cisco Meraki

Servicios de Gobierno Definidos por Software y la nueva Arquitectura de Servicios Administrados para ITC del Gobierno

1 Introducción

Por décadas los administadores de la infraestructura de comunicaciones y tecnologías de información (TIC) de las Dependencias de la Administración Pública Federal han adquirido a través de complejas licitaciones servicios de conectividad privada entre sus oficinas centrales y remotas, enlaces a Internet, así como infraestructura de red alámbrica e inalámbrica, telefonía y un sinnúmero de componentes tecnológicos para poder soportar las operaciones del Gobierno.

En años recientes, los procesos de adquisición cambiaron a concursar servicios administrados por un periodo de tiempo determinado en la licitación (tres años, por ejemplo); si bien esta modalidad ha ayudado a los administradores de TIC a enfocarse en soportar las plataformas y tecnologías para brindar servicios a los Ciudadanos y a los empleados del Gobierno, los anexos técnicos del proceso de licitación siguen estando enfocados en describir caracterísiticas de los componentes tecnológicos, generando rigidez e incapacidad para desplegar nuevos servicios y capacidades que la ola tecnológica genera durante la vida del contrato.

En la actualidad, cada vez son más los servicios que los Ciudadanos y los Empleados de Gobierno demandan se encuentren en línea, generando dinámicas de digitalización de los actuales procesos, provocando el que veamos cada día más y nuevos servicios de Gobierno Digital.

Estos servicios de Gobierno Digital (Government Digitization) requieren estar siempre en línea, accedidos vía red privada e Internet, a través de aplicaciones móviles, con contenidos de imagenes y video, pero sobre todo, deben ser desplegados de manera ágil y contar con la flexibilidad para ajustarse a las condiciones y requerimientos variables que se demandan. Bajo los procesos de digitalización gubernamental, los empleados de Gobierno, pero sobre todo los Ciudadanos, no pueden esperar a los “tiempos de TI” cómo sucedía en el pasado.

En el plano tecnológico, se ha evolucionado de enlaces dedicados a enlaces privados virtuales basados en MPLS, y en años recientes a la evolución de habilitación de redes virtuales, superpuestas y definidas por software (SD-WAN). Esta última, SD-WAN, ha dejado de ser un conjunto de tecnologías de laboratorio para pasar a la adopción masiva, tanto por fabricantes de tecnología, operadores de servicios y usuarios.

Todo esto conlleva a la necesidad de tecnologías de conectividad, comunicaciones y cómputo que puedan ser elásticas, es decir que crezcan conforme la demanda del servicio lo requiera, y que ajusten sus capacidades y rendimiento de manera dinámica y automática. Además claro, de los servicios tradicionales (legacy) como acceso a bases de datos, correo electrónico, respaldos y telefonía IP.

En términos de aseguramiento de los servicios, los administradores de TIC del Gobierno pueden expandir la visibilidad de su red no solo a indicadores operativos que miden los niveles de acuerdo de servicios (SLA), integración con mesas de ayuda para la generación automática de tickets y demás integraciones operativas, si no también podrán contar con tableros de control ejecutivos (dashboards) para visualizar los nuevos indicadores de usabilidad que les permitan tener la visibilidad de lo que sucede en los componentes del servicio administrado y medir el impacto de las inversiones realizadas.

Los Servicios de Gobierno Definidos por Software aprovechan las tecnologías de conectividad privada y oferta de Internet de banda ancha disponibles, así como las nuevas tecnologías y plataformas de red elásticas, poderosas pero simples, las cuáles son orquestadas y automatizadas de manera centralizada a través de software que permite generar los servicios de gobierno con tecnología que simplemente funciona.

2 Qué es SD-GS

Los Servicios de Gobierno Definidos por Software (SD-GS) es una Arquitectura que permite habilitar los servicios de comunicaciones y TI de la Administración Pública Federal de una manera simple, automatizada, elástica y con la visibilidad de lo que sucede en los servicios contratados.

