PLAN DE TRANSICIÓN AL PROTOCOLO IPV6 DE LA SUPERINTENDENCIA NACIONAL DE ADUANAS Y DE ADMINISTRACIÓN TRIBUTARIA

I.-INTRODUCCIÓN

Dado el crecimiento de la demanda de usuarios en la Internet, se requiere asignar una identificación única o dirección IP para cada equipo de los usuarios. La dirección IP es una numeración en un formato específico como **a.b.c.d,** el cual permite que la información vaya de un lugar de origen a un destino y es el principal recurso técnico para que los dispositivos logren conectarse a Internet.

El protocolo de Internet versión 4 (IPv4) que usa el formato antes indicado es el que actualmente y globalmente se emplea e identifica cerca de 4,300 millones de direcciones IP (aproximadamente 2^{32}) de los dispositivos de los usuarios. Sin embargo, éstas no son suficientes para abastecer la demanda actual, por el auge de los teléfonos móviles con acceso a Internet, redes sociales y el interés de interconectar cada uno de los diversos dispositivos tecnológicos.

En junio del año 2014 se anunció oficialmente que las direcciones IP del protocolo IPv4 han entrado en fase de agotamiento final. Para resolver esta situación crítica de escasez de las direcciones IPv4 se ha desarrollado un nuevo protocolo de Internet de conectividad, denominado **IPv6 con una capacidad de asignar 340 sextillones** de direcciones. A nivel mundial, para la asignación de direcciones IP existen organismos jerárquicos siendo el principal IANA (Internet Assigned Numbers Authority) que es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet. También podemos mencionar a la Corporación de Internet para la Asignación de Nombres y Números (ICANN). Estos organismos delegan los recursos de internet bajo ciertas políticas al Registro Regional de Internet (RIR) el cual es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo las cuales realizan una posterior subdelegación de recursos a sus clientes principales que incluyen a los proveedores de servicios de Internet (ISP) .

Esta nueva versión del protocolo provee nuevas e importantes características en las conexiones tales como:

La capacidad de direccionamiento extendida.

Mayor seguridad, puesto que al tener suficientes direcciones IP se podrá identificar con mayor facilidad a cada dispositivo en la red, porque cada uno tendrá su propia dirección IP.

Encriptación de los datos, de tal manera que la comunicación entre dos puntos será realmente privada y nadie podrá intervenirla.

Etiquetar los paquetes de datos para realizar una mejor gestión del tráfico de las comunicaciones.

Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores, alineados a 64bits (preparados para su procesado óptimo con los nuevos procesadores de 64bits), y con la cabecera de longitud fija, más simple, que agiliza su procesado por parte del enrutador.

Simplificación del formato de cabecera.

Autoconfiguración de direcciones.

Procesamiento simplificado en los routers.

Mejor soporte para las extensiones y opciones.

Adelantos en Multicast y Anycast.

Calidad de Servicio (QoS) y clase de Servicio(CoS).

El protocolo IPv6 cubrirá la necesidad de asignar el nuevo direccionamiento a todos los dispositivos tecnológicos usados para la conexión a internet, lo cual facilitará la conectividad en banda ancha, poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

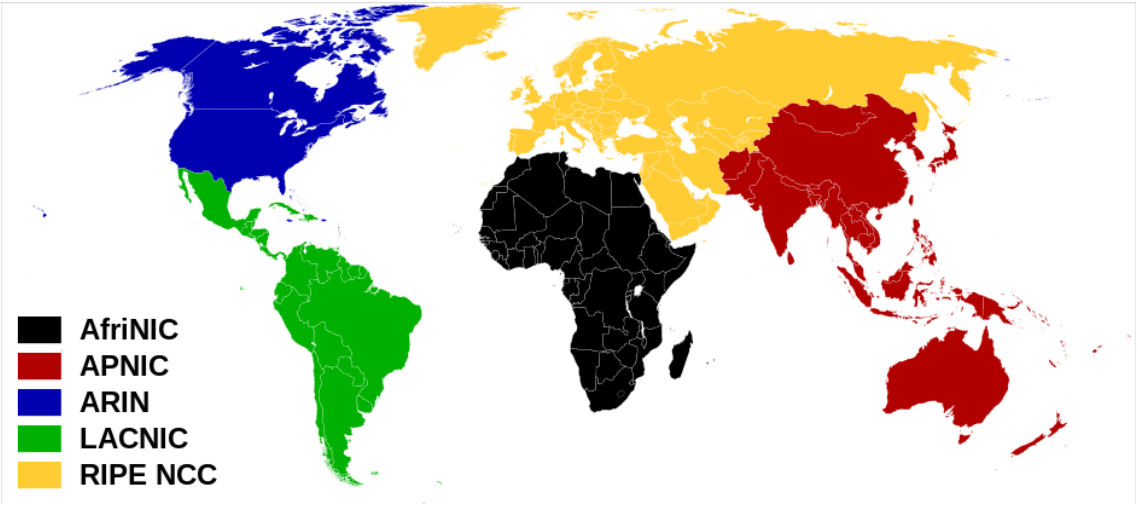
En los últimos años se ha manifestado que el despliegue de IPv6 es relativamente lento en el mundo, considerando que varios de los RIR ya han iniciado la última fase de asignación de sus últimos bloques (prefijo /8s) de direcciones IPv4, por lo que resulta importante dinamizar la implementación del protocolo IPv6 (Ver tabla 1).

Tabla 1: Disponibilidad de las IPv4 en los RIR

REGISTRO REGIONAL DE INTERNET (RIR)	**Direcciones IPv4 disponible set. 2017** **Cada bloque /8 equivale aprox. a 16 millones de direcciones IP.**
APNIC (Asia/Pacifico)	0.35/8s
ARIN (América del Norte y parte del Caribe)	0.00/8s
AFRINIC (África y parte Océano Indico)	0.79/8s
LACNIC (América Latina y parte del Caribe)	0.24/8s
RIPE NCC (Europa, centro y medio de Asia)	0.72/8s

Fuente: www.nro.net

Gráfico 1: Distribución Geográfica del Registro Regional de Internet (RIR)



Fuente: Wikipedia

La transición no va a ser fácil y pasarán años hasta completar el tránsito a IPv6, un tiempo en el que los proveedores, los sitios web y los fabricantes de dispositivos deberán ir adaptando sus infraestructuras a este cambio.

Sin embargo, surgen otros inconvenientes como el hecho de llevar a cabo la respectiva transición de un protocolo a otro (IPv4 a IPv6) de una manera práctica en organizaciones que cuentan con infraestructura tecnológica, sin afectar los servicios, tecnologías y procesos que actualmente gestionan. Es por ello que es necesario realizar los estudios y evaluaciones preliminares con el fin de elaborar un Plan de Transición al protocolo IPv6 en la SUNAT.

II.-BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y normas modificatorias.
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo y normas modificatorias.
- Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática y normas modificatorias.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de Información en el Perú- La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 083-2011-PCM, que crea la Plataforma de Interoperabilidad del Estado.
- Decreto Supremo N° 081-2017-PCM, que aprueba la Formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013 – 2017.

- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 350-2015-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado y norma modificatoria.
- Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses.
- Ley N° 30225 – Ley de Contrataciones del Estado y normas modificatorias.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Memorándum Electrónico N° 00069-2017–SUNAT/100000.

III.-OBJETIVOS DEL PLAN DE TRANSICIÓN

- Realizar el **despliegue del nuevo direccionamiento IPv6** en las redes, dispositivos, servicios y aplicaciones con que cuenta SUNAT para Internet y estar preparados para la transición global del protocolo a fin de estar integrados con los avances tecnológicos, lo cual repercute en la innovación de las entidades de la Administración Pública.

- Adoptar una **metodología de coexistencia gradual de los protocolos IPv4 e IPv6** durante el tiempo que sea pertinente en la SUNAT a fin de evitar impactos en la disponibilidad y gestión de los servicios informáticos.

IV.-ALCANCE DEL PLAN DE TRANSICIÓN

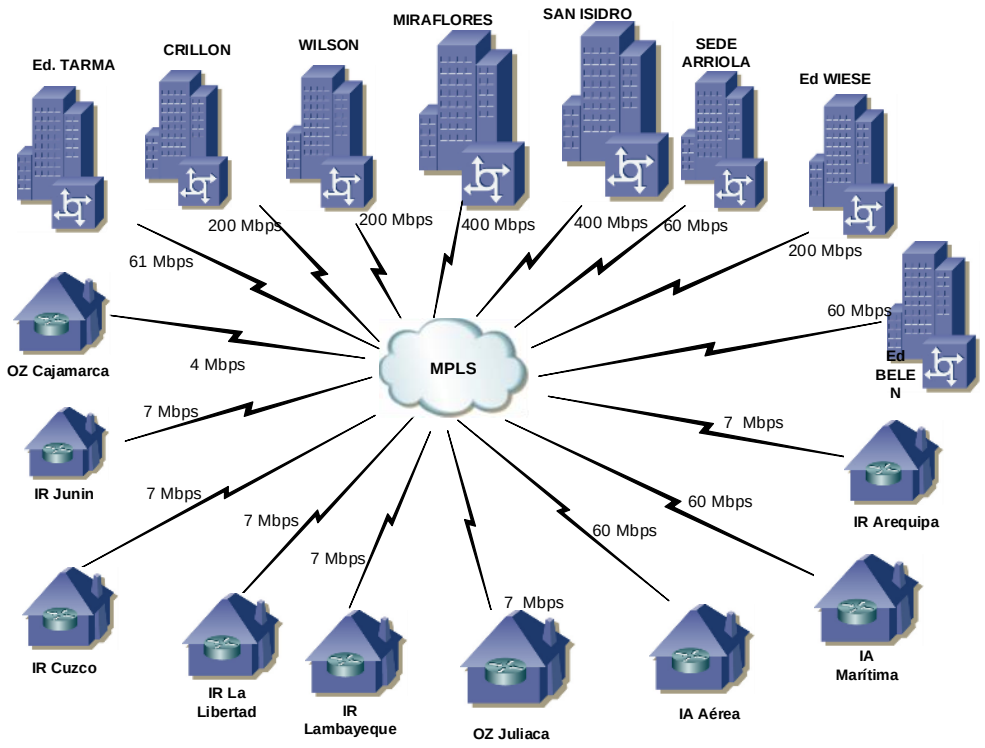
4.1.-INFRAESTRUCTURA

La SUNAT cuenta con una infraestructura interna de enlaces de datos MPLS en el cual se permite integrar a las diversas dependencias: intendencias regionales, centros de servicios al contribuyente, intendencias de aduanas, oficinas zonales, puestos de control, así como brindar a los usuarios los siguientes servicios:

- Aplicaciones administrativas y del negocio.
- Intranet.
- Correo institucional.
- Telefonía IP.
- Videoconferencia.
- Video vigilancia.
- Repositorios de archivos.

Todos estos enlaces se integran en una topología del tipo estrella hacia los ***datacenters de San Isidro y Miraflores*** en donde a la fecha se concentra toda la infraestructura de los servicios que se ofrece tanto a los usuarios internos, así como a los contribuyentes y operadores del negocio de aduanas.

