió con las recomendaciones hechas por la auditoría de Banxico para el centro de datos y ahora el Banco busca ampliar su gama se servicos con dicha institución, el centro de datos ya no es limitante para logralo; ahora se realizan mejoras a nivel configuración en la infraestructura para dar cumplimiento y lograr los objetivo que se plantean.

Despertó en mí el interés en ver que otras opciones hay en el tema de los centros de datos. Estos están evolucionando y empieza a manejarse la posibilidad de no tener toda la infraestructura y sistemas corporativos on premise, y se propone la alternativa de contar con un centros de datos híbridos, una parte en el centro de datos de la empresa y otra parte en la nube. Para entender mejor esto, comencé a involucrarme en tecnologías cloud como Amazon Web Services, AWS, como se puede ver en la imagen 26.

El Banco ya comenzó a platearse dicha opción de un centro de datos híbrido y en primer instancia su DRP cuenta con algunos servicios en la nube de AWS, en donde he participado en la migración de los mismo. Con estas acciones el Banco piensa en un futuro tener todo su DRP en la nube para en caso de una incidencia en sus sistemas e/o infraestructura centra; ya sea limitante para continuar con sus tareas financieras básicas y así pueda actuar de inmediato y no perder tiempo para continuar operando. Aún hay muchas cosas que realizar pero ya iniciamos.

Imagen 26: Certificado – Alberto Lorenzo

En el tema de la ciberseguridad, después de la experiencia vivida el Banco a implementado nuevos lineamientos y políticas en varios rubros en su infraestructura; adquiriendo algún tipo de solución y en otros casos sólo probandola temporalmente. Por mi parte, como administrador de toda la solución de red, me he capacitado en temas de ciberseguridad y ethical hacking, como se ilustra en las imagenes 27 y 28; para poder ser un recurso humano que aporte un valor agregado a la institución para prevenir y actuar de mejor forma durante alguna nueva amenza de seguridad informática.

A la fecha el área de seguridad infórmatica del Banco ha solventado todas las ciberamenazas en la infraestrucutura. Además, estamos registrados en boletines informativos de varios provedores de hardware y sofware en este campo, los cuales nos han ayudado mucho; realizamos análisis de vulnerabilidades a los servidores y sistemas constantemente y validamos con los boletines si tenemos algún riesgo y actuamos en caso de tener para prevenir.

Imagen 27: Constancia de Introducción a la Ciberseguridad

Imagen 28: Certificado de Ethical Hacking

La solución de Lync Server 2013, pese a ya estar fuera de soporte por el fabricante y de haber evoluciona primero a Skype for Business y por último a Teams, sigue siendo una solución robusta para tema de comunicaciones unificadas. Si además tomamos en cuenta que los servidores empleados de igual forma se encuentran en un estado similar, donde ya su tiempo de vida operativa esta por terminar o ya concluyo, debido igual a que el fabricante ya no produce estos equipos, y es un poco complicado adquirir refacciones nuevas.

El Consorcio ha hecho todo lo posible para continuar dando soporte y manteniendo operativa la solución. Los factores gubernamentales, dado que el banco es una dependencia descentralizada del gobierno federal, no ha permitido renovar nada en términos de soluciones de TI. Se mantiene operando con sistemas desde el 2015 o 2016. Pero en el mejor estado funcional posible para cumplir totalmente con sus funciones financiera. Lync Server 2013 ha permitido al Banco poder trabajar remotamente desde inicios de la pandemia de COVID 19 hasta hoy, Octubre 2021.

Por último, aprovechando mis conocimientos en programación logre apoyar al Consorcio para desarrollar un sistema de tarificación con ayuda de un sistema de virtualización, Linux, Apache, PHP y MariaDB. Hacer de cierto modo un tipo ingeniería inversa para ver como Lync Server 2013 registra las llamadas y lograr obtener un sistema de reporteo a la medida de las necesidades del Banco fue un gran logro. Este sistema permite hoy al Banco poder cubrir con diferentes requerimientos administrativos.

Al momento que un empleado se deslinda laboralmente de la institución, debe realizar un ajuste para clasificar sus llamadas como personales o laborales antes de su salida. Por lo regular, casi todas las llamadas son catalogadas por los empleados como llamadas laborales y la recaudación económica por este concepto es mínima. Pero se ha visto reflejado en el total de la factura una reducción en la cantidad a pagar.

El 2020 trajo un gran cambio en el aspecto laboral y un gran reto en el tema de infraestructura para el Banco. Día a día nos enfrentamos a temas como el de que la infraestructura de cierta forma es un poco obsoleta, desde el 2015 esté operando; y va presentando fallas. Se hace el mejor esfuerzo para mantenerla operando correctamente. El Banco cubre complemente sus funciones y nosotros vamos aprendiendo cada día más nuevas opciones tanto propietarias como open sorce para lograr nuestro trabajo.

Bibliografía

- ANEXO 2 – Propuesta Técnica BANCO, México 7 de diciembre de 2015.
- Gartner. (2015). Securing the Next-Generation Data Center with Software-Defined Security https://www.gartner.com/smarterwithgartner/securing-the-next-generation-data-center-with-software-defined-security/
- Harvard Business Review. (2009). The Disappearing Data Center. https://hbr.org/2009/07/the-disappearing-data-center
- KIO Networks (Agosto 1, 2019). Harvard Business Review. (2009). The Disappearing Data Center. https://hbr.org/2009/07/the-disappearing-data-center
- CISCO. https://www.cisco.com/c/es_mx/solutions/security/secure-data-center-solution/index.html
- CISCO Networking Academy https://www.netacad.com/es
- MTNET. https://www.mtnet.com.mx/estandares-internacionales-para-el-diseno-de-centros-de-datos/
- © Microsoft 2021. https://docs.microsoft.com/en-us/previous-versions/office/lync-server-2013/microsoft-lync-server-2013 https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms130214(v=sql.105)
- ORACLE VirtualBox. https://www.virtualbox.org/
- Debian. https://www.debian.org/index.es.html
- PHP. https://www.php.net/
- MariaDB Foundation. https://mariadb.org/
- Python. https://www.python.org/
- Seguridad Cero. https://www.seguridadcero.com.pe/
- Proyecto Aurora. https://www.proyecto-aurora.org
- NETEC. https://www.netec.com/
- AWS. https://aws.amazon.com
- RED HAT: https://www.redhat.com/es/topics/open-source/what-is-open-source
- MS SQL SERVER: https://www.microsoft.com/es-mx/sql-server/
- MySQL-MariaDB: https://mariadb.com
- Python: https://www.netacad.com/es/courses/programming/pcap-programming-essentials-python