RESOLUCIÓN DE CONSEJO UNIVERSITARIO N° 0225-2024

Arequipa, 28 de mayo de 2024.

Visto el Oficio Nº 149-2024-UM-OPPM/UNSA de la Unidad de Modernización de la Oficina de Planeamiento, Presupuesto y Modernización, mediante el cual, remite para aprobación el Proyecto de "PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPv4) A VERSIÓN 6 (IPv6)".

CONSIDERANDO:

Que, la Universidad Nacional de San Agustín de Arequipa está constituida conforme a la Ley N° 30220, Ley Universitaria, y se rige por sus respectivos estatutos y reglamentos, siendo una comunidad académica orientada a la investigación y a la docencia, que brinda una formación humanista, ética, científica y tecnológica con una clara conciencia de nuestro país como realidad multicultural.

Que, el artículo 8° de la citada Ley Nº 30220, Ley Universitaria, concordante con el artículo 8° incisos 1, 2, 4 y 5 del Estatuto Universitario, establece respecto a la autonomía universitaria que: *"(…) La Universidad se rige con la autonomía inherente a las Universidades y se ejerce de conformidad con lo establecido en la Constitución, la Ley y demás normativas aplicables. Esta autonomía se manifiesta en los siguientes regímenes: **8.1 Normativo**, implica la potestad autodeterminativa para la creación de normas internas (Estatuto y Reglamentos) destinadas a regular la institucionalidad universitaria. **8.2 De gobierno**, implica la potestad autodeterminativa para estructurar, organizar y conducir la institución universitaria, con atención a su naturaleza, características y necesidades. Es formalmente dependiente del régimen normativo (…) **8.4 Administrativo**, implica la potestad autodeterminativa para establecer los principios, técnicas y prácticas de sistemas de gestión, tendientes a facilitar la consecución de los fines de la institución universitaria, incluyendo la organización y administración del escalafón de su personal docente y administrativo (…)".*

Que, mediante Decreto Supremo N° 081-2017-PCM, "Decreto Supremo que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública", se estableció una obligación para todas las entidades de la administración pública de elaborar un Plan de Transición al Protocolo IPv6, el cual deberá ser aprobado por los titulares de las entidades.

Que, en consecuencia, mediante documento del visto, la Unidad de Modernización, remite el Proyecto del "PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPv4) A VERSIÓN 6 (IPv6)", elaborado en coordinación con la Oficina de Tecnologías de la Información, el cual tiene como objetivo general: *"Diseñar el plan de transición del protocolo IPv4 a IPv6 en redes de datos, acorde a los lineamientos del Decreto Supremo Nº 081-2017-PCM, en la red de comunicaciones de la Universidad Nacional de San Agustín de Arequipa".*

Que, en atención a lo señalado en los párrafos precedentes, el Consejo Universitario en su **sesión del 24 de abril de 2024**, acordó aprobar el "PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPV4) A VERSIÓN 6 (IPV6)", previa verificación de la disponibilidad presupuestal por parte de la Oficina de Planeamiento, Presupuesto y Modernización.

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA SECRETARIA GENERAL

Que, a través del Oficio N° 0443-2024-OUPL-UNSA, la Oficina de Planeamiento, Presupuesto y Modernización, señala que para el ejercicio fiscal 2024, se cuenta con disponibilidad presupuestal por el monto de S/ 45,900.00 (Cuarenta y Cinco Mil Novecientos con 00/100 soles), para atender lo solicitado en el "PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPV4) A VERSIÓN 6 (IPV6)".

Por estas consideraciones, estando a lo acordado y conforme a las atribuciones conferidas al Consejo Universitario por la Ley Universitaria Nº 30220,

SE RESUELVE:

1. **APROBAR** el **"PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPV4) A VERSIÓN 6 (IPV6)".**

2. **DISPONER** que la **Oficina de Tecnologías de la Información**, en coordinación con la Dirección General de Administración, será la encargada de velar por el cumplimiento del **"PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPV4) A VERSIÓN 6 (IPV6)".**

3. **ENCARGAR** a **la Oficina de Tecnologías de la Información,** en coordinación con la **Oficina de Comunicación e Imagen Institucional**, la publicación de la presente Resolución y del **"PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPV4) A VERSIÓN 6 (IPV6)"**, en el Portal Web Institucional.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

DRA. RUTH MARITZA CHIRINOS LAZO
SECRETARIA GENERAL

DR. HUGO JOSE ROJAS FLORES
RECTOR

Cc.: VRA, VRI, DIGA, DSA, DA, OTI, OCII, UM y Archivo (exp).
Expediente N° 1028709-2021
/ejps

UNIDAD DE MODERNIZACIÓN	Versión: 1 Aprobado con RCU N° -2024 de fecha / /2024

UNSA
UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

PLAN DE TRANSICIÓN DEL PROTOCOLO INTERNET 4 (IPv4) A VERSIÓN 6 (IPv6)