Gráfico 2: Topología Red SUNAT



Fuente propia SUNAT

Para los servicios públicos, SUNAT cuenta con cuatro (4) enlaces internet configurando una arquitectura de alta disponibilidad y con contingencia de operadores ISP.

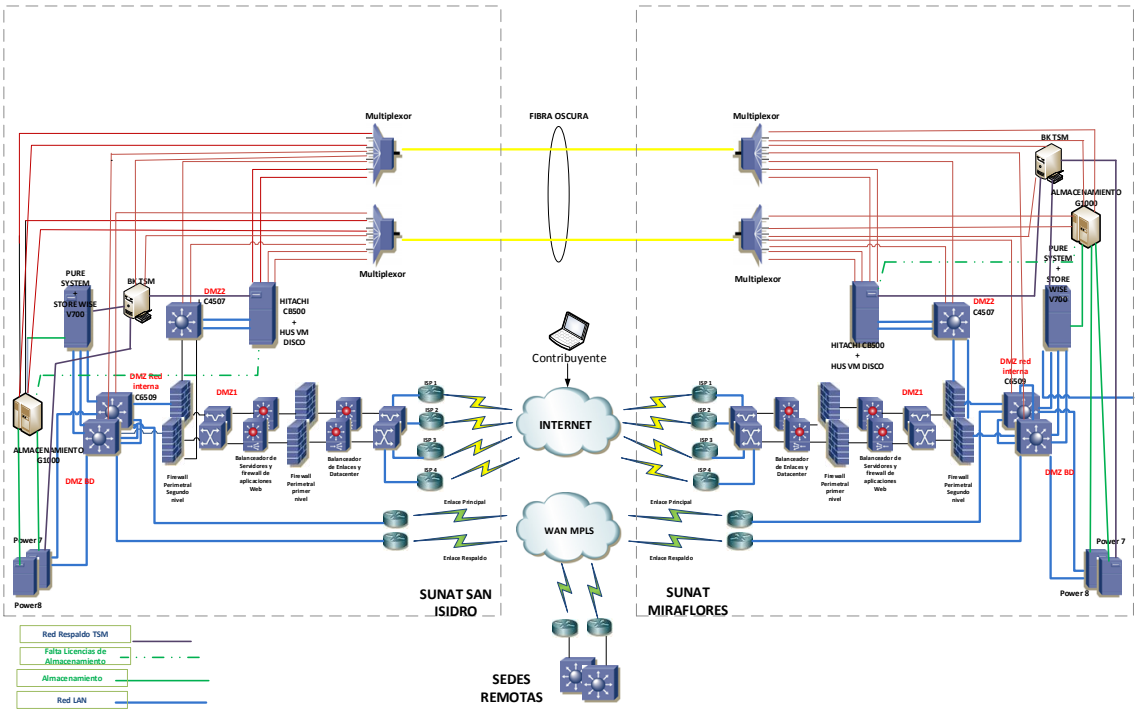
Las redes internas, servidores de aplicaciones internas, de bases de datos y de almacenamiento se encuentran protegidos y aislados de las conexiones hacia internet por una configuración de cascada-doble de Firewalls; así mismo los servidores de aplicaciones y web se encuentran aislados en las denominadas zonas desmilitarizadas, configurando las tres capas mínimas de seguridad en cuanto al acceso de los servicios públicos:

Plataforma Web.

Plataforma de Aplicaciones.

Plataforma de Bases de Datos.

Gráfico 3: ESQUEMA DE LA RED EN SUNAT



Fuente propia SUNAT

Describiendo el Grafico 3-Esquema de la Red en SUNAT, los 02 datacenters, ubicados en las sedes de Miraflores y San Isidro, se conectan entre sí mediante un tendido de fibra oscura, integrándose servidores Hitachi CB500 alojados en una Red DMZ, así como servidores de almacenamiento y bases de datos ubicados en la red interna. Adicionalmente, cada datacenter cuenta con una infraestructura interna de enlaces de datos MPLS de alta disponibilidad, es decir, operando con un enlace principal y un enlace redundante.

El tendido de fibra oscura es un tendido de fibra exclusiva entre los datacenters (San Isidro y Miraflores) a través del cual se integra con los multiplexores de 8 slots o puertos configurados en alta disponibilidad.

Tabla 2: Puertos – Multiplexores SUNAT

Puertos - Servicios	Datacenter San Isidro	Datacenter Miraflores	BW por puerto
Sistema G1000 SAN (x2puertos) Switch Brocade	Base de Datos	Base de Datos	8Gbps
Sistema SAN NUBE Hitachi CB500 (x2 puertos) conecta Switch Brocade	Sistema Hitachi	Sistema Hitachi	8Gbps
San Isidro-Miraflores (x1 puerto) conecta a Switch Cisco 6509	Sincronización del Exchange Ruteos de las redes de cada Datacenter.	Sincronización del Exchange Ruteos de las redes de cada Datacenter.	10 Gbps
DMZ2 Zona App (x1 puerto) conecta a Switch Cisco 4507	Sincronización DMZ2	Sincronización DMZ2	1 Gbps

Sistema Switch TSM (x1 puerto)	Sistema de Respaldo	Sistema de Respaldo	8 Gbps
Puerto Libre de Contingencia			8Gbps

Fuente propia SUNAT

Para los servicios públicos o la denominada Red externa-internet, SUNAT cuenta con cuatro (4) enlaces internet conectados a cada uno de los centros de datos, configurados con arquitectura de alta disponibilidad de enlaces y contingencia de operadores ISP; esto se concreta con la funcionalidad de los balanceadores globales instalados en esta zona.

En cada datacenter, para la protección perimétrica de red, se cuenta con equipos Firewall corporativos configurados en cascada doble para la protección y aislamiento de la red interna (en donde están alojados servidores de aplicación, bases de datos y almacenamiento) hacia las conexiones a internet.

El primer nivel de seguridad perimétrico protege los servicios web ubicados en la DMZ1; aquí se ubican los balanceadores internos, que son equipos encargados de optimizar la carga de accesos a los servidores web.

El segundo nivel de seguridad perimétrico protege los servicios de aplicaciones ubicados en la DMZ2 y a todos los servidores ubicados en la zona de la Red Interna.

En el Datacenter de San Isidro existen otras conexiones externas, por lo cual la Red interna es protegida por el Firewall Extranet. En este nodo se gestiona los enlaces dedicados con los servicios externos de Bancared, agentes de Aduanas y otras entidades públicas como Reniec, MEF, Tribunal Fiscal, Essalud, ONP; adicionalmente, se cuenta con otro Firewall dedicado a gestionar los accesos de navegación de los usuarios internos hacia internet y el control de acceso remoto seguro a la red de SUNAT.

Tabla 3: Firewall Corporativos - SUNAT

FIREWALL CORPORATIVOS	San Isidro	Miraflores
Primer Nivel @ (Web)	Si	Si
Segundo Nivel @ (App)	Si	Si
Firewall Extranet	Si	
Firewall funcionarios	Si	
Firewall Extranet/funcionarios		Si

Fuente propia SUNAT

En el Datacenter de Miraflores se cuenta con un Firewall del tipo corporativo, el cual se configura como nodo extranet y gestiona los servicios que se cuenta con terceros; además, está protegiendo a la red interna de Miraflores. Este mismo equipo se usa en caso de contingencia para la gestión de los accesos de navegación de los usuarios internos hacia internet.

Los switches CORE son la parte principal de la Red Interna en donde se concentran los servidores de producción, bases de datos, Call Center, sistemas de almacenamiento, multiplexores, ruteadores hacia la Red MPLS.

Como se había mencionado anteriormente, la Red MPLS (IP-VPN SUNAT) - ver gráfico 2- es la estructura de enlaces de comunicaciones de todas las sedes de SUNAT, que permite integrar a todos los usuarios a nivel nacional.

Cada sede de SUNAT (intendencia regional, intendencia de aduanas u oficina zonal) cuenta con un enlace principal y otro de respaldo que a través de sus ruteadores se integra a la Red MPLS. Por otro lado, también cuenta con un switch principal en el que se concentran todos los equipos que brindan servicios en su respectiva región como son: los servidores controladores de dominio Windows, files server, centrales telefónicas, radioenlaces, firewalls SOHO, ruteadores así como los switches de acceso destinados a concentrar a las estaciones de trabajo, equipos inalámbricos de red y periféricos de oficina (ver gráfico 3).

En cuanto a los locales de centros de servicios al contribuyente, por lo general cuentan con una infraestructura dedicada a la gestión de colas, firewalls SOHO y los ruteadores de comunicaciones las cuales son concentrados a través de un switch principal. La principal función del firewall SOHO es la de proteger la red interna del local de la SUNAT del segmento de red denominadas cabinas para uso explícito de los contribuyentes.

Respecto al cableado estructurado y dado que es un componente pasivo, se precisa que no representa un factor crítico de cambio o reemplazo puesto que en la mayoría de los locales y sedes de la SUNAT se cuenta con cableado estructurado en categoría 6; en los centros de datos (San Isidro y Miraflores) se cuenta con categoría 6A y fibra óptica multimodo lo cual está garantizando una velocidad de datos en la red local de 1Gbps (Gigabit por segundo).

En general se puede mencionar en la siguiente tabla el alcance del presente Plan en la SUNAT con la relación recursos/componentes:

Tabla 4: Descripción Recursos/Componentes en SUNAT

RECURSOS	EQUIPOS O COMPONENTES
Redes	Equipos concentradores redes locales (switches). Multiplexores. Controladores y equipos de accesos inalámbricos. Equipos de Ruteo interno. Equipos de Ruteo externo (Internet – Extranet). Firewalls de Internet. Balanceadores. Firewalls tipo SOHO.
Servidores	Telefonía IP y Call Center. Almacenamiento y Base de Datos. Contenedores de Aplicaciones y Web. Portal Web. Proxy. DNS. DHCP. Seguridad: Antispam-IPS-DLP-WAF
Dispositivos periféricos y end-points.	Estaciones de Trabajo. Impresoras. Teléfonos IP. Equipos Videoconferencia. Cámaras IP. Lectoras de Marcación. Equipo de control de UPS, climatización, electromecánico entre otros.