Esta Arquitectura cambia los paradigmas de las redes tradicionales, ya que abstrae el software del hardware y envía el plano de control a la Nube, lo que permite la creación de redes superpuestas virtuales (redes overlay) las cuáles son Orquestadas y Gestionadas de manera centralizada y en una sola vista, consolidando en un solo punto de gestión los enlaces, seguridad e infraestructura de red (WAN, LAN, WLAN) de las multiples oficinas remotas de la Dependencia con las oficinas centrales, permitiendo una rápida implementación, optimización de costos de ancho de banda, menor TCO, así como la simplificación de la operación, contando además con visibibilidad y analíticos que permiten proteger los SLAs de los servicios y aplicaciones, así como contar con indicadores de usabilidad para medir el impacto de los servicios contratados.

Los pilares de la Arquitectura son:

Red Virtual Superpuesta
Creación de una red virtual superpuesta (red privada “overlay”)

para uso de la Dependencia de Gobierno, la cuál está sustentada en elementos de conectividad de diferentes características que pueden ser MPLS, Broadband, LTE, Satelital o una combinación de ellas. El Proveedor de Servicios podrá también utilizar enlaces de otros Operadores con la finalidad de complementar la oferta y cobertura del servicio. La Arquitectura de SD-GS crea la Red Virtual Superpuesta (red overlay) sobre estos enlaces de manera automática generando una red privada virtual segura, la cuál habilita los servicios de comunicación e IT de la Dependencia.

Descentralización del Internet

Permite el acceso a Internet de manera directa de la oficina remota, sin necesidad de utilizar el enlace privado para transportar tráfico de Internet a la oficina central. Al permitir que el tráfico de Internet salga a través de cada oficina remota, se genera una descentralización que permite aprovechar los enlaces dedicados para las aplicaciones de IT y comunicaciones de la Dependencia, así como mejorar la experiencia del usuario ya que las velocidades de navegación serán mayores al no haber cuellos de botella en los enlaces de Internet centralizados. La Arquitectura SD-GS permite mantener orquestadas y centralizadas la aplicación de políticas de navegación, restricción de sitios, tráfico por usuario, seguridad, aún y que las salidas a Internet estén descentralizadas en cada oficina.

Selección Inteligente de Enlaces

En oficinas con dos enlaces redundantes (MPLS + Broadband, MPLS + LTE, 2xBroadband, Broadband + LTE, etc), de manera automática se determina el mejor camino basado en parámetros de rendimiento del enlace por aplicación, determinados en los Acuerdos de Nivel del Servicio, tales como: retardo, pérdida de paquetes, jitter, voz (MOS). Los criterios pueden ser establecidos de manera personalizada para cada tipo de aplicación o servicio. La Arquitectura SD-GS orquesta de manera centralizada los algoritmos y criterios de selección, permitiendo la aplicación de políticas incluso por tipo de sitio, región geográfica, tipo de enlaces y tipo de aplicación.

Seguridad Distribuída como Servicio

Habilita elementos de seguridad a los sitios remotos y oficinas centrales tales como: firewall de siguiente generación, prevención de intrusos (IPS), filtrado de contenidos por categoría/url, Geo-based, Anti-malware. La Arquitectura SD-GS crea un servicio overlay de seguridad el cuál permite ejecutar la protección en la frontera de cada sitio remoto/central, pero gestionado y orquestado de manera centralizada, lo que permite tener homologadas la implementación de las reglas y políticas de seguridad en todos los sitios. De ser requerido, la Arquitectura SD-GS provee la flexibilidad de generar políticas por sitio o grupo de sitios, todo orquestado centralmente.

LAN/WLAN como Plataforma

Provee servicios de conectividad de red local de manera alámbrica e inalámbrica a las oficinas centrales y remotas para la conexión de computadoras, dispositivos móviles, teléfonos, videocámaras, sensores, y cualquier tipo de dispositivo que requiera conectividad a los servicios centrales de la Dependencia o bien, a Internet. Este servicio proporciona acceso con tecnologías y funcionalidades homologadas en todos los edificios de la Dependencia, creando una experiencia de uso simple, ubicua y con la movilidad que requieren los usuarios de la Dependencia, así como sus invitados. Al crear diversas redes tales como: red corporativa, red de invitados, red de voz, red de sensores, etcétera, cada una con diferentes mecanismos de autorización y seguridad, se habilita el servicio de conectividad para cada tipo de usuario o dispositivo, proporcionando a cada uno de ellos las recursos, accesos y funcionalidades adecuadas a su perfil. La Arquitectura SD-GS desasocia la infraestructura física y orquesta de manera centralizada los elementos de red necesarios