	Nombres y Apellidos	Dependencia	Firma	Fecha
Elaborado por:	Mg. Alvaro Javier Montes de Oca Beltrán	Oficina de Tecnologías de la Información	Firmado digitalmente por: MONTES DE OCA BELTRAN Alvaro Javier FAU 20103646499 hard 05/02/24 Motivo: En señal de conformidad Fecha: 28/05/2024 16:57:47-0500	
Revisado por:	Dr. Marco Antonio Camacho Zárate	Unidad de Modernización		25/02/24
Aprobado por:	Dr. Hugo José Rojas Flores	Consejo Universitario	RECTORADO	/04/24

1. INTRODUCCIÓN

El Protocolo de Internet (Internet Protocol IP) es un conjunto de reglas para la comunicación de datos digitales, clasificado funcionalmente en la capa de red según el modelo internacional OSI.

El diseño del protocolo IP se realizó presuponiendo que la entrega de los paquetes de datos sería no confiable. Por ello, IP tratará de realizar la entrega del mejor modo posible, mediante técnicas de encaminamiento, sin garantías de alcanzar el destino final, pero tratando de buscar la mejor ruta o camino entre las conocidas por el dispositivo de red que esté usando IP.

Los datos en una red de comunicaciones basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un dispositivo intente enviar paquetes a otro con el que no se había comunicado antes.

IP provee un servicio de datagramas no fiable (también llamado de "mejor esfuerzo": lo hará lo mejor posible, pero sin ofrecer garantías). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP. Las cabeceras IP contienen las direcciones de los dispositivos de red de origen y destino (direcciones IP), direcciones que serán usadas por los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en el Internet de hoy. El actual y más popular protocolo de red es IPv4, siendo su sucesor el IPv6; poco a poco Internet está agotando las direcciones IPv4 disponibles, por lo que IPv6 utiliza direcciones de origen y destino de 128 bits, muchas más direcciones que las que provee IPv4 con 32 bits. Las versiones de IP, de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada en un protocolo experimental. Otros números han sido asignados, usualmente en más protocolos experimentales, pero no han sido muy extendidos.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

Los dispositivos de una red de comunicaciones, como las computadoras, impresoras, teléfonos IP, etc., conectados a la red, son identificados por etiquetas de longitud fija y no deben duplicarse en la mencionada red de comunicaciones.

Dichas etiquetas utilizadas por el protocolo son llamadas direcciones IP, están formadas por 32 bits y se asignan al adaptador de red de cada dispositivo que forme parte de una red de datos; las direcciones IP no son siempre las mismas 7 cada equipo, puede que se asigne una IP diferente cada vez que un dispositivo se conecta a la red, en este caso se trata de direcciones IP dinámicas; por el contrario, si es necesario que la etiqueta sea siempre la misma se llamará dirección IP fija.

Los sistemas de Internet se basan en la pila de protocolos conocida como TCP/IP, cada uno de los cuales encargado de una función de comunicación específica y determinando en conjunto la forma en que los dispositivos se comunican. Actualmente en el nivel de INTERNET de la pila de protocolo TCP/IP que cumple la función de direccionamiento y enrutamiento, se utilizan dos Protocolos de Internet.

El primero conocido como protocolo de Internet versión 4 (de ahora en adelante IPv4); creado desde 1960 con fines experimentales de uso de internet. Dispone aproximadamente de 40 millones de direcciones IP, las cuáles debido al crecimiento exponencial del servicio a nivel mundial, ya están agotadas según la Corporación de Internet, para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés). Frente a este problema, alrededor de los años 90 el Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés) desarrolló el Protocolo de Internet versión 6, o IPv6, el cual dispone de alrededor de 340 Sextillones de direcciones IP.

Tan sólo en Latinoamérica, según el Registro de Direcciones de Internet de América Latina y el Caribe (LACNIC), en el 2014, la provisión de direcciones IPv4 para la región se agotó y comenzaron a regir políticas restrictivas de entrega de direcciones IPv4 en el continente. Además, entran en vigor las políticas de "agotamiento gradual" y "nuevos miembros" que establecen modificaciones en los procedimientos y requerimientos de entrega de recursos IPv4. También se activa la política de "Transferencias de bloques IPv4 dentro de la región LACNIC" que habilita y regula la transferencia de recursos entre entidades de la región.

El protocolo IPv6, está disponible para su implementación segura y probada, desde el año 2012 y se plantea como una solución definitiva a largo plazo, pues se propone una adopción paulatina de IPv6 en coexistencia con IPv4 en un mecanismo denominado Dual Stack, lo que facilitaría a prestadores de servicios de Internet, empresas, universidades, hogares y otros usuarios, no interrumpir ni afectar su infraestructura de red.

En este documento se presenta una propuesta de planeación de la transición del protocolo de Internet versión 4 a versión 6, contemplando únicamente las fases de diagnóstico y planeación en la red LAN del campus universitario y de implementación en los servidores del segmento de red de la DMZ y algunos equipos del segmento de red de la OTI.

UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA SECRETARIA GENERAL

2. BASE LEGAL

2.1. Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado.
2.2. Ley Universitaria N° 30220 y Estatuto de la Universidad Nacional de San Agustín de Arequipa, aprobado, promulgado y publicado mediante Resolución de Asamblea Estatutaria N° 001-2015-UNSA-AE del 10 de noviembre de 2015; con modificaciones aprobadas en sesiones de Asamblea Universitaria de fechas: 11 de abril de 2016 con RAU N° 001-2016, 26 de julio, 25 de agosto, 14 de septiembre de 2016, 28 de setiembre de 2016 con RAU N° 007-2016, del 18 de diciembre de 2017, 26 de diciembre de 2017 con RAU N° 0009-2017, 28 de diciembre del 2017, 29 de diciembre de 2017 con RAU N° 0010-2017, 20 de noviembre de 2019 con RAU N°008-2019, 11 de setiembre de 2021 con RAU N° 006-2021, 14 de octubre de 2021 con RAU N° 009-2021, 20 de junio de 2022 y 14 de julio de 2022 con RAU N° 017-2022 y 10 de octubre de 2023 con RAU N° 0013-2023.
2.3. Decreto Supremo Nº 081-2013-PCM, aprueba la Política Nacional de Gobierno Electrónico.
2.4. Decreto Supremo Nº 081-2017-PCM, aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública.

3. OBJETIVOS DEL PLAN DE TRANSICIÓN

3.1. Objetivo general

Diseñar el plan de transición del protocolo IPv4 a IPv6 en redes de datos, acorde a los lineamientos del Decreto Supremo Nº 081-2017-PCM, en la red de comunicaciones de la Universidad Nacional de San Agustín de Arequipa.

3.2. Objetivos específicos

3.2.1. Aumentar la disponibilidad de Direcciones IP.
3.2.2. Garantizar la continuidad de los Servicios de Internet.
3.2.3. Mejorar la Seguridad.
3.2.4. Facilitar el despliegue de Nuevos Servicios.
3.2.5. Promover la innovación y el desarrollo Tecnológico.
3.2.6. Minimizar la Dependencia de Traducción de Direcciones (NAT).
3.2.7. Garantizar la Interoperabilidad entre sistemas IPv4 e IPv6.
3.2.8. Capacitar y concientizar a la comunidad sobre el uso y ventajas de IPv6.
3.2.9. Cumplimiento de los requisitos regulatorios y recomendaciones de los organismos competentes.
3.2.10. Monitoreo y evaluación continua de los servicios de internet.
3.2.11. Elaborar y validar el inventario de activos de información.
3.2.12. Analizar y desarrollar el plan de diagnóstico.
3.2.13. Generar el plan de trabajo para la adopción del protocolo IPv6.

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA SECRETARIA GENERAL

4. ALCANCE DEL PLAN DE TRANSICIÓN

Este proyecto busca proponer un "plan de transición" de IPv4 a IPv6 en redes de datos, teniendo en cuenta las instrucciones brindadas en el D.S. 081-2017-PCM, donde se especifica que al momento de hacer la planeación de la transición en la UNSA; se deben realizar actividades concretas como:

4.1. Implementación del protocolo IPv6, incluyendo un cronograma con actividades (configuración de servicios, configuración del protocolo IPv6, formulación de política de seguridad, entre otros), plazos, responsables y entregables a fin de la implementación del IPv6 en la UNSA. Debe ser coordinado con el Oficial de Seguridad de la Información.

4.2. Realización de Pruebas, incluyendo un cronograma con actividades (pruebas de funcionalidad, calidad del servicio, compatibilidad de los equipos y monitoreo del IPv6, pruebas frente a las políticas de seguridad, afinamiento de las configuraciones realizadas, entre otros), plazos, responsables y entregables para el desarrollo de pruebas en la UNSA.

4.3. Capacitación y sensibilización, incluyendo un cronograma con actividades, plazos, y responsables de la capacitación a especialistas en Tecnologías de Información (TI) y sensibilización a funcionarios en el protocolo IPv6.

La creación de este documento debe estandarizar el proceso de transición a IPv6 y vale la pena mencionar que este se limita al desarrollo de la fase de planeación de la migración a IPv6, lo que implica que no habrá descrito ningún proceso que tenga que ver con el diseño de la red necesaria para la migración o con la implementación del nuevo protocolo.

5. DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

5.1. Inventario de activos informáticos:

El proceso de recolección de la información necesaria en el inventario de Hardware y Software se realizará en cada una de las dependencias de la UNSA, de manera consecutiva se organizará la información de acuerdo con las plantillas sugeridas, con esta base se establece la información concerniente a equipos de cómputo, equipos de comunicación, servidores, aplicativos, equipos de impresión y otros dispositivos conectados en red. Se debe considerar el correcto funcionamiento de dichos equipos en la red de datos de la entidad, teniendo en cuenta su uso en las actividades cotidianas.