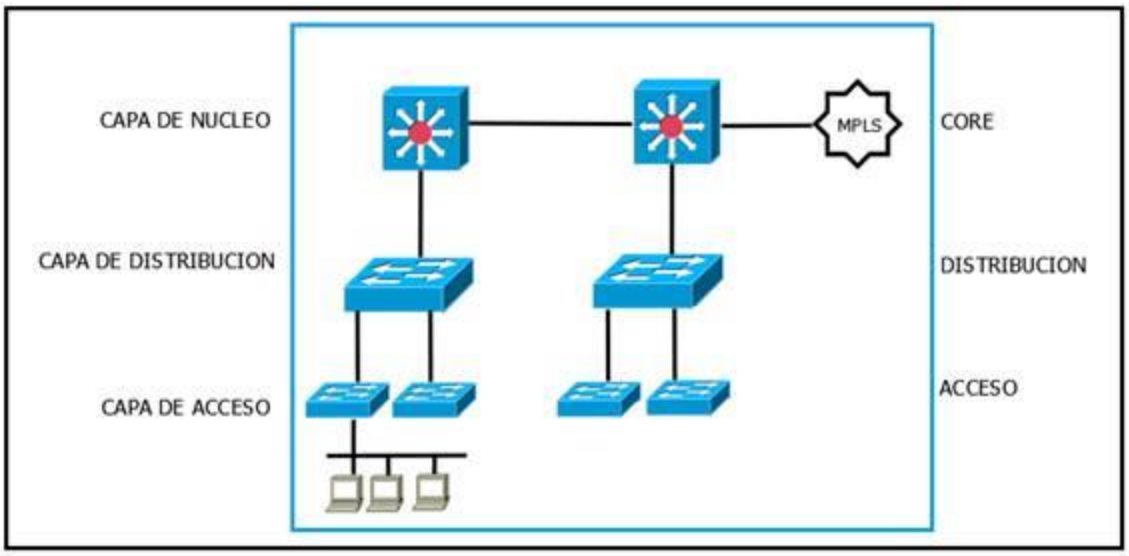
Personal	SUNAT cuenta con personal con experiencia en redes, los cuales son los primeros candidatos para una capacitación especializada. También es importante que nociones y conceptos generales sobre IPv6 involucren a personal de otras áreas y especialidades tales como: Bases de Datos, Arquitectura de Aplicaciones, Seguridad Informática, Desarrollo de Sistemas, Soporte y Mesa de Ayuda
Servicios Críticos	Comprobante de Pago Electrónico. Autenticación SOL. Presentación PDT. Libros Electrónicos. Cuadre y Generación de Notas de Abono (Extranet). RHE SOL. PLAME. T-Registro. Factura y Boleta Portal. Factura Grandes Emisores Guía de Remisión Grandes Emisores Guía de Remisión Portal Retenciones y percepciones Grandes Emisores. Comprobantes de Percepción Electrónica Portal. Comprobantes de Retención Electrónica Portal. Guía de Remisión Electrónica- Bienes Fiscalizables. Teledespacho Web. Envío de Entrega Rápida -Acta Traslado. Pago Electrónico Aduanero. Consulta Levante. SEIDA Numeración Manifiesto Marítimo. SEIDA Nota de Tarja. SEIDA ICA. Portal del Funcionario Aduanero: RN Tarja Marítimo. Portal del Operador CX: RN Tarja Marítimo.
Aplicaciones, SO, Otros Servicios	SO de Servidores. SO de Estaciones de Trabajo. Aplicativos y clientes de oficina: exploradores, correo. Clientes de App del negocio. Clientes de Comunicaciones Unificadas. Servicios de Colas.

Fuente propia SUNAT

4.2.-TOPOLOGIA ACTUAL DE LA RED EN SUNAT

El modelo jerárquico de conectividad que se emplea en organizaciones como SUNAT es el que se muestra en el gráfico 4, en donde la primera capa nuclear (core) está destinado para los datacenters la cual conectará a los servidores de producción; luego se identifica a la capa distribución/acceso para la integración de pisos; es decir, se concentra los equipos y periféricos de usuarios finales.

Gráfico 4: Modelo Conectividad LAN



Fuente CISCO

El actual protocolo IPv4 que se emplea establece un conjunto de direcciones IP de longitud de 32 bits (4 bytes), en el que la dirección está estructurada como una parte de red y una parte de sistema principal, siendo dichas partes establecidas de acuerdo con la clasificación de la dirección, ya sea A, B, C, D o E, según el número de bits iniciales; por tanto, el número total de direcciones IPv4 que se puede generar es de un total de 4.294.967.296.

En el direccionamiento IPv4 todas las direcciones IP presentes son públicas, exceptuando tres intervalos de direcciones que se han designado como privadas (10/8,172.16/12 y 192.168/16). Por lo general, dichas direcciones privadas son utilizadas para los sistemas de las redes locales de una intranet corporativa, teniendo la particularidad de no poder ser direccionadas a través de internet. En el caso de SUNAT se tiene esta distribución:

Tabla 5: Clases de Direcciones IPv4

SEGMENTO DE RED	CLASE	ZONA
10/8	A	Red Interna
192.168/16	B	Redes DMZ
172.16/12	B	Vlan internas o redes internas “sub-neteadas”.

Fuente propia SUNAT

La configuración de VLAN (segmento o redes virtuales) se realiza en los switches principales (CORE) y tiene por objetivo aumentar la seguridad y administrar el flujo de datos entre un segmento a otro.

Tabla 6: Muestra de VLAN Configurados en Switch CORE de SUNAT

#VLAN	NOMBRE DE LA VLAN
1	default
2	VLAN_NULA
4	MESA_PROVEEDORES
5	JIN_PRUEBAS
7	Serv_P740
10	SERVERS
15	GENESIS
16	BK-GENESIS
17	videoconf
18	CAMARAS_IP
19	Peoplesoft
20	Red_Usuarios
21	Residente_Callcenter
22	MAINSOFT
23	ACECO_IT
24	ContrataGpoWindows
25	PIP_IQF
26	LIMPIEZA
27	Fabrica Desarrollo

Fuente propia SUNAT

Tabla 7: Muestra de Direcciones IPv4 en Sedes SUNAT

SEDE SUNAT	DIRECCION DE RED	MASCARA
Wilson	150.200.0.0	255.255.0.0
Miraflores	10.2.0.0	255.255.0.0
San Isidro	10.0.0.0	255.255.0.0
IA Marítima	10.6.0.0	255.255.192.0
IA Aérea	10.5.0.0	255.255.192.0
Edificio Wiese.	10.16.0.0	255.255.0.0
Belén	10.17.0.0	255.255.0.0
Crillon	10.18.0.0	255.255.0.0
Arriola	10.168.0.0	255.255.0.0
IR Arequipa	10.56.0.0	255.255.0.0
OZ Juliaca	10.89.0.0	255.255.0.0
IR Ica	10.57.0.0	255.255.0.0
IR Lambayeque	10.60.0.0	255.255.0.0
IR La Libertad	10.59.0.0	255.255.0.0

Fuente propia SUNAT

Tabla 8: Muestra de VLAN en Redes DMZ- SUNAT San Isidro

NOMBRE SEGMENTO DMZ SAN ISIDRO	#VLAN	DIRECCION DE RED	MASCARA
Sello de Tiempo	300	192.168.20.0	255.255.255.240
Call Center	75	172.30.0	255.255.255.0
DMZ1 Calidad	34	192.168.34.0	255.255.255.0
DMZ2 Calidad	44	192.168.44.0	255.255.255.0
DMZ1 Desarrollo	46	192.168.46.0	255.255.255.0
DMZ2 Desarrollo	56	192.168.56.0	255.255.255.0
Interna Calidad	106	172.18.3.0	255.255.255.0
Interna Desarrollo	105	172.18.1.0	255.255.255.0
Desa_adu	55	192.168.55.0	255.255.255.0

Fuente propia SUNAT

4.3.- CARACTERÍSTICAS GENERALES DEL PROTOCOLO IPV6

Las *direcciones IPv6 tienen una longitud de 128 bits*, lo que equivale a 16 octetos que son escritos en una secuencia de 8 grupos de 4 dígitos hexadecimales, debido a que los diseñadores del protocolo optaron por representarlas de esta manera para permitir una representación más compacta que un grupo de unos y ceros. A pesar de esto, continúa siendo bastante complicada de manipular y recordar. En la tabla 9 se muestra algunos ejemplos de formatos como la reducción de ceros, el direccionamiento IP en su forma abreviada y las clases de direcciones.

Tabla 9: Representación de Dirección IPv6

	FORMATO COMPLETO	FORMATO ABREVIADO
REPRESENTACIÒN	x:x:x:x:x:x:x:x	Valor hexadecimal de 16 bits
EJEMPLOS	FEDC:DA98:7654:3210:FEDC:BA98:7654:3210	
	1080:0:0:0:8:800:200C:417A	
DIRECCION UNICAST	**1080:0:0:0:8:800:200C:417A**	1080::8:800:200C:417A
DIRECCION MULTICAST	FF01:0:0:0:0:0:0:101	FF01::101
DIRECCION DE LOOPBACK	0:0:0:0:0:0:0:1	::1(similar en IPv4 a 127.0.0)
DIRECCION NO ESPECIFICADA	0:0:0:0:0:0:0:0	::
EJEMPLO DE PREFIJOS DE 60 BITS	2AB:0000:0000:CD30:0000:0000:0000/60	2AB:CD30:0:0:0/60
NOTACION DECIMAL	0:0:0: 0:192.168.0.2	::192.168.0.2
	0:0:0:0:0:0:C0A8:2	::C0A8:2
DIRECCION COMPLETA	12AB:0:0:CD30:123:4567:89AB:CDEF/60	12AB::CD30:123:4567:89AB:CDEF/60

Fuente: **Clavijo B. L, Ramirez C. A, 2010, Configuración e Implementación de Redes de Datos con Direccionamiento IPv4 e IPv6, Colombia.**

Una de las nuevas características que presenta el protocolo IPv6 es la capacidad de dar soporte a direcciones IP que utilizan el protocolo IPv4; esto es de gran importancia para la coexistencia de los dos protocolos en infraestructuras de las redes actuales y las redes futuras.

Tabla 10: Equivalencias de direcciones IPv4 eIPv6

Dirección IPv4	Dirección Ipv6	Definición
IP públicas	Direcciones Globales	Direcciones ruteables en Internet
10.0.0/8,192.168.0.0/16, 172.16.0.0/12	fec0::/48	Direcciones del tipo privado
127.0.01	::1	Dirección Loopback.
224.0.0.0/4	ff00::/8	Direcciones multicast.
0.0.0.0	::	Dirección no especificada
169.254.0.0/16	fe80::/64(link local)	Direcciones de autoconfiguración.
146.83.206.114	::ffff:146.83.206.114	Direcciones IPv4 compatibles.

Fuente: Carmona A. P, Ulloa S. R, 2003, Configuración de Servicios de Internet con Soporte de Protocolo Internet versión 6 sobre GNU/Linux, Chile

Existen *tres tipos de direcciones en IPv6* y son:

Unicast: identifican a una interfaz única; esto quiere decir que un paquete destinado a una dirección unicast será entregado únicamente a la interfaz identificada con dicha dirección.

Anycast: estas direcciones identifican a un conjunto de interfaces, de tal manera que un paquete enviado a una dirección anycast será entregado a un miembro que pertenezca a este grupo, que generalmente es el más cercano según la distancia asignada en el protocolo de encaminamiento.

Multicast: igual que las direcciones anycast, con la diferencia de que un paquete que sea enviado a una dirección multicast, es entregado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6; en reemplazo se han creado este tipo de direcciones.

Una de las características para resaltar es la *capacidad de autoconfiguración de IPv6*, pues ahorra a los administradores de la red mucho trabajo, su instalación e implementación es fácil y sencilla, debido a que ha sido diseñada con el fin de garantizar que la configuración manual no sea necesaria.

La *seguridad en IPv6* se da a través del IPsec, el cual es un concepto que se aplica cuando el paquete está listo y antes de ser enviado por la red; es obligatorio en IPv6 y su uso es opcional con IPv4. El IPsec fue diseñado para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes y en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas por un único nodo.