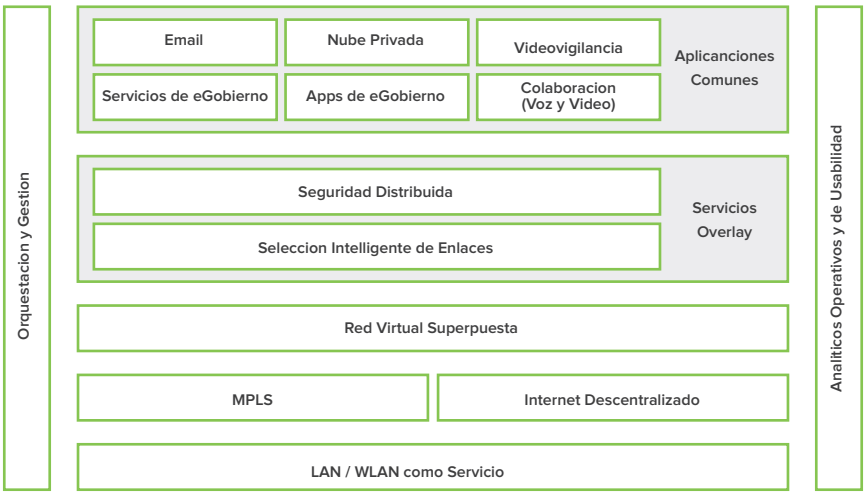

Figura 1. Arquitectura de Servicios de Gobierno Definidos por Software

para habilitar el servicio (switches, APs), lo que permite mantener una homogeneidad de servicios en toda la red de la Dependencia, todos con el mismo nivel de rendimiento, funcionalidades, seguridad, visibilidad y gestión.

Orquestación

Al desasociar el plano de control y crear una instancia central de gestión y orquestación, la Arquitectura SD-GS permite la implementación de infraestructura a través de mecanismos "plug and play", creando un despliegue verdaderamente "Zero Touch" y elástico. Esto permite que los servicios se encuentren disponibles de manera más ágil, minimizando errores en la implementación y generando un menor Costo Total de Propiedad ya que el Operador requiere mucho menor esfuerzo y recursos especializados para desplegar un sitio, o bien, crear adhesiones o reemplazos por reubicación o falla (elasticidad). Además, al mantener de manera centralizada la gestión de todos los componentes habilitadores del servicio, la Arquitectura SD-GS permite la homologación de funcionalidades en toda la red, ya que las configuraciones, cambios de políticas y habilitación de nuevas funcionalidades se realizan una sola vez y son aplicadas de manera automática en todos y cada uno de los elementos de red (gateways, switches, APs).

Analíticos Operativos y de Usabilidad

Con la telemetría generada por los elementos de red, de manera central se consolidan miles de millones de bloques de información que se presentan a través de tableros de control, los cuáles permiten tener visibilidad del comportamiento y rendimiento de cada componente del servicio, de los usuarios y aplicaciones. Esta visibilidad permite medir los Niveles de Servicio contratados, su disponibilidad y planeación de crecimiento, pudiendo incluso integrarse con los sistemas de Mesa de Ayuda del Proveedor del Servicio para que al detectarse una falla del servicio, ya sea por caída o rendimiento, se levanten automáticamente los tickets de soporte necesarios, los cuáles a su vez se verán reflejados en el tablero de control. Adicionalmente, la Arquitectura SD-GS toma los datos de monitoreo y los transforman en Indicadores de Usabilidad, los cuáles se presentan en tableros de control ejecutivos, lo que permite tener visibilidad del uso y aprovechamiento de los servicios contratados, poder medir la experiencia del usuario, de las aplicaciones, así como saber los hábitos de uso y preferencias de los usuarios del servicio.

3 Componentes

La Arquitectura se compone de dos grandes segmentos: Conectividad de la oficina central y oficinas remotas, y servicios de conectividad y comunicaciones al usuario dentro de cada oficina.

3.1 Software Defined WAN

La conectividad de la oficina central y las oficinas remotas es habilitada por la Red Virtual Superpuesta, la cuál genera una red privada segura utilizando diferentes tipos de enlaces los cuáles pueden ser de múltiples tecnologías tales como MPLS, Banda Ancha, LTE, Satelital, etcétera, incluso los enlaces de un mismo sitio pueden ser provistos por diferentes proveedores de servicios, ya que la Red Virtual Superpuesta genera la red privada virtual segura para cada sitio.