5.2. Equipos de cómputo, plazos, responsables, inventario de Hardware y Software

5.2.1. Plazos: No corresponde
5.2.2. Responsables:
5.2.2.1. Subunidad de Control Patrimonial y Almacenes: Inventario Hardware.

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA SECRETARIA GENERAL

5.2.2.2. Oficina de Tecnologías de la Información: Inventario Software.

5.2.3. Inventario de Hardware

La UNSA cuenta con una infraestructura informática, la que se encuentra registrada en el inventario 2024, descrito al detalle en la siguiente dirección URL:

DirecciónURL: https://www.unsa.edu.pe/IPv6/Bienes202403.pdf

Resumen:

DENOMINACIÓN	CANTIDAD	Soporte IPv6
COMPUTADORA PERSONAL PORTÁTIL	1717	SI
COMPUTADORA PERSONAL ESCRITORIO (UNIDAD CENTRAL DE PROCESO – CPU)	6518	SI
IMPRESORA CONECTADA EN RED	1408	SI
PUNTO DE ACCESO INALÁMBRICO (ACCESS POINT WIRELESS)	179	SI
RUTEADOR DE RED (ROUTER)	192	SI
SWITCH PARA RED	383	SI
SERVIDOR	8	SI
SISTEMA DE ALMACENAMIENTO DE DISCOS EXTERNOS	2	SI

5.2.4. Inventario de Software

En cuanto a los sistemas operativos y versiones de los mismos, se encuentran registrados en el inventario 2024, descrito al detalle en la siguiente dirección URL:

Dirección URL : https://www.unsa.edu.pe/IPv6/Bienes202403.pdf

5.3. Infraestructura Tecnológica

Dentro de los dispositivos de red, el 98% que soportan la infraestructura a nivel de campus están formados por switches administrables de capa 2, con soporte de VLANs 802.1q y conexiones TRONCALES, los cuales, al no realizar función de enrutamiento, no se requieren sean compatibles con IPv6. Los switches CORE y DISTRIBUCIÓN que realizan enrutamiento entre VLANs requieren ser actualizados, por lo que se solicitó la adquisición por renovación tecnológica, el cual se encuentra en proceso de adquisición. En cuanto a los equipos de acceso inalámbrico, que se cuentan en el campus, soportan IPv6. Los dispositivos de borde y seguridad, proporcionados por el proveedor de servicio para la conectividad a Internet, también soportan IPv6.

Dirección URL : https://www.unsa.edu.pe/IPv6/Infraestructura-RED.jpg

5.4. Aplicaciones y servicios que no soportan IPv6

Los servidores y aplicaciones informáticas que no trabajan bajo la administración de la Oficina de Tecnologías de la Información, no soportan IPv6.

5.5. Aplicaciones y servicios que soportan IPv6

En cuanto al sistema de almacenamiento (SAN) y servidores que trabajan en clúster para crear máquinas virtuales, todos los que están bajo la administración de la OTI, soportan IPv6.

- **Admisión Pregrado:**
  https://apps.unsa.edu.pe/sisadmision/public/acceso-admin/
- **Admisión Posgrado:**
  https://apps.unsa.edu.pe/sisadmision-posgrado/public/acceso-admin
- **Sistema de Trámite Documentario (Tramited):**
  https://ouis.unsa.edu.pe/tramited
- **Helpdesk:**
  https://apps.unsa.edu.pe/help-desk/
- **Sistema de Monitoreo (Sismo):**
  http://sismo.unsa.edu.pe/bytsig
- **Sistema de Convenios:**
  https://apps.unsa.edu.pe/convenio/public/
- **Sistema de Recursos Humanos:**
  https://desarrollo.unsa.edu.pe/rrhh/beta/rrhh/public/acceso-admin
- **Sistema nuevo de Bibliotecas:**
  https://apps.unsa.edu.pe/bibliotecas_unsa_2/public/login
- **Sistema de caja:**
  https://ouis.unsa.edu.pe/siscaja/
- **Sistema de grados y títulos:**
  https://sg.unsa.edu.pe/sisgrad
- **(Opacdr):**
  https://ouis.unsa.edu.pe/talleres/
- **Unsapay:**
  https://ouis.unsa.edu.pe/unsapay/login

UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTIN DE AREQUIPA SECRETARIA GENERAL

- **Unsa Center**
  https://apps.unsa.edu.pe/unsacenter/public/

- **Sistema de comedor:**
  https://apps.unsa.edu.pe/siscom/public/login

5.6. Evaluación de riesgos, para su posterior análisis.

La gestión de riesgos es un proceso continuo, por eso es necesario usar un plan de tratamiento de riesgos con la finalidad de implementar las recomendaciones y mejorar la toma de decisiones. En consecuencia, los riesgos son valorados en función al impacto que podría generar al logro de los objetivos y su probabilidad de ocurrencia.