Tabla 11: Principales diferencias de Protocolos IPv4 e IPv6

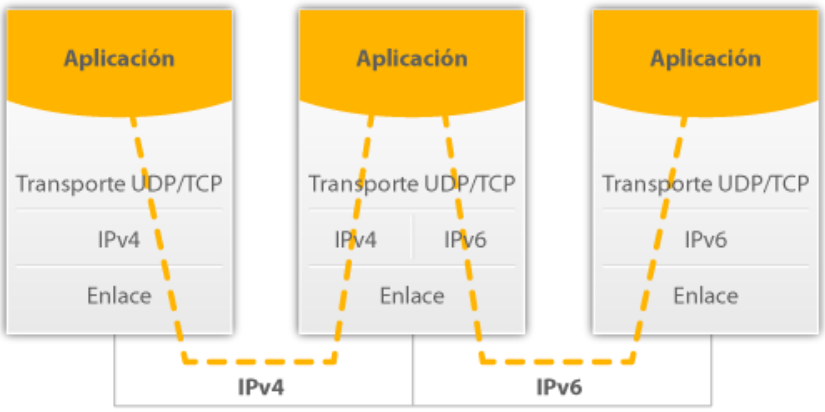
IPv4	IPv6
Las direcciones tanto de origen como de destino son de 32 bits de longitud (4 Bytes).	Las direcciones de origen y destino son de 128 bits de longitud (16 Bytes).
IPSec es un protocolo opcional.	IPSec es una obligatoriedad.
No existe identificación de paquetes QoS que manejen los routers en sus cabeceras.	Con la utilización del campo flow label se tiene entendido que se está manejando QoS.
La fragmentación de un paquete lo realiza el host como el router, que produce retardos.	La fragmentación en IPv6 lo realiza únicamente el host porque el paquete es procesado en el nodo final de destino.
Su cabecera tiene un cheksum.	Es eliminado el campo cheksum.
Se emplean solicitudes ARP para resolver direcciones IPv4 en una dirección de capa física.	Las tramas ARP son reemplazadas con mensajes multicast neighbor Discovery.
Usan registros A para la resolución de direcciones IPv4 a dominios.	Usan registros AAAA para la resolución de las direcciones IPv6.
Se utilizan las direcciones Broadcast para enviar un paquete a todos los nodos de las subredes.	Se utiliza una dirección multicast para poder enviar la información a los nodos de un ámbito local del vínculo.
Se debe configurar las direcciones de manera manual o utilizando DHCP.	No requiere de configuraciones manuales o utilizar DHCP.

Fuente: repositorio.utn.edu.ec

Los *mecanismos de transición del protocolo IPv6* podemos agruparlos en tres categorías o estrategias que se han definido hasta la actualidad:

- **Doble Pila (Dual-Stack),** este mecanismo de transición soporta ambas versiones del protocolo IP (IPv4/IPv6). Para su implementación se tiene que configurar todos los nodos con ambas pilas de protocolos (IPv4/IPv6), soportando direccionamiento (estático, DHCPv4, SLAAC o DHCPv6) y los protocolos de enrutamiento especificadas para cada versión (OSPFv3, RIPng, BGP4, IS-IS, entre otros).

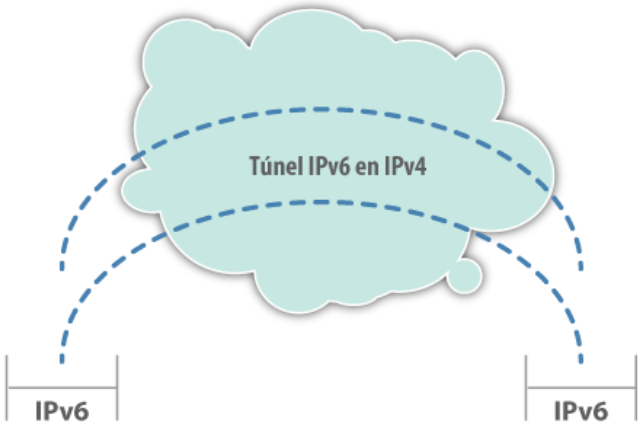
Gráfico 5: Modelo Transición Doble Pila



Fuente: portalipv6.lacnic.net

- **Túneles/Encapsulamiento**, las técnicas que se agrupan en este mecanismo de transición parten del principio de establecer un túnel virtual de comunicación entre dos redes IPv6 a través de una red con IPv4. La red IPv6 envía un paquete con el formato IPv6 hasta su enrutador de borde, este enrutador encapsula el protocolo IPv6 en una cabecera IPv4 con valor de campo de protocolo 41, el cual indica que está encapsulando un paquete IPv6. Cuando el paquete es encapsulado por el protocolo IPv4 es importante verificar los valores configurados del MTU (Máximum Transfer Unit) y del MRU (Máximum Receive Unit) y la conversión de los mensajes ICMPv4/ICMPv6.

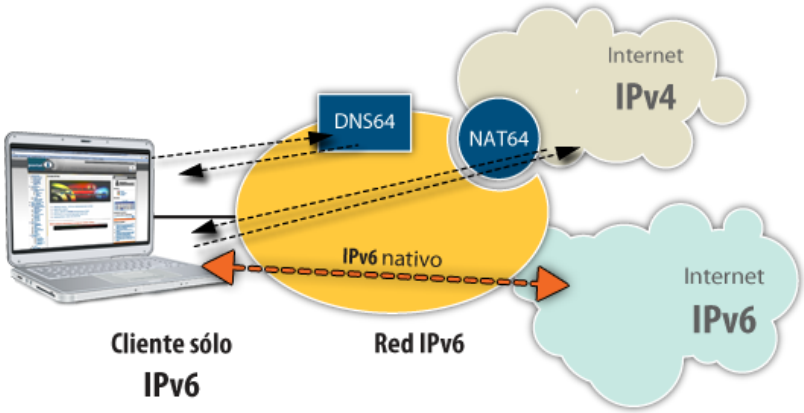
Gráfico 6: Modelo Transición Túnel



Fuente: portalipv6.lacnic.net

- **Traducción (Translation)**, esta técnica permite traducir direcciones IPv6 en direcciones IPv4 y viceversa. En el escenario en el que una red IPv4 inicie el proceso de comunicación hacia una red IPv6 utilizando alguna técnica de traducción, la red IPv4 deberá utilizar doble pila (IPv4/IPv6) desde el host que quiera comunicarse.

Gráfico 7: Modelo Transición Traducción



Fuente: portalipv6.lacnic.net

Tabla 12: Mecanismos de Transición de IPv6

TIPO	CONSUMO RECURSOS	COSTO OPERATIVO	COMPLEJIDAD
Doble Pila	Alto	Alto	Bajo
Túneles	Mediano	Mediano	Mediano
Traducción(NAT64/DNS64)	Alto	Alto	Alto

Fuente propia SUNAT

V.- DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

Definir las etapas preliminares que permitirán realizar una transición hacia el protocolo IPv6:

5.1.-Situación Actual:

Tabla 13: Componentes y Relevamiento en SUNAT

COMPONENTES	RELEVAMIENTO
Enlaces de telecomunicaciones	INTERNET: Direcciones públicas, BW contratado, DNS, datos del ISP WAN: BW contratado, datos del Carrier. RF: BW configurado, datos del contratista Diagramas de Red.
Parque de switches, balanceadores y multiplexores.	Inventario: Marca y Modelo de Core-SAN-Distribución Versión IOS release y feature que permita identificar el soporte del protocolo IPv6.

Servidores BD y respaldo	Inventario: Marca y Modelo de los equipos, Sistema Operativo release, versiones, Software BD versiones.
Telefonía y videoconferencia	Inventario: marca y modelo equipos o servidores CORE, sistema operativo y versiones, software y versiones. Listado de equipos periféricos de la solución.
Redes inalámbricas	Inventario: marca y modelo equipos o servidores CORE, sistema operativo versiones. Listado de equipos periféricos de la solución.
Seguridad de redes: Firewalls, Antispam-IPS-DLP-WAF.	Inventario: marca y modelo equipos, sistema operativo versiones, software versiones.
Gestión y monitoreo de TI	Soluciones de gestión y monitoreo. Software de mesa de ayuda. Lista de aplicativos.
Sistemas de información (internos y externos)	Elaborar un mapa y la arquitectura de los sistemas internos y externos para conocer su interacción.
Servicios tercerizados	Servicios de housing, hosting, cloudcomputing, alquileres de equipos, mesas de ayuda externas, centro de datos de respaldo, entre otros.
Parque informático de escritorio	Inventario de equipamiento y su software que interactúa directamente con el usuario.
Soluciones especializadas de datacenter	Inventario de equipos y software que gestionan y monitorean: UPS, Electromecánico, Climatización, Contra incendio, Cableado inteligente, entre otros.
Personal de TI	Descripción del personal, sus roles y responsabilidades. Evaluación al personal de TI para conocer el grado de conocimiento del nuevo protocolo IPv6.

Fuente propia SUNAT

En el **Anexo 3** se adjunta modelo de los formatos para la elaboración de los inventarios y control de equipos configurados en IPv6 y del detalle de los componentes de la infraestructura tecnológica de SUNAT.

5.2.-Identificar Brechas

- Nuevos servicios de acceso a Internet con IPv6.
- Equipos de redes y comunicaciones que se deba reemplazar con el total soporte de IPv6.
- Actualizaciones de sistemas operativos con el soporte de IPv6.
- Equipos de seguridad a ser reemplazados.
- Identificar las aplicaciones de los servicios críticos que requieran adaptación o de nuevos desarrollos para ser compatibles con el IPv6.
- De contar con hardware que ya cuenta con el total soporte de IPv6, revisar lo necesario para poder configurarlo con el nuevo protocolo.

Es recomendable contar con la asistencia de los representantes de fábrica con quienes se tiene contratos de soporte de la plataforma tecnológica de SUNAT a fin de que nos brinden información técnica específica relacionado a las compatibilidades con el

protocolo IPv6. Por ejemplo, esta información se contempla en el campo “Soporte IPv6 (SI/NO)” en el FORMATO DETALLE DE EQUIPO DE REDES (ver Anexo 3).

Para los casos de plataformas tercerizadas que están fuera de los datacenters pero que están brindando servicios a SUNAT, es recomendable solicitar al proveedor o contratista que cuente con los recursos necesarios para iniciar proceso de migración a IPv6 que agregue cláusulas con este alcance en las especificaciones técnicas o contratos de servicios.

5.3.-Impacto o evaluación del cambio

Identificar los componentes que tengan un mínimo contenido de riesgo o que generen menor impacto.

Iniciar el proceso de transición por el componente que menos afecte o impacte a los servicios de TI, especialmente aquellos que son el soporte de los procesos de negocio de la entidad de tal manera que permita al personal iniciar la experiencia y mejorar las habilidades técnicas hacia el nuevo protocolo IPv6.

Por las razones mencionadas, en SUNAT se sugiere iniciar la transición con los siguientes servicios:

Tabla 14: Servicios para Iniciar Transición al Protocolo IPv6

SERVICIOS	ALCANCE
Portal Web (páginas planas).	Red Externa, publicación en internet.
DNS.	Red interna, referencia de la nomenclatura de servidores
DHCP.	Red interna, delegación dinámica de direcciones IP a las estaciones de trabajo y periféricos de oficinas
Proxy.	Red Interna, control de acceso de los usuarios a la navegación internet.