Los escenarios de conectividad pueden ser (sin limitarse a):

- MPLS
- Broadband
- Satelital
- MPLS + Broadband
- Broadband + Broadband • Broadband + LTE
- Satelital + LTE

Los enlaces físicos provistos por diferentes tecnologías e incluso proveedores, son consolidados de manera lógica a través de la Red Virtual Superpuesta, la cual crea una red privada virtual entre todas las oficinas de manera automática y segura, que es orquestada y gestionada a través de la Nube con cero líneas de comandos. La RVS además del auto establecimiento de la red privada virtual, permite que la red se ajuste de manera dinámica a los cambios en las condiciones de los enlaces sin la necesidad de intervención manual del administrador de TIC. Al proporcionar control granular de cómo determinado tipo de tráfico responden a los cambios de disponibilidad y rendimiento de los enlaces WAN (latencia, jitter, pérdida de paquetes), la RVS puede garantizar un rendimiento óptimo para aplicaciones críticas y ayudar a evitar interrupciones del tráfico altamente sensible al rendimiento de los enlaces, como lo es la Voz sobre IP.

Una vez que se establece la Red Virtual Superpuesta, su comportamiento a nivel lógico es el de una red privada virtual, por lo que a través de esta red se pueden ejecutar aplicaciones tales como telefonía IP, video, así como acceso a bases de datos y aplicaciones

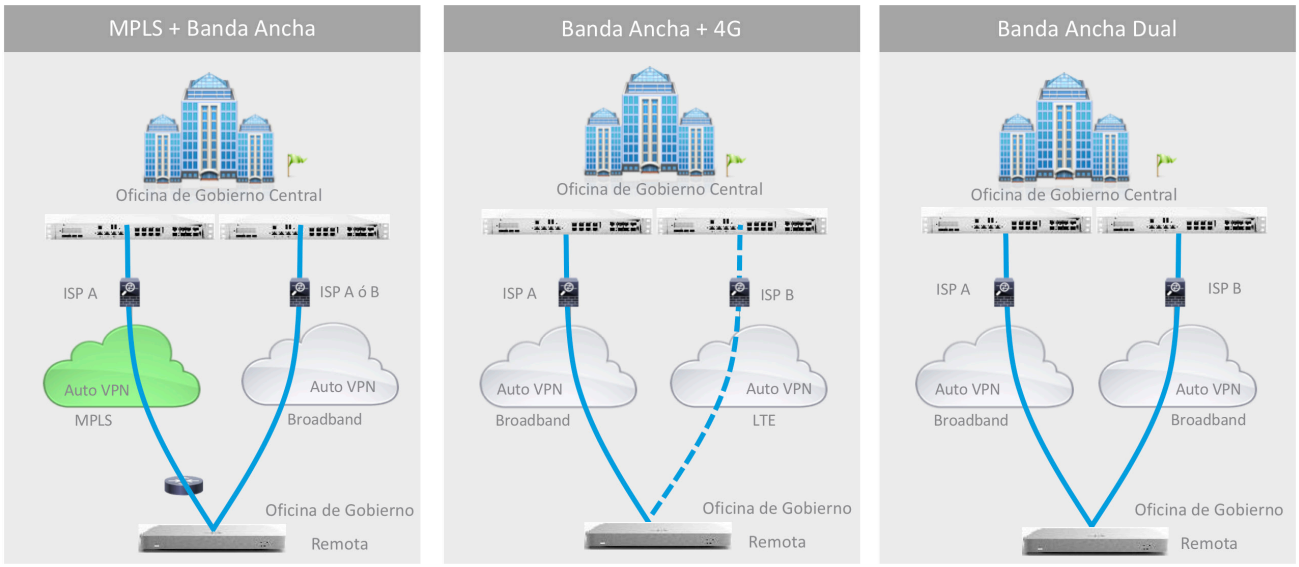

Figura 2. Escenarios de Conectividad de los Sitios

alojadas en el Centro de Datos de la Dependencia de Gobierno.

Esta Arquitectura permite contar con redundancia en las oficinas remotas a través de enlaces de internet de banda ancha, celular (LTE) o satelital, ya sea del mismo proveedor del enlace MPLS o de otro operador, creando un servicio de red de alta disponibilidad, flexible, con mayor cobertura y de óptimo costo.