N°	Riesgo	Impacto	Probabilidad	Valoración		
				Alta	Media	Baja
1	Pérdida de información	Alto	Baja		X	
2	No disponibilidad de repuestos de los equipos obsoletos,	Alto	Baja		X	
3	Incompatibilidad de hardware (Equipos informáticos y de comunicaciones)	Alto	Baja		X	
4	Inestabilidad de las aplicaciones	Alto	Media	X		
5	Problemas de conectividad con las Oficinas y Sedes	Alto	Media	X		
6	Problemas con los servicios de Internet.	Alto	Media	X		
7	Problemas de funcionamiento del sistema operativo	Alto	Media	X		
8	Incompatibilidad de las aplicaciones con el sistema operativo	Alto	Media	X		

Cuadro de Valoración:

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

5.6.1. Infraestructura Informática

N°	Descripción	Cantidad	Soporte IPv4	Soporte IPv6	Riesgo
1	Switch Core	1	SI	SI	Bajo
2	Switch Distribución	3	SI	SI	Bajo
3	Switch Acceso	379	SI	NO	Bajo
4	Punto de Acceso Inalámbrico (Access Point Wireless)	179	SI	SI	Bajo
5	Ruteador de red (router)	192	SI	SI	Bajo
6	Servidor	8	SI	SI	Bajo
7	Sistema de Almacenamiento de Discos Externos	2	SI	SI	Bajo
8	Computadora Personal Portátil	1717	SI	SI	Bajo

9	Computadora Personal Escritorio	6518	SI	SI	Bajo
10	Impresora Conectada En Red	1408	SI	SI	Bajo

5.6.2. Servicios

N°	Descripción	Cantidad	Soporte IPv4	Soporte IPv6	Riesgo
1	Servicio de Internet	1	SI	SI	Bajo
2	Servicio de Seguridad Administrada	1	SI	SI	Bajo
3	Servicio de Ciberseguridad y Análisis de Vulnerabilidades	1	SI	Si	Bajo
4	Google Workspace for Education Plus	28000	SI	SI	Bajo

5.6.3. Aplicaciones Informáticas

N°	Descripción	Cantidad	Soporte IPv4	Soporte IPv6	Riesgo
1	Aplicativos Internos	15	SI	SI	Bajo

5.6.4. Conclusiones del Diagnóstico de la Infraestructura Tecnológica

a) Se han identificado equipos informáticos que no soportan y no serían compatibles con el protocolo IPv6, pero no son relevantes para la migración al protocolo IPv6.
b) Es necesario mantener actualizado el inventario a detalle, de los activos informáticos (hardware, software y aplicaciones) a fin de tener un panorama general de la compatibilidad al momento de la migración al protocolo IPv6.

6. IMPLEMENTACIÓN DEL PROTOCOLO IPv6

Cronograma con actividades (configuración de servicios, configuración del protocolo IPv6, formulación de política de seguridad, entre otros), plazos, responsables y entregables de la implementación del IPv6 en la UNSA.

Ver anexo 12.2 al final del documento.

7. REALIZACIÓN DE PRUEBAS

Cronograma con actividades (pruebas de funcionalidad, calidad del servicio, compatibilidad de los equipos y monitoreo del IPv6, pruebas frente a las políticas de seguridad, afinamiento de las configuraciones realizadas, entre otros), plazos, responsables y entregables para desarrollo de pruebas de la universidad.

Ver Anexo 12.2 al final del documento.

8. CAPACITACIÓN Y SENSIBILIZACIÓN

Cronograma con actividades, plazos y responsables de la capacitación a especialistas en Tecnologías de Información (TI) y sensibilización a funcionarios en el protocolo IPv6.

Ver Anexo 12.2 al final del documento.

9. PRESUPUESTO ESTIMADO

El presupuesto está basado principalmente en horas-hombre de configuraciones y capacitaciones.