Fuente propia SUNAT

Se debe indicar que previo a iniciar la transición de uno de estos servicios y dependiendo de las brechas identificadas, se debe haber culminado las tareas en cuanto a la remediación de compatibilidad de IPv6; es decir, contar con la plataforma preparada para la migración.

VI.- IMPLEMENTACIÓN DEL PROTOCOLO IPv6

El objetivo principal en el despliegue es lograr la utilización de los estándares IPv4 e IPv6 en una infraestructura común proporcionando al usuario una experiencia que no requiera estar al tanto de qué protocolo se está utilizando.

Debemos remarcar que la parte más crítica a solventar es la coexistencia entre ambos estándares debido a su incompatibilidad. A largo plazo IPv4 se desvanecerá, pero como el proceso podría tardar algunos años más no debemos perder de vista tres requisitos esenciales en cualquier planificación para el despliegue de IPv6:

- La integración de IPv4 e IPv6 no debe afectar a los servicios y aplicaciones existentes.

- No debe haber ninguna reducción en la seguridad de la red derivada de la migración hacia IPv6.
- Se reutilizará la infraestructura existente, capacidades, contenidos y entornos de aplicación siempre que sea posible.

Para adaptar una red a IPv6 **manteniendo la interoperabilidad con IPv4**, podemos seguir una **metodología genérica** basada en las siguientes fases:

FASE PRELIMINAR

6.1.- Contar con una campaña de comunicación a los usuarios internos sobre los alcances del proyecto de migración.

6.2.- Contar con personal calificado con conocimiento en todas las áreas necesarias para el desarrollo del proyecto: nociones y conceptos sobre IPv6.

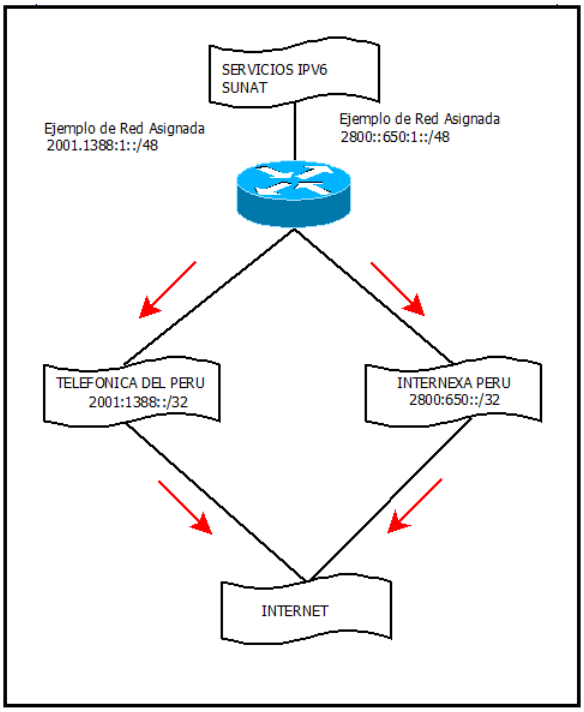
6.3.-Trabajar en conjunto con proveedores de servicio internet- ISP al momento del diseño de la red tanto interna como externa de la entidad. En este caso se consultó a los actuales proveedores de servicio internet a la SUNAT, Telefónica del Perú, Óptica Networks, Level 3, Internexa, los cuales manifestaron que cuentan con infraestructura lista de servicios internet con IPv6.

Se requiere coordinar con los proveedores de servicios internet para lograr la conectividad integral de IPv6 con el exterior.

- Habilitación y configuración de los ruteadores de internet.
- Estructurar el esquema de direccionamiento.
- Armar piloto o maqueta, definiendo el servicio web a publicar con IPv6.

En ese sentido, como cliente se debe solicitar la asignación de una red IPv6 para publicar servicios a internet, por ejemplo: 2001:1388:1: :/48 (ver Gráfico 8).

Gráfico 8: Servicios Internet con IPv6



Fuente propia SUNAT

Tabla 15: Carriers de Internet con IPv6

	ESTADO IMPLEMENTACION IPv6			
ISP	**Implementado**	**Actualmente Implementado**	**Planes de Implementación**	**Descripción**
Level 3	x			Level 3 fue el primero y continúa siendo el único proveedor de telecomunicaciones globales con IPv6 nativo instalado en sus redes de backbone tanto privadas como públicas. La empresa está en una posición inmejorable para posibilitar la transición a IPv6. Más de 40 clientes con servicios IPv6 y más de 5 años de experiencia en la operación de IPv6. Los clientes de Level 3 mezclan ambos protocolos, IPv6 e IPv4, en el mismo puerto y dentro de la misma VPN. El protocolo IPv6 se ha desplegado en forma nativa en el

				backbone MPLS usando 6PE. Tenemos peerings IPv6 con más de 20 socios.
Internexa	x			La empresa es originaria de Colombia, pero posee IPv6 nativo desde enero de 2011 tanto para Colombia, Ecuador, Perú y Chile.

Fuente: LACNIC

FASE PREPARACIÓN DE LA PLATAFORMA (REMEDIACIÓN)

6.4.- Remediar las brechas identificadas en el proceso de relevamiento de información del inventario tecnológico (párrafos 5.1 y 5.2) y verificar el estado actual de todos los dispositivos y aplicaciones; esto incluye considerar las adquisiciones necesarias sea SW y HW.

FASE CONFIGURACIÓN Y PRUEBAS CON UN SERVICIO

6.5.-Diseño de la red con el nuevo esquema IPv6:

6.5.1.-Plan de Numeración IPv6

- Por temas de administración y simplificación, a la configuración, los servidores y equipamiento de red (“switch”, “router”, “firewall”, entre otros) se les asignará su dirección IPv6 de forma manual.

  En una primera fase, habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de los servicios de: DNS, DHCP, Proxy, Portal Web.

- Es conveniente utilizar mecanismos de autoconfiguración existentes en IPv6, como el DHCPv6, que permite centralizar toda la asignación de direcciones de los equipos pertenecientes a un sitio o sede, como es el caso de las estaciones de trabajo y equipos periféricos.

Tabla16: Direcciones IP para cada equipo en IPv6

#	Equipo	Siglas	IPv4	Ejemplo IPv6
1	Router (LAN)	ROU	NET.net.1.X	2001:1388:1::1:x
2	Server	SRV	NET.net.2.X	2001:1388:1::2:x
3	Concentrador	SW	NET.net.3.X	2001:1388:1::3:x
4	Radioenlaces	WIR	NET.net.4.X	2001:1388:1::4:x
5	Central Telefónica	PBX	NET.net.5.X	2001:1388:1::5:x
6	Gateway	GWY	NET.net.6.X	2001:1388:1::6:x
7	Impresoras	PRT	NET.net.7.X	2001:1388:1::7:x
8	Print Server	PRS	NET.net.8.X	2001:1388:1::8:x
9	UPS	UPS	NET.net.9.X	2001:1388:1::9:x

10	Lectoras	LEC	NET.net.10.X	2001:1388:1::10:x
11	Servidor Telefonía IP	SIP	NET.net.11.X	2001:1388:1::11:x
12	Consola	CON	NET.net.12.X	2001:1388:1::12:x
13	Eq. Seguridad	SEC	NET.net.13.X	2001:1388:1::13:x
14	IDS	IDS	NET.net.14.X	2001:1388:1::14:x
15	Aire Acondicionado	AAC	NET.net.15.X	2001:1388:1::15:x
16	Bridge	BRD	NET.net.16.X	2001:1388:1::16:x
17	Equipo de Videoconferencia	VID	NET.net.17.X	2001:1388:1::17:x
18	Cámaras IP	CIP	NET.net.18.X	2001:1388:1::18:x
19	Balanceador de carga	BAL	NET.net.19.X	2001:1388:1::19:x

Fuente propia SUNAT

6.5.2 Protocolos de enrutamiento IPv6

En cuanto al enrutamiento interno, el uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Para aprovechar nuevas características del IPv6 se han desarrollado nuevas versiones o complementos de enrutamientos:

Tabla17: Protocolo de Enrutamiento

Protocolo de Enrutamiento	Versión IPv6
OSPF	OSPFv3
BGP	BGP-MP
EIGRP	EIGRP for IPv6

Fuente propia SUNAT

Asignar las rutas en los switches core de la red, ruteadores internos y firewalls.

- Dado que IPv6 es un protocolo capa 3, su uso es transparente para todos los dispositivos capa 2; es decir, no habrá un impacto en la configuración de los “switches” de acceso que se encuentran a lo largo de las dependencias de SUNAT.
- Una vez configurada la red IPv6 en SUNAT es necesario avanzar con el despliegue en los servicios básicos de red como el DHCP, DNS, PROXY.

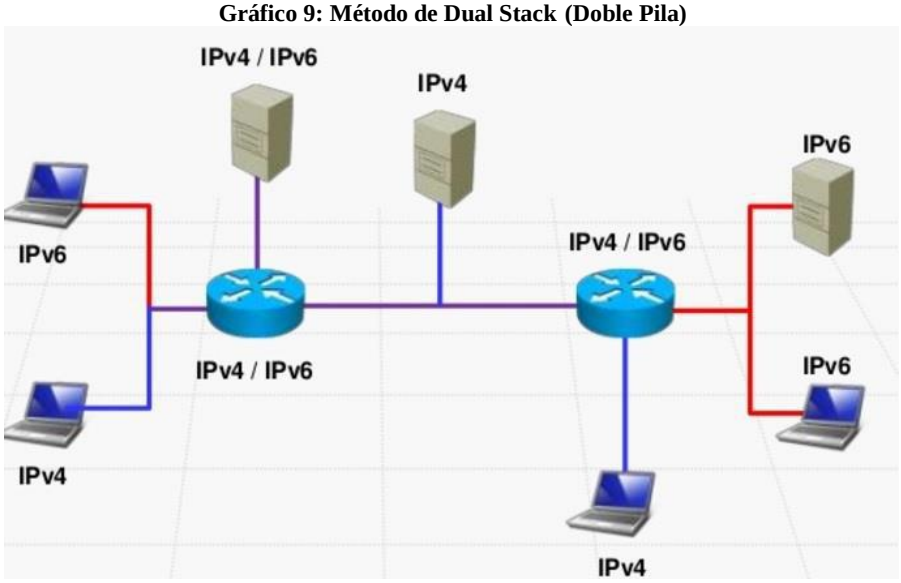
6.5.3.-Metodo de Transición

El objetivo de la transición no es reemplazar todos los servicios IPv4 existentes; lo que se pretende es buscar diferentes escenarios para la migración que no impacte en la operatividad y continuidad de los servicios.

Por ejemplo, contando con un esquema de doble pila IPv6 hacia internet y publicado un servicio público como el portal web (paginas estáticas), evaluamos la estabilidad del servicio con un continuo monitoreo.

Si por tema de criticidad no es viable considerar la migración del portal web (páginas estáticas) ya se había mencionado en la etapa de evaluación del cambio 5.3 en tener otros servicios como el DHCP, PROXY o DNS.