Al contar con enlaces de banda ancha en los sitios remotos, los usuarios podrán acceder a Internet de manera directa sin tener que utilizar el enlace MPLS para transportar tráfico de Internet al sitio central. A través de este servicio, se aprovechan de mejor manera los enlaces dedicados para las aplicaciones de IT y comunicaciones de la Dependencia, así como se mejora la experiencia del usuario ya que las velocidades de navegación serán mayores al acceder a Internet de manera local. A través de la gestión en la Nube, se determina qué tráfico debe ser transportado vía la Red Virtual Superpuesta y cuál puede desahogarse de manera local a través de los enlaces de Internet (Split tunnel).

A través de la orquestación y gestión en la Nube, la Arquitectura SD-GS crea un servicio overlay de seguridad el cual permite ejecutar la protección en la frontera de cada sitio remoto/central, habilitando elementos de seguridad a los sitios remotos y oficinas centrales tales como: firewall de siguiente generación, prevención de intrusos (IPS), filtrado de contenidos por categoría/url, Geo-based, Anti-malware, pero gestionado y orquestado de manera centralizada lo que permite tener homologadas la implementación de las reglas y políticas de seguridad en todos los sitios.

3.2 Software Defined LAN/WLAN

Dentro de cada oficina central o remota, se requieren servicios de conectividad alámbrica e inalámbrica para que los usuarios puedan acceder a los sistemas institucionales, bases de datos, Internet, así como habilitar los servicios de comunicaciones unificadas (voz, video, mensajería) y herramientas de colaboración de la Dependencia.

Para lograr la homologación de los servicios, la Arquitectura de SD-GS desasocia la infraestructura física de las funcionalidades lógicas en los componentes de red LAN/WLAN, lo que permite que la implementación inicial y crecimientos se mantengan con el mismo nivel de rendimiento, funcionalidades y operación.
En el plano físico, los componentes se dividen en dos:

Switches, con características físicas tales como:

- 8, 24 o 48 puertos Ethernet 10/100/100
- Multigigabit Ethernet (opcional) Uplink 1/10/40G óptico
- 15 ó 30 Watts de PoE por puerto Stack físico (opcional)
- Redundancia en fuentes de poder (opcional)

Puntos de Acceso Inalámbrico (APs), con características físicas tales como:

- Estándar 802.11ac wave2
- MIMO2x2, MIMO3x2, MIMO4x4
- Interior o Exterior
- Multigigabit (opcional)