Implementación del protocolo IPv6		Plazos		Presupuesto Estimado
Planificación y Evaluación		Jefatura OTI/UITST	Elaboración Plan de trabajo y Anexos	Soles S/.
1.1	Formación del equipo de implementación	2 semanas	Jefatura OTI/UITST	
	a)	Selección de un equipo responsable de la implementación	40 horas	450.00
	b)	Identificar Roles y Responsabilidades	40 horas	450.00
1.2	Evaluación de la Infraestructura Anual	4 semanas	Responsable Infraestructura de red	
	a)	Realizar un inventario de la red actual.	120 horas	1,350.00
	b)	Evaluar el soporte actual para IPv6.	40 horas	450.00
	c)	Identificar dispositivos y aplicaciones que necesitan actualizarse.	40 horas	450.00
1.3	Establecimiento de Objetivos y Alcance	2 semanas	Jefe de Equipo	
	a)	Definir metas específicas para la implementación de IPv6.	40 horas	450.00
	b)	Determinar el alcance de la implementación	40 horas	450.00
Diseño y Configuración		Jefe de Equipo	Informe del diseño y configuración	
2.1	Desarrollo de Políticas de IPv6	8 semanas	Responsable Infraestructura de red	
	a)	Establecer políticas de seguridad y asignación de direcciones IPv6.	80 horas	900.00
	b)	Definir políticas de enrutamiento y segmentación de red.	80 horas	900.00
	c)	Implementación de enrutamiento y VLANs en Switch y Routers	80 horas	900.00
	d)	creación de repositorio de respaldo de configuraciones	80 horas	900.00
2.2	Actualización de Equipos y Software	8 semanas	Responsable Inventario	
	a)	Identificar ubicación de equipos que requieren actualizaciones	120 horas	1,350.00
	b)	programación de visita en campo para actualizaciones	40 horas	450.00

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA RECTORADO

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA SECRETARIA GENERAL

	c)	Realizar actualizaciones según sea necesario.	240 horas	2,700.00
2.3	Configuración de Dispositivos de Red	4 semanas	Responsable actualización	
	a)	Configurar enrutadores, switches y firewalls para admitir IPv6.	80 horas	900.00
	b)	Implementar cambios en la infraestructura de red.	120 horas	1,350.00
2.4	Pruebas de Conectividad	2 semanas	Responsable Soporte IPv6	
	a)	Realizar pruebas de conectividad interna para comunicación IPv6.	40 horas	450.00
	b)	Verificar la interoperabilidad con sistemas y servicios externos.	40 horas	450.00
Implementación		Jefe de Equipo	Informe de implementación de IPv6	
3.1	Implementación Gradual en Segmentos de Red	20 semanas	Responsable actualización	
	a)	Implementar IPv6 en segmentos de red específicos de manera gradual.	180 horas	2,025.00
	b)	Monitorizar el rendimiento y solucionar problemas a medida que surgen.	120 horas	1,350.00
3.2	Migración de Servicios Críticos	16 semanas	Responsable Infraestructura de red	
	a)	Migrar servicios críticos a IPv6.	180 horas	2,025.00
	b)	Asegurarse de que los servicios esenciales funcionan sin problemas.	160 horas	1,800.00
3.3	Capacitación y Concientización	4 semanas	Responsable Soporte IPv6	
	a)	Proporcionar capacitación a personal de TI y usuarios finales sobre IPv6.	80 horas	900.00
	b)	Crear materiales de concientización para la comunidad universitaria.	40 horas	450.00
	c)	Documentar las lecciones aprendidas y actualizar la documentación.	40 horas	450.00
Evaluación y Optimización Continua		Jefe de Equipo	Informe del funcionamiento y operación del protocolo IPv6	
4.1	Monitoreo y Evaluación	12 semanas	Responsable Infraestructura de red	
	a)	Implementar herramientas de monitoreo para supervisar el tráfico IPv6.	240 horas	2,700.00
	b)	Evaluar el rendimiento y la seguridad de la red.	240 horas	2,700.00
4.2	Optimización Continua	36 semanas Responsable Soporte IPv6	1440 horas	16,200.00
			TOTAL	S/. 45,900.00

10. PLAZOS

Si bien la transición a IPv6 es un proceso cuyo despliegue es relativamente rápido debido a que actúa directamente en capa 3 y actualmente se cuenta con soporte y

activación del IPv6 en la mayoría de equipos de red, se debe tener en cuenta que la migración completa de la red es un proceso paulatino que normalmente, tarda años y a la vez se deben respetar los plazos definidos en el Decreto Supremo para las entidades de la Administración Pública:

10.1. Elaboración y aprobación del Planes de Transición: máximo de un (1) año, contado a partir de la vigencia del presente Decreto Supremo (***10 agosto 2017)***, el mismo que ***una vez aprobado deberá ser comunicado a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros***.

10.2. El Plan debe implementarse progresivamente en un plazo máximo de **cuatro (4) años** luego de su aprobación.

10.3. **Los plazos de implementación del Plan de Transición al Protocolo Internet versión 6 (IPv6) UNSA** entran en vigencia al día siguiente de su aprobación por resolución de Consejo Universitario.

11. CONCLUSIONES Y RECOMENDACIONES

El plan de transición a IPv6 diseñado de acuerdo con los lineamientos dados por el Decreto Supremo Nº 081-2017-PCM ayudará no sólo en el levantamiento de la información necesaria a fin de conocer y entender el funcionamiento actual de la red de datos de la entidad, sino que servirá a efecto encontrar las falencias a nivel de red que puedan retrasar el proceso de migración y sugerir estrategias con la finalidad de superarlas. De esta manera se obtendrá una visión mucho más detallada de la red de comunicaciones de la Universidad, que efectivamente permitirá obtener el diagnóstico e indicar el nivel de preparación de la UNSA y así empezar con la etapa de implementación de IPv6.