Gráfico 9: Método de Dual Stack (Doble Pila)



Fuente: Metodología Transición, Edwin Segura (Garometta 2012)

FASE EXTENSIÓN A OTROS SERVICIOS

6.5.4 Configuración de Servicios Básicos de Red.

De todo lo aprendido en la fase anterior se puede manejar la migración al IPv6 focalizándose en los *segmentos de red de las estaciones de trabajo de la INSI*. Para ello es necesario habilitar IPv6 en los switches CORE y de ACCESO de estos segmentos y en los servidores que gestionan los servicios DHCP.

Hay que recordar que a estas alturas la red de SUNAT debería tener configurado nodos de red con esquema de doble pila; es decir, la convivencia de ambos protocolos IPv4 e IPv6 está ya estructurado.

Luego de los periodos de estabilizaciones se iniciará la configuración de modo progresivo a los segmentos de red del resto de sedes SUNAT.

FASE SERVIDORES DE PRODUCCIÓN

6.5.5. Configuración de los Servidores de Producción

En una última etapa se considera orientar la configuración IPv6 a los recursos más críticos que son los servidores de producción:

Bases de datos.

Sistemas de almacenamiento.

Repositorios de aplicaciones.

Sistema de call center.

Comunicaciones unificadas y dispositivos end-point.

Es probable que exista remanentes de dispositivos **end-point** que aun cuenten con direcciones IPv4 tales como: impresoras, lectoras de asistencia, equipos de control de UPS, equipos Tx/Rx de radioenlaces y otros, que pueden tomar un poco más de tiempo en estandarizar y habilitarlos al IPv6. Para ellos son los switches y routers los elementos base de soportar el esquema doble pila IPv6; es decir, de soportar ambos protocolos IPv4/IPv6, garantizando la migración de manera controlada.

6.6.-Aplicación de políticas de seguridad del protocolo IPv6 en los equipos de seguridad y comunicaciones.

Actualizar las herramientas y proceso de seguridad.

Obtener equipos certificados.

Desarrollar prácticas de programación adecuadas para IPv6.

Contar con auditorias que conozcan IPv6.

Existen varias recomendaciones para evitar los problemas asociados al reconocimiento local o remoto de una red. La principal es que los identificadores de interfaz de los nodos IPv6 no sean números correlativos y que no partan desde el límite inferior del rango (evitar las secuencias: 1,2,3, etc.). Esto se puede lograr mediante el uso de la autoconfiguración de direcciones IPv6, ya que es posible obligar a los nodos a generar un identificador de interfaz pseudo-aleatorio o basado en la dirección física de la interfaz.

FASE POST-IMPLEMENTACIÓN

6.7.- Estrategias de monitoreo

El monitoreo de la red y de los servicios que hay implementados sobre ella cobran importancia cuanto más críticos nos resultan estos servicios o vínculos de la red. Eso dependerá fuertemente del tipo de red de la que hablemos; la criticidad o no del monitoreo dependerá del grado de control que queramos llevar sobre los servicios. No obstante, más allá de esta medida que podría resultar hasta subjetiva, lo cierto es que realizar un buen monitoreo no solo nos permite sentir que tenemos controlada la situación, sino que objetivamente permite, entre otras cosas:

Incluir en la herramienta de monitoreo las nuevas direcciones IPv6 y validaciones de los servicios mediante ambos protocolos (recordar que IPv4 no se elimina).

Detectar y prevenir problemas.

Diagnosticar causas de fallas.

Determinar las acciones que solucionarán el problema.

Conformar planes de contingencia.

6.8.-Estrategia Post-implementación

Como culminación del proceso de transición es necesario que se realicen pruebas de funcionalidad sobre el protocolo de IPv6, con el fin de validar la implementación del mismo y su correcto desempeño en tema de aplicaciones, servicios y demás sistemas

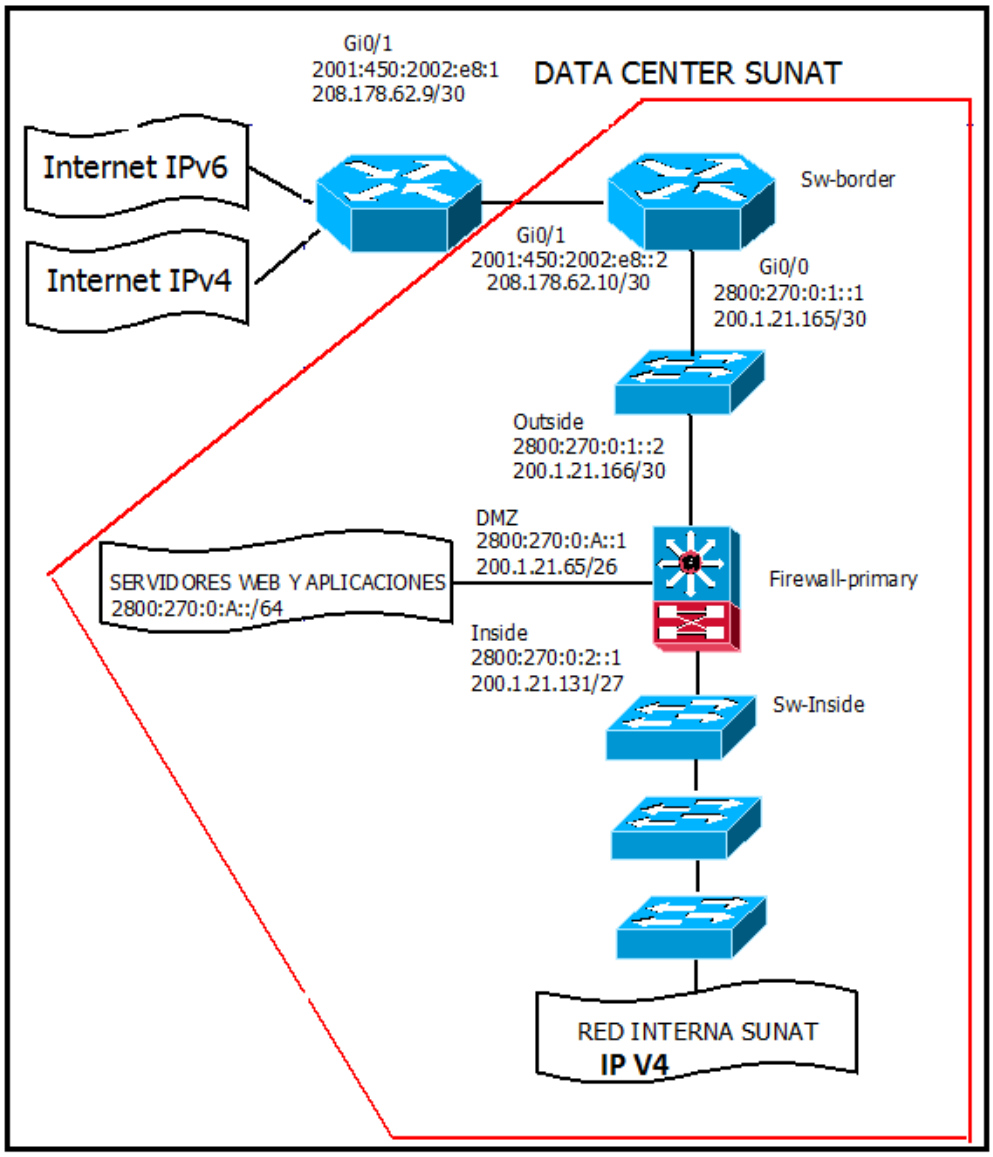
que se ven afectadas por dicho cambio. Para tal fin, deben adelantarse las siguientes actividades:

- La realización de pruebas y monitoreo de la funcionalidad del protocolo IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad, generando tráfico de IPv6 desde la entidad hacia el internet y viceversa.
- La realización de pruebas de funcionalidad del protocolo IPv6 con respecto a las políticas de seguridad perimetral de servidores de cómputo, servidores de comunicaciones y demás equipos de comunicaciones.
- La realización del afinamiento de las configuraciones de hardware, software y servicios de la entidad, tomando como referencia el informe de configuraciones del protocolo IPv6 de la fase pasada.
- La elaboración de un inventario final de servicios, aplicaciones y sistemas de comunicaciones bajo el esquema de funcionamiento del protocolo IPv6.

De esta manera, debe tenerse como resultado de esta fase los siguientes entregables:

- Informe en donde se especifiquen los cambios de las configuraciones realizadas.
- Inventario final de la infraestructura de TI sobre el protocolo IPv6.

Gráfico 10: Esquema Transición Dual Stack



Fuente propia SUNAT

VII.-REALIZACIÓN DE PRUEBAS

Ya se ha señalado en el **apartado 6.3** del presente documento la necesidad de realizar ***un piloto o maqueta***, configurando una plataforma paralela de servidor web, así como de contar con conectividad IPv6 hacia internet. Los principales componentes de la maqueta serían:

Estación de trabajo con SO Linux.

Software Nginx/Iplanet para activar servicios www.

Solicitar al proveedor (carrier) activar el protocolo IPv6 en los enlaces internet.

Solicitar la asignación de segmentos de redes IPv6 a ser publicados por internet para esta maqueta.

Realizar las configuraciones, monitoreo y las pruebas de acceso con clientes IPv6 e IPv4.

Elaborar informes técnicos indicando recursos, secuencias que fueron necesarias, conclusiones y recomendaciones para la configuración de IPv6.

Finalizado el piloto y con la remediación de brechas en el relevamiento de información, así como el diseño de la red IPv6 para los servicios y plataforma de TI de la SUNAT, es recomendable iniciar la **implementación de manera parcial**, teniendo en cuenta las aplicaciones más críticas con las que cuenta la entidad. Para ello es preciso contar con un segmento de red alterno para realizar las pruebas antes de iniciar la producción y así evitar la interrupción de cualquiera de los servicios y aplicaciones.

Se había mencionado **en el apartado 5.3 iniciar la transición con los servicios web de la entidad** (páginas planas) adoptando la configuración de nodo (equipo de red) con el esquema de doble pila a fin de minimizar los riesgos. Esta consideración permitirá:

- Funcionalidad y monitoreo del protocolo IPv6 en los servicios que ofrece la entidad por internet.
- Funcionalidad del protocolo IPv6 frente a las políticas de seguridad perimetral (firewalls) de la entidad.
- Afinamiento de las configuraciones de hardware, software y servicios de la entidad.
- Aplicar los criterios de seguridad IPv6 en la plataforma configurada.
- Elaborar un inventario final de servicios, aplicaciones y sistemas migrados.

VIII.- CAPACITACIÓN Y SENSIBILIZACIÓN

Una de las tareas fundamentales para la implementación de IPv6 es la capacitación del personal técnico quien se encargará de la implementación. Esto tiene el propósito de que el personal se familiarice con los conceptos y lógica de funcionamiento del protocolo. Sin este paso es muy probable que se caiga en malentendidos y confusiones entre el funcionamiento de IPv4 e IPv6. En ese sentido se debe tener en cuenta los siguientes puntos:

- Elección de los ingenieros y/o profesionales que trabajan en las áreas técnicas de TI de la entidad, para cumplir con todas las actividades que este proyecto demanda.
- Talleres de entrenamiento al personal técnico sobre conceptos, configuraciones, seguridad de redes IPv6 (equipos de redes, servidores).
- Reforzar las capacidades para revisar las opciones técnicas y ver cuál es la apropiada relacionado al proceso de migración del protocolo IPv6.