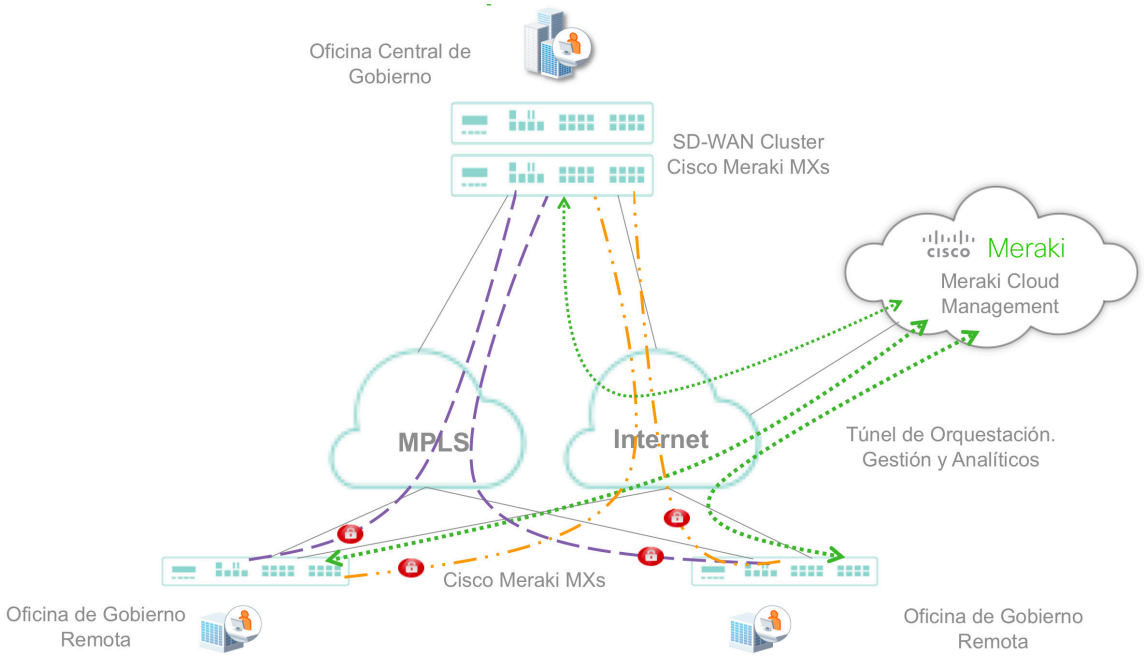

Figura 3. Conectividad WAN Definida por Software

Las funcionalidades lógicas requeridas para crear una red de grado gubernamental, son aplicadas a todos los elementos físicos descritos anteriormente, manteniendo homogeneidad de servicios y el rendimiento adecuado en cada capa de la red. Para esto, se requiere que los componentes físicos soporten las siguientes funcionalidades:

- Capacidad de crear aislamiento lógico del tráfico de datos y voz, el cuál debe respetarse en todos los elementos de la red del edificio.
- Capacidad para prevenir loops de capa 2 aún y en conexiones redundantes a diferentes equipos de uplink.
- Capacidad para poder respetar el etiquetado de Calidad de Servicio en los paquetes que ingresan a los componentes físicos, para su posterior tratamiento de acuerdo a las prioridades de cada paquete.
- Capacidad para poder crear etiquetas de Calidad de Servicio en los paquetes que ingresan a los componentes físicos, para su posterior tratamiento de acuerdo a las prioridades de cada paquete.
- Capacidad de autenticación de los equipos que se conectan a la red alámbrica/inalámbrica con un Directorio Activo o LDAP.
- Capacidad de multidifusión de paquetes.
- Capacidad para crear diferentes perfiles de conexión inalámbrica para usuarios de la red de Gobierno, invitados, etcétera, cada uno con diferentes mecanismos de autorización y seguridad.
- Capacidad para manejar portales de conexión para invitados, los cuáles se conectarán de manera simple, pero a su vez se identifica el tráfico y solo se les permite tener navegación en Internet.

La Arquitectura SD-GS a través de una plataforma de gestión y orquestación en la Nube, los elementos de red necesarios para habilitar el servicio (Security Gateways, Switches, APs) mantienen una comunicación con la Nube a través de un tunel de gestión seguro y eficiente en consumo de ancho de banda, desasociando el plano de control del plano de datos , lo que permite gestionar la infraestructura física y orquesta de manera centralizada los elementos del servicio, permitiéndo la implementación de infraestructura a través de mecanismos de conectar y funcionar (plug&play), creando un despliegue sin necesidad de realizar configuraciones en sitio ni preconfiguraciones previas (zero touch deployment). Esto genera que los servicios se encuentren disponibles de manera más ágil, que sean escalables, elásticos y que todos los elementos cuenten el mismo nivel de funcionalidades, orquestación y visibilidad.

3.3 Analíticos

Bajo esta Arquitectura, los analíticos se dividen en dos: analíticos operativos y analíticos de usabilidad, los cuales se presentan a través de tableros de control (dashboards) ejecutivos.

Los analíticos operativos permiten medir parámetros de rendimiento de la red tales como: latencia, jitter, pérdida de paquetes, así como disponibilidad de todos los componentes de la solución (infraestructura LAN/WLAN/WAN). Estos indicadores operativos son la base para la medición de los Acuerdos de Disponibilidad del Servicio (SLA) los cuáles permiten al Administrador de TIC verificar la correcta operación y rendimiento de los servicios administrados contratados.

Por otra parte, los analíticos de usabilidad convierten los datos en información relevante que facilita la medición del impacto de los servicios administrados contratados. Adicionalmente, provee inteligencia a través de indicadores que determinan la efectividad de los servicios y sus componentes, lo que permite una mejor toma de decisión sobre el incremento o reubicación de un determinado componente tecnológico o enlace de conectividad.

La Arquitectura SD-GS proporciona los mecanismos de interoperabilidad a través de interfaces abiertas programables (API) que permiten la creación de tableros de control personalizados con indicadores operativos y de usabilidad, integración con mesas de ayuda, creación dinámica de tickets en caso falla o degradación del enlace o componente tecnológico, y diversas integraciones que otorgan una gran visibilidad y flexibilidad al Administrador de TICs del Gobierno sobre los enlaces y componentes del servicio administrado.