11.1. El despliegue del inventario de activos de información es un primer paso valioso que se dio en la determinación del porcentaje de compatibilidad y el grado de avance de la red en la implementación de IPv6, por ello se puede decir que es una de las actividades más importantes de la fase de planeación, pues con ésta se determinará en primera instancia que la UNSA está apta para comenzar con el proceso de migración.

11.2. El diseño del plan de trabajo está basado en el resultado del levantamiento de información y se sugieren actividades específicas de acuerdo a las necesidades de la misma. Si bien las técnicas de levantamiento de información, diagnóstico y determinación de actividades previas son procesos arbitrarios, es importante hacer más propias las tareas específicas de cada actividad del plan de trabajo, pues deben ir encaminadas a superar las falencias encontradas y buscar la manera de mitigar inconvenientes de acuerdo con ellas.

11.3. Se recomienda de aplicación inmediata a las respectivas dependencias, que se incluya el soporte del protocolo IPv6, en la elaboración de las

Especificaciones Técnicas para las futuras Adquisiciones de dispositivos informáticos, y se den de baja progresivamente aquellos que no ofrezcan soporte de ambos protocolos IPv4 e IPv6.

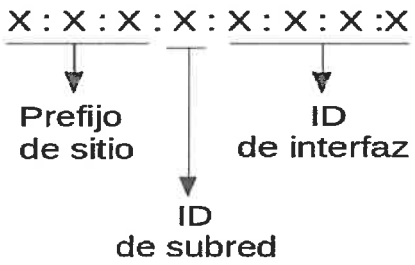
11.4. Se recomienda de aplicación inmediata, que los desarrolladores de software que presten servicios a la UNSA implementen sus servicios con compatibilidad completa de IPv4 e IPv6 y actualicen sus productos para el respectivo soporte.

11.5. Finalmente, se concluye que el proceso de transición permitirá que se trabajen a la par el protocolo versión 4 y el protocolo versión 6, lo que no afectará de forma alguna los procesos cotidianos en la UNSA. Por otra parte, se recomienda ir realizando una transición parcial, diseñar un segmento de red para realizar pruebas y así evitar problemas en aplicaciones críticas de la entidad.

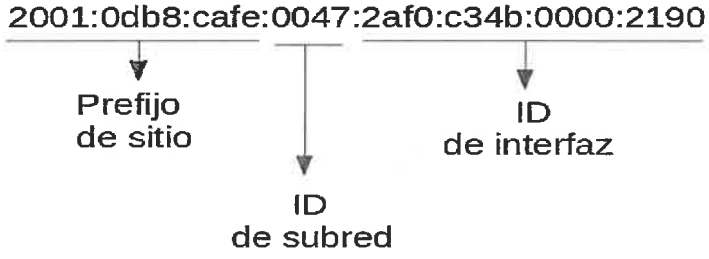
12. ANEXOS

12.1. Direcciones IPv6

Las direcciones IPv6 tienen un tamaño de 128 bits, distribuidos en ocho campos de dieciséis bits denominados coloquialmente HEXTETOS, representados por cuatro números hexadecimales cada uno y separados por dos puntos. En la figura se puede observar el formato de una dirección IPv6, los cuarenta y ocho primeros bits, es decir, los tres primeros hextetos contienen el prefijo de sitio, éste describe la conexión de la organización, representa a la topología publica y es el segmento que suelen asignar al sitio, los ISP o RIR (Registro Regional de Internet). Los siguientes dieciséis bits o 4to hexteto, lo ocupa el ID de subred y describe la topología privada, es asignado por el administrador de la red. Los últimos sesenta



Ejemplo:



y cuatro bits o cuatro campos de la derecha, contienen el ID de interfaz y se puede configurar manual o automáticamente.