De igual forma, al ser la comunicación interna con los usuarios un factor importante en un proceso de cambio, y más aún al estar relacionada a la tecnología de la información, es necesario contar con el apoyo de la Alta Dirección a fin de garantizar los recursos y el apoyo institucional que permitirá:

- Presentar la organización de los equipos de trabajo para la gestión del proyecto de transición.
- Desplegar la transición al IPv6 en la entidad y estar preparados a la integración global del protocolo hacia nuevas tecnologías.
- Convocar el compromiso de participación para las próximas tareas que involucra el proceso de migración.

La siguiente tabla muestra los perfiles a considerar en la capacitación:

Tabla18: Perfiles de Capacitación – Transición Protocolo IPv6

#	PERFILES DE CAPACITACIÒN IPv6	ESPECIALIDAD	UUOO
1	Infraestructura y Seguridad	Base de Datos y S. O	GA, GOSU y OSI
		Web.	
		Redes y Telecomunicaciones.	
		Seguridad Informática.	
		Plataforma Virtualización	
2	Desarrollo	Desarrollo de Sistemas. Calidad de Sistemas.	GDS Y GCS
3	Atención de Usuarios	Helpdesk.	GOSU
		Atención de Usuarios.	

Fuente propia SUNAT

IX.-CONCLUSIONES

- Es importante considerar, en la fase preliminar de la transición, una infraestructura tecnológica paralela en base a la implementación de un piloto o maqueta que permita la interacción con servicios web IPv6.

- La adopción de IPv6 en la SUNAT debe realizarse de manera gradual. Se está proponiendo iniciar la transición con servicios de menor impacto y culminar con los servicios o plataformas críticas.

- Debe existir un periodo de coexistencia entre los protocolos IPv4 e IPv6. Para ello se debe preparar la plataforma (remediación) a fin de que soporte las funcionalidades de ambos protocolos activando las configuraciones de Dual Stack (Doble Pila).

- Considerar como lineamiento que el desarrollo de especificaciones técnicas de adquisiciones de hardware, sistemas operativos, software u otro componente de tecnología de información en SUNAT soporte y tenga compatibilidad con el protocolo IPv6.

X.- PRESUPUESTO ESTIMADO

Tabla 19: Planes de Acción

Línea de Acción	Proyecto	Objetivo	Presupuesto
Capacitación.	Capacitación de IPv6 al personal técnico de INSI.	Contar con la formación especializada del personal que está asociado al proyecto.	30 personas x 1000 x S/3.3 **S/ 99,000.00**

Migración enlaces internet con IPv6.	Contratación de nuevos servicios de Internet con IPv6.	Tener plataforma de enlaces internet expedita para ofrecer servicios con IPv6.	Por renovación de servicios enlaces internet x 3 años: **S/ 9'300,000.00**
Revisión de los equipos de comunicaciones.	Adquisición de equipos de comunicaciones y software monitoreo con soporte IPv6.	Contar con los equipos de red configurados y con soporte IPv6	Por renovación del parque switches x 5 años: **S/ 25`000,000.00**
Revisar aplicaciones con soporte IPv6.	Desarrollo o adaptación de aplicaciones con IPv6.	Contar con los servicios críticos de atención al contribuyente con el soporte de IPv6.	
Revisión S.O.		Actualización de S.O. de Servidores para IPv6	
Horas Hombre		Participación del personal técnico INSI en el despliegue.	30% x 30 especialistas x S/ 7500 mensual: **S/ 67,500.00**
Imprevistos		Retrasos administrativos, técnicos	**10% a 15%** del costo total del proyecto.

Fuente propia SUNAT

XI.- ANEXOS

ANEXO 1: CRONOGRAMA

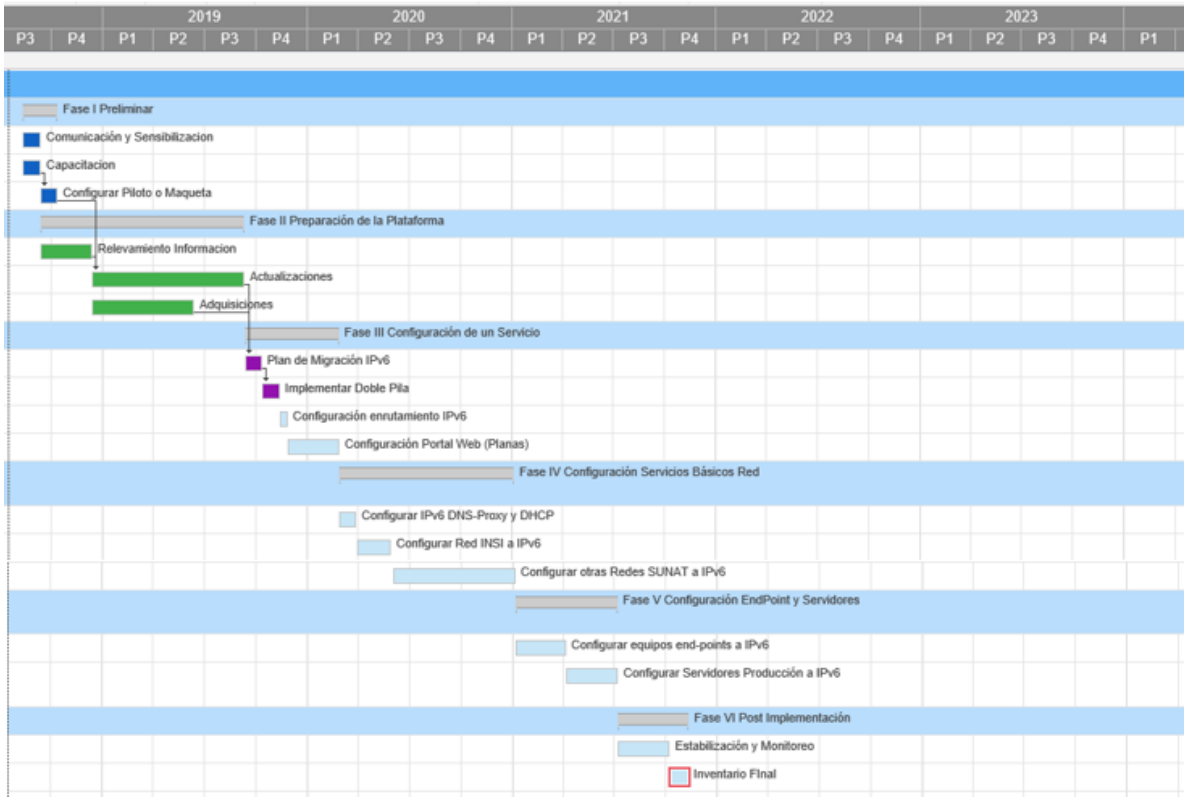
FASES	ACTIVIDADES	ALCANCE	TIEMPO	ÁREA RESPONSABLE	ARTÍCULO 4° D.S. 081-2017-PCM
I.-PRELIMINAR	Comunicación y Sensibilización	INSI	1 mes	Gerencia de Gestión de Procesos y Proyectos de Sistemas / Gerencia de Arquitectura /Gerencia de Operaciones y Soporte a Usuarios	9
	Capacitación.	Personal técnico INSI	1 mes		
	Asignación de redes IPv6 base y piloto (maqueta).	Enlaces Internet e infraestructura paralela para el piloto(maqueta).	1 mes.		
II.-DIAGNÓSTICO Y PREPARACIÓN DE LA PLATAFORMA (REMEDIACIÓN)	Relevamiento y Diagnóstico de la información (Inventario SW, HD, Infraestructura, Aplicaciones y Servicios que no soportan IPv6)	Identificar brechas de los componentes de la infraestructura tecnológica de SUNAT	3 meses	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Gerencia de Desarrollo de Sistemas	6
	Actualización y Adquisiciones	Actualización de SW para que funcionen con IPv4/IPv6: • Nodos principales de red • Servidores • Estaciones de Trabajo • Equipos end-point. • Aplicaciones	9 meses		
		Adquisiciones de Sw o Hw para reemplazar a equipos o SW que no soportan IPv6 y herramientas de Monitoreo para IPv6.	6 meses		
III, IV y V: ALCANCE DE INFRAESTRUCTURA SUNAT					5

III.- IMPLEMENTACIÓN: CONFIGURACION / PRUEBAS CON UN SERVICIO	Plan de Migración IPv6	Router principales. Firewalls nodos. Switches CORE. Switches de Acceso. Servidores. Segmentos de Red.	1 mes	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Gerencia de Desarrollo de Sistemas /Oficina de Seguridad Informática	7
	Implementar mecanismo de transición: doble pila. Entregables asociados a la realización de las actividades de configuración.	Ruteadores principales y/o Equipos de capa3.	1 mes		
	Asignación de protocolo de enrutamiento de IPv6 y políticas.	Ruteadores principales.	0.5 mes		
	Pruebas de migración con un servicio Entregables Asociados a la realización de pruebas de funcionalidad, seguridad, configuraciones de HW, SW, servicios, conectividad, entre otros.	**Portal Web** Estabilidad Monitoreo.	3 meses.	Gerencia de Calidad de Sistemas / Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Oficina de Seguridad Informática	8
IV.- CONFIGURACION SERVICIOS BASICOS DE RED	Habilitar IPv6 en los servicios básicos de red.	**DNS-Proxy-DHCP**. Mecanismo doble pila Estabilidad Monitoreo	1 mes	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Oficina de Seguridad Informática	7
	Habilitar IPv6 en equipos de usuarios (estaciones de trabajo).	Red INSI Estabilidad Monitoreo	2 meses		
		Otras redes SUNAT.	6 meses		
V.- CONFIGURACIÓN ENDPOINT SERVIDORES DE PRODUCCIÒN	Habilitar IPv6 equipos end-points.	Impresoras. Marcadores. Equipos de control. Equipos Tx/Rx de RF. Estabilidad Monitoreo.	3 meses	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios/ Oficina de Seguridad Informática	7
	Habilitar IPv6 Servidores.	Servidores de Datacenter	3 meses		
POST IMPLEMENTACIÓN	Estabilización y Monitoreo	Monitoreo y afinamiento de funcionalidades Seguridad de la plataforma y servicios	3 meses	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Gerencia de Calidad de Sistemas / Gerencia de Desarrollo de Sistemas / Oficina de Seguridad Informática	-
	Inventario post implementación.	De la plataforma de TI - IPv6	1 mes	Gerencia de Arquitectura / Gerencia de Operaciones y Soporte a Usuarios / Gerencia de Desarrollo de Sistemas	-
		TOTAL	**45.5 meses**		