Al contar con elementos de red que generan poderosos flujos de información a través de la inspección profunda de los paquetes, y con la flexibilidad que brindan las interfaces abiertas programables (APIs) , los Administradores de TIC de las Dependencias solicitan a los operadores del servicio administrado la creación de poderosos tableros de control operativos para medir indicadores de salud de los componentes tecnológicos y alinearlos al cumplimiento de los Niveles de Acuerdo de Servicio; tableros de control ejecutivos que permiten visualizar de forma fácil e intuitiva la salud de los servicios, así como indicadores que permiten conocer la utilización que los usuarios hacen de los servicios, demostrándo la usabilidad de los mosmos, permitiéndoles justificar las inversiones realizadas o bien, tomar mejores decisiones sobre cambios en las ubicaciones y/o capacidades del servicio; incluso, las interfaces programables (APIs) permiten la integración con otros sistemas tales como Mesas de Ayuda para la autogeneración de reportes en caso de falla , seguimiento de tickets en los tableros de control, o bien, contratar más capacidad en los servicios a través de market places de aplicaciones y servicios.

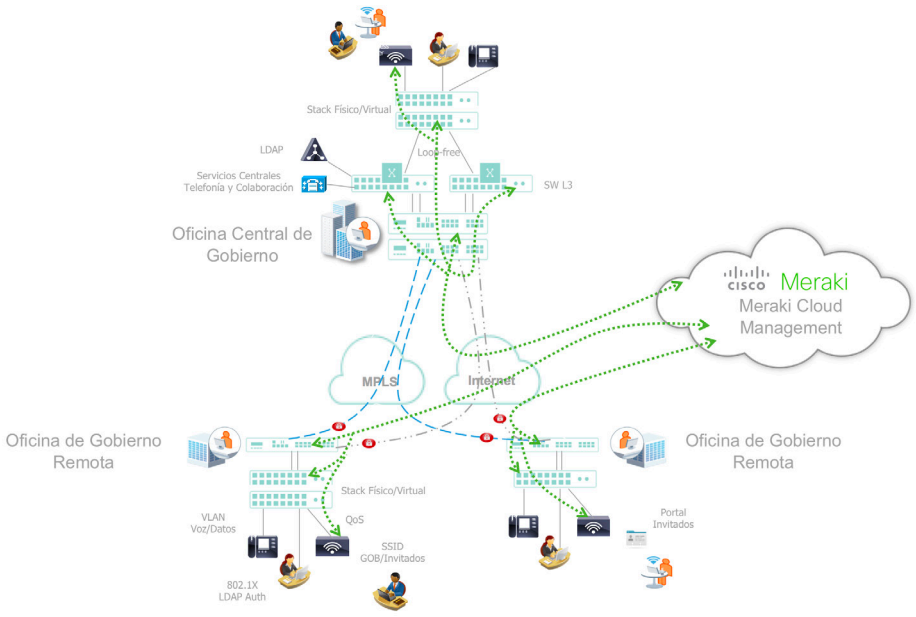

Figura 4. Servicios de Conectividad Definidos por Software dentro de los Edificios de Gobierno

4 Beneficios

Los beneficios de esta Arquitectura se cuantifican de acuerdo a la perspectiva de los diferentes actores involucrados en la Solución.

Desde la perspectiva del Usuario, los beneficios son:

- Los servicios de comunicaciones y de IT **funcionan**.
- Son rápidos (**Velocidad**).
- Sin riesgos (**Seguridad**).
- Cuentan con **cobertura** y **movilidad** para el uso de los servicios.

Desde la perspectiva de administrador de Tecnologías de Información y Comunicaciones (CIO), los beneficios son:

- Habilitación de servicios a sus usuarios (conectividad, voz, colaboración, acceso a sistemas y aplicativos, Internet) de manera ágil y elástica.
- Optimizar costos de ancho de banda
- Incrementar la capacidad de la Red
- Simplificar la operación
- Disminuir el TCO
- Protección de SLAs de los servicios contratados
- Indicadores de Usabilidad
- Habilitación de nuevos servicios en los contratos de servicios administrados:
  - Redundancia en enlaces o Internet directo
  - Incrementos de ancho de banda por demanda o Seguridad
  - Analíticos