Fuente propia SUNAT

DIAGRAMA DE GANTT

1	Nombre de la tarea	Fecha de I	Fecha fina	% Completado	Duración	Predecesores
2	**TAREAS IPv6 SUNAT**					
3	**Fase I Preliminar**	**10/08/18**	**10/10/18**	**0%**	**44d**	
4	Comunicación y Sensibilizacion	10/08/18	10/09/18		22d	
5	Capacitacion	10/08/18	10/09/18		22d	
6	Configurar Piloto o Maqueta : Web	11/09/18	10/10/18	0%	22d	4
7	**Fase II Preparación de la Plataforma**	**11/09/18**	**12/06/19**	**0%**	**261d**	
8	Relevamiento Informacion	11/09/18	11/12/18	0%	66d	
9	Actualizaciones	12/12/18	10/09/19		195d	8; 5
10	Adquisiciones	12/12/18	12/06/19		131d	
11	**Fase III Configuración de un Servicio**	**11/09/19**	**26/02/20**	**0%**	**121d**	
12	Plan de Migración IPv6	11/09/19	10/10/19	0%	22d	9; 10
13	Implementar Doble Pila	11/10/19	11/11/19		22d	12
14	Configuración enrutamiento IPv6	12/11/19	26/11/19		11d	
15	Configuración Portal Web (Planas)	27/11/19	26/02/20		66d	
16	**Fase IV Configuración Servicios Básicos Red**	**27/02/20**	**04/01/21**	**0%**	**223d**	
17	Configurar IPv6 DNS-Proxy y DHCP	27/02/20	27/03/20	0%	22d	
18	Configurar Red INSI a IPv6	30/03/20	29/05/20		45d	
19	Configurar otras Redes SUNAT a IPv6	01/06/20	04/01/21		156d	
20	**Fase V Configuración EndPoint y Servidores**	**05/01/21**	**06/07/21**	**0%**	**131d**	
21	Configurar equipos end-points a IPv6	05/01/21	05/04/21	0%	65d	
22	Configurar Servidores Producción a IPv6	06/04/21	06/07/21		66d	
23	**Fase VI Post Implementación**	**07/07/21**	**09/11/21**	**0%**	**90d**	
24	Estabilización y Monitoreo	07/07/21	07/10/21	0%	67d	
25	Inventario Final	08/10/21	09/11/21		23d	



ANEXO 2: RIESGOS INICIALES IDENTIFICADOS Y EVALUADOS A LO LARGO DE LAS DIFERENTES FASES DEL PROYECTO PARA SU POSTERIOR ANALISIS

RIESGOS	IMPACTO	PROBAB.	VALORACIÓN	ACCIONES PARA MITIGAR	FASE
Falta de capacitación del personal técnico.	Alto	Alta	Alto	Refuerzo de conocimientos relacionados al protocolo IPv6 al personal.	Diagnóstico, Remediación y Configuración
Pérdida de información de los equipos.	Alto	Baja	Medio	Respaldo de toda la información de la plataforma de TI.	Remediación y Configuración
Inestabilidad de aplicaciones y SO. Incompatibilidades de SW y HW.	Alto	Media	Alto	Revisión y configuración del código de las aplicaciones y SO. Contar con la permanente asistencia técnica del fabricante. Descargar las actualizaciones necesarias.	Configuración
Daños físicos en los equipos.	Alto	Baja	Medio	Mantenimiento y revisión continúa de los equipos (configuraciones). Alcance de los contratos de soporte y mantenimiento.	Configuración
Tiempo extremo en la adaptación al IPv6.	Medio	Media	Medio	Control y seguimiento del Proyecto de Migración con la gestión de un Jefe de Proyecto Informático.	Configuración
Falta de apoyo Institucional.	Alto	Baja	Medio	Contar con el apoyo permanente del Intendente de la INSI como sponsor del proyecto.	Todas las Fases.

Fuente propia SUNAT

Leyenda:

Impacto: Alto, Medio y Bajo
Probabilidad: Alta, Media y Baja
Cuadro de Valoración:

Impacto				
Alto	**M**	**A**	**A**
Medio	**M**	**M**	**A**
Bajo	**B**	**B**	**M**
	Baja	Media	Alta

Probabilidad

ANEXO 3: FORMATOS DE TRABAJO PARA EL RELEVAMIENTO DE INFORMACIÓN

FORMATO DE INVENTARIO Y CONTROL DE EQUIPOS CONFIGURADOS EN IPv6

Ítem	Cantidad	Equipo	Observaciones	Tiempo de renovación de equipo	Indicador de Control: % equipos configurados IPv6			
					Año 1	Año 2	Año 3	Año 4
01	4	Switches	CORE	5 años	100%			
02	8	Routers	Enlaces Internet	3 años	50%			
03	4	Balanceadores Locales	Servicios Internet	5 años	0%			
04	4	Balanceadores Globales	Servicios Internet	5 años	100%			
05	4	Firewall	Servicios Internet	5 años	50%			
06	700	Switches	Borde	5 años	90%			
07	2	Switches	DMZ	5 años	50%			

DETALLE DE EQUIPOS DE REDES

Modelo	#Serie	Dirección IP	Interfaces	Versión IOS	Soporte IPv6(Si/No)	Brechas
						Upgrade BIOS
						Reemplazo

FORMATO DE INVENTARIO DE ESTACIONES DE TRABAJOS Y EQUIPO DE OFICINA

Ítem	Cantidad	Equipo	Sistema Operativo	Tiempo de renovación de equipo	Indicador de Control: % equipos configurados IPv6			
					Año1	Año2	Año3	Año4
01	13,970	Computadora de Escritorio	Windows 7 64 bits	3 años	100%			
02	2,801	Computadora Portátil	Windows 7 64 bits	3 años	100%			
03	4	Tableta	Mac OS	1 año	100%			
04	6	Computadora para Diseño	Mac OS	3 años	100%			
05								
06								

DETALLE DE ESTACIONES DE TRABAJO Y EQUIPOS DE OFICINA

Marca	Modelo	Procesador	Memoria	Sistema Operativo	Soporte IPv6/Si/No)	Brechas
					No	Upgrade BIOS

FORMATO DE INVENTARIO DE SERVIDORES DE PRODUCCIÓN

Ítem	Cantidad	Tipo de servidor	Sistema Operativo	Tiempo de renovación de equipo	Indicador de Control: % servidores configurados IPv6			
					Año1	Año2	Año3	Año4
01	2	Power 795	AIX7.1 64bits	5 años	100%			
02	6	Power 740	AIX7.1 64bits	5 años	100%			
03	1	Power 770	AIX7.1 64bits	5 años	100%			
04	3	Power 850	AIX7.1 64bits	5 años	100%			
05								
06								

DETALLE DE SERVIDORES

Marca	Modelo	Procesador	Memoria	Tarjeta de RED	Sistema Operativo	Soporte IPv6(Si/No)	Brechas
						No	Upgrade SO Upgrade drivers

FORMATO DE INVENTARIO DE APLICACIONES DE LA INSTITUCIÓN

Ítem	Nombre de la aplicación	Descripción funcional	Tiempo de adquisición o desarrollo	Soporta IPv6 (Si/No)	Brechas
01	Aplicación 1	Negocio	5 años	No	Actualizar librerías
02	Aplicación 2	Administrativo	10 años	No	Modificaciones en el código.
03					
04					
05					
06					

FORMATO DE INVENTARIO DE DIRECCIONES IPv4 – IPv6 POR SEDE SUNAT

SEDE SUNAT	DIRECCIÓN DE RED IPv4	MASCARA IPv4	DIRECCCIÓN IPv6 POR ASIGNAR	MASCARA IPv6 POR ASIGNAR
Wilson	150.200.0.0	255.255.0.0		
Miraflores	10.2.0.0	255.255.0.0		
San Isidro	10.0.0.0	255.255.0.0		

FORMATO DE INVENTARIO DE DIRECCIONES IPv4 – IPv6 POR SEGMENTO

NOMBRE SEGMENTO DMZ SAN ISIDRO	#VLAN	DIRECCIÓN DE RED IPv4	MASCARA IPv4	DIRECCIÓN RED IPv6 POR ASIGNAR	MASCARA IPv6 POR ASIGNAR
Sello de Tiempo	300	192.168.20.0	255.255.255.240		
Call Center	75	172.30.0	255.255.255.0		
DMZ1 Calidad	34	192.168.34.0	255.255.255.0		

FORMATO CONTROL DE INVENTARIO CONFIGURACIONES IPv4 – IPv6

#	Equipo	Siglas	IPv4	Ejemplo IPv6
1	Router (LAN)	ROU	NET.net.1.X	2001:1388:1::1:x
2	Server	SRV	NET.net.2.X	2001:1388:1::2:x
3	Concentrador	SW	NET.net.3.X	2001:1388:1::3:x
4	Radioenlaces	WIR	NET.net.4.X	2001:1388:1::4:x
5	Central Telefónica	PBX	NET.net.5.X	2001:1388:1::5:x
6	Gateway	GWY	NET.net.6.X	2001:1388:1::6:x

ANEXO 4: REFERENCIAS BIBLIOGRÁFICAS

- Información del Portal Srvtele INSI-SUNAT.
- TOMY B., M. 2017. Modelo de Referencia de Transición de IPv4 a IPv6 para el Sector Gobierno del Perú. Tesis Mag. PUCP, Fac. Ing. Telec. 75 p.
- SARAVIA C., J. 2015. Desarrollo de un Plan de Transición para la Migración de IPv4 a IPv6, utilizando la Metodología PPDIOO en La Red de la Universidad Autónoma del Perú, Tesis Título. Universidad Autónoma del Perú, Fac. Cien. 61 p.
- HUAITALLA H., R. 2014. Solución de Conectividad en IPv6 a la Red Académica Avanzada Peruana para la Universidad Nacional de Santa, Tesis Título, UNI, Fac, Ing. Elec. 119 p.
- CLAVIJO B.L, RAMIREZ C.M.,2010. Configuración e Implementación de Redes de Datos con Direccionamientos IPv4 E IPv6, Facultad de Ingeniería de Telecomunicaciones. Medellín, Colombia .69p
- MERA T., G. 2016. Propuesta de Transición de Servicios de IPv4 A IPv6 para la Red de Datos Cableada del Gobierno Autónomo Descentralizado Municipal San Miguel de Ibarra, Ecuador. 16 p. (Disponible en http://repositorio.utn.edu.ec/handle/123456789/5707).
- LANDY R., D. 2013. Propuesta de un Plan de Implementación para la migración a IPv6 en la red de la Universidad Politécnica Salesiana Sede Cuenca, Ecuador. Tesis Título. Univ. Politéc. Salesiana Sede Cuenca. 179 p.
- JARA S., F. 2009. Estudio e Implementación de una Red IPv6 en la UTFSM, Tesis Título. Fac. Ing, Valparaíso, Chile. 95 p.
- CARMONA A.P, ULLOA S. R, 2003, Configuración de Servicios de Internet con soporte de Protocolo Internet versión 6 sobre GNU/Linux, Tesis. Universidad de la Frontera de Temuco, Chile .126p
- CASTRO G., N. 2010. Introducción de IPv6 en Telecom Argentina. LAGNOC, San Pablo, Brasil. 35 p. (Disponible en www.cu.ipv6tf.org/lacnic14/lacnog/IPV6_Presentacion-Draft_final.pdf)
- Información del IPv6 Portal, http://portalipv6.lacnic.net/articulos/
- Información del Portal Cisco, https://supportforums.cisco.com/t5/seguridad-documentos/planificaci%C3%B3n-y-despliegue-de-ipv6-faq/ta-p/3155378
- Información del Portal Salle, http://blogs.salleurl.edu/networking-and-internet-technologies/category/ipv6/
- Información del Portal Vincke, https://www.vyncke.org/ipv6status/detailed.php?country=ar&type=Gov
- Información del Portal NRO, https://www.nro.net/
- Información del Portal lacnic, http://www.lacnic.net/agotamiento