Desde la perspectiva del Operador y proveedor del Servicio Administrado, los beneficios son:

- Incrementar **cobertura**, ya que puede integrar tecnologías más allá de MPLS.
- **Simplificar** la administración.
- Incrementar **oferta de servicios**:
  - Redundancia en los enlaces o Internet directo
  - Incrementos de ancho de banda por demanda o Seguridad
  - Analíticos
- Extensión del contrato de Servicios Administrados en un solo click.
- Menor costo de operación de la solución y por consecuencia un mayor ROI.
- Visibilidad en el cumplimiento de los SLAs y gestión de las penalidades y deductivas.
- Mayor **rentabilidad**.

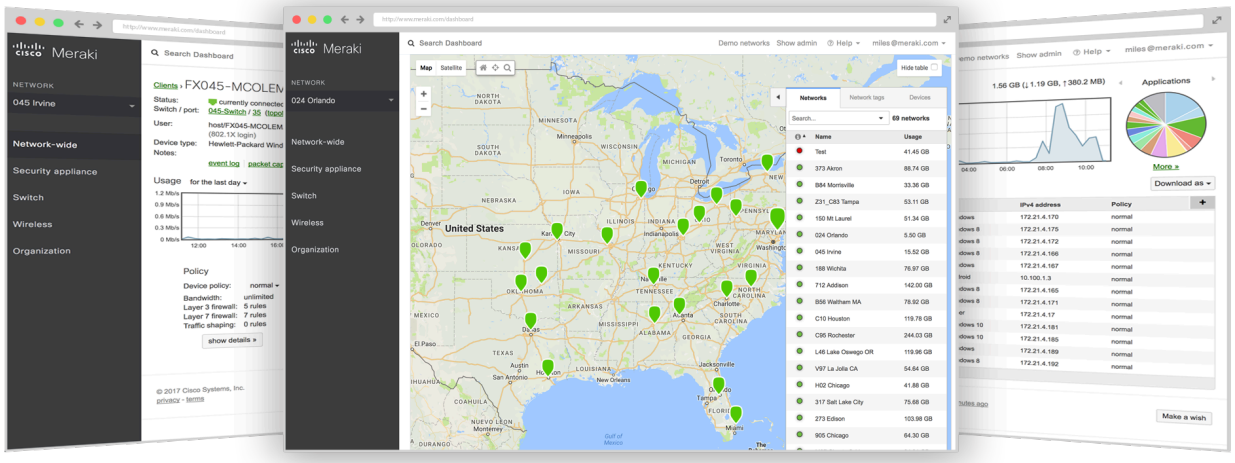

Figura 5. Tableros de control ejecutivos e integraciones via interfaces abiertas programables

5 Conclusiones

La Arquitectura de Servicios de Gobierno Definidos por Software (SD-GS) es la piedra angular para la creación de una nueva forma de Servicios Administrados para ITC del Gobierno, ya que habilita a los administradores de TIC del Gobierno a poder solicitar servicios de comunicaciones y TI de la Administración Pública Federal de una manera simple, automatizada, elástica y con la visibilidad de lo que sucede en los servicios contratados.

Al cambiar paradigmas con respecto a las redes tradicionales, esta Arquitectura permite que las Licitaciones de tecnología de información y comunicaciones se enfoquen en qué servicios tecnológicos se requieren para soportar los procesos de digitalización y gobierno digital que los Ciudadanos y los Empleados del Gobierno demandan, dejando al lado los requerimientos basados en components tecnológicos y un sin fin de protocolos y funcionalidades que éstos deberían cumplir.

Desde la perspectiva del Opeador de Servicios, la Arquitectura SD-GS le permite la integración de nuevas tecnologías de última milla, de mayor capacidad y cobertura, así como un nuevo portafolio de servicios, lo que amplía sus posibilidades de oferta en los procesos de adquisición. Además, la orquestación y automatización que ofrece la arquitectura de gestión centralizada en la nube, les permite una rápida implementación, optimización de costos, menor TCO, así como la simplificación de la operación, contando además con visibilidad y analíticos que permiten proteger los SLAs de los servicios y aplicaciones, así como contar con indicadores de usabilidad para medir el impacto de los contratados.

En resumen, la Arquitectura de Servicios de Gobierno Definidos por Software habilita los nuevos servicios de Gobierno con tecnología que simplemente funciona!