12.2. Cronogramas de Implementación, pruebas y capacitación.

				implementación del protocolo IPv6	Plazos	Responsables	Entregables
1				Planificación y Evaluación	2 meses	Jefatura OTI/UITST	Elaboración Plan de trabajo y Anexos
	1.1			Formación del equipo de implementación	2 semanas	Jefatura OTI/UITST	Asignación de Roles y Responsables
		a		Selección de un equipo responsable de la implementación	5 días	Jefatura OTI/UITST	Oficio designación Jefe del equipo de implementación
		b		Identificar Roles y Responsabilidades	5 días	Equipo implementación	Oficio designación Responsables y miembros del equipo
	1.2			Evaluación de la Infraestructura Anual	4 semanas	Responsable Infraestructura de red	Informe del estado de la infraestructura tecnológica de red actual
		a		Realizar un inventario de la red actual.	15 días	Responsable Inventario	Tabla en Excel con características de equipos
		b		Evaluar el soporte actual para IPv6.	5 días	Responsable Soporte IPv6	Hojas de datos de equipamiento de red
		c		Identificar dispositivos y aplicaciones que necesitan actualizarse.	5 días	Responsable actualización	Tabla del estado de todas las aplicaciones y equipos
	1.3			Establecimiento de Objetivos y Alcance	2 semanas	Jefe de Equipo	Redacción de objetivos y alcance
		a		Definir metas específicas para la implementación de IPv6.	5 días	Jefatura OTI/UITST	Listado de metas por áreas
		b		Determinar el alcance de la implementación	5 días	Jefatura OTI/UITST	Conclusiones del alcance de la implementación IPv6
2				Diseño y Configuración	6 meses	Jefe de Equipo	Informe del diseño y configuración
	2.1			Desarrollo de Políticas de IPv6	8 semanas	Responsable Infraestructura de red	Elaboración de las políticas para el uso de IPv6
		a		Establecer políticas de seguridad y asignación de direcciones IPv6.	10 días	Jefe UITST	Cuadro de asignación de direcciones IPv6 e IPv4
		b		Definir políticas de enrutamiento y segmentación de red.	10 días	Jefe UITST	topologías lógicas y físicas, detalle de subredes y VLANs
		c		Implementación de enrutamiento y VLANs en Switch y Routers	10 días	Jefe UITST	Tablas de enrutamiento por dispositivo
		d		creación de repositorio de respaldo de configuraciones	10 días	Jefe UITST	Registro de archivos de configuración de dispositivos de red
	2.2			Actualización de Equipos y Software	8 semanas	Responsable Inventario	Tabla de equipos por ubicación y software instalado
		a		Identificar ubicación de equipos que requieren actualizaciones	15 días	Jefe UITST	Listado de equipos y registro de estado previo
		b		programación de visita en campo para actualizaciones	5 días	Jefe UITST	Cronograma de visita para actualización
		c		Realizar actualizaciones según sea necesario.	30 días	Jefe UITST	actualización del listado de equipos
	2.3			Configuración de Dispositivos de Red	4 semanas	Responsable actualización	Reporte de configuración de dispositivos
		a		Configurar enrutadores, switches y firewalls para admitir IPv6.	10 días	Jefe UITST	Nuevos archivos de configuración de los dispositivos de red
		b		Implementar cambios en la infraestructura de red.	15 días	Jefe UITST	Lista de incidencias de la implementación de cambios

			implementación del protocolo IPv6	Plazos	Responsables	Entregables
	2.4		Pruebas de Conectividad	2 semanas	Responsable Soporte IPv6	Informe de Pruebas de Conectividad
		a	Realizar pruebas de conectividad interna para comunicación IPv6.	5 días	Jefe UITST	Checklist de pruebas de conectividad
		b	Verificar la interoperabilidad con sistemas y servicios externos.	5 días	Jefe UITST	Prueba de Conexiones desde intranet e internet
3			Implementación	10 meses	Jefe de Equipo	Informe de implementación de IPv6
	3.1		Implementación Gradual en Segmentos de Red	20 semanas	Responsable actualización	Reporte de implementación por segmento de red
		a	Implementar IPv6 en segmentos de red específicos de manera gradual.	60 días	Jefe UITST	Detalle de incidencias de implementación de IPv6 por áreas
		b	Monitorizar el rendimiento y solucionar problemas a medida que surgen.	40 días	Jefe UITST	recopilación de tickets e incidencias reportadas y solución
	3.2		Migración de Servicios Críticos	16 semanas	Responsable Infraestructura de red	Reporte de migración de servicios críticos
		a	Migrar servicios críticos a IPv6.	60 días	Jefe UITST	Procedimiento de migración de cada servicio critico
		b	Asegurarse de que los servicios esenciales funcionan sin problemas.	20 días	Jefe UITST	Reporte de verificación de funcionamiento de servicios
	3.3		Capacitación y Concientización	4 semanas	Responsable Soporte IPv6	Listados de asistencia y notas de capacitaciones
		a	Proporcionar capacitación a personal de TI y usuarios finales sobre IPv6.	10 días	Jefe UITST	Plan de capacitación
		b	Crear materiales de concientización para la comunidad universitaria.	5 días	Jefe UITST	Resumen de materiales, diapositivas, documentos, normas, etc.
		c	Documentar las lecciones aprendidas y actualizar la documentación.	5 días	Jefe UITST	Reporte de evaluaciones aplicadas en capacitaciones
4			Evaluación y Optimización Continua	12 meses	Jefe de Equipo	Informe del funcionamiento y operación del protocolo IPv6
	4.1		Monitoreo y Evaluación	12 semanas	Responsable Infraestructura de red	Reporte de monitoreo mensual
		a	Implementar herramientas de monitoreo para supervisar el tráfico IPv6.	30 días	Jefe UITST / SOC ISP	Capturas de monitoreo de manera semanal, mensual y anual
		b	Evaluar el rendimiento y la seguridad de la red.	30 días	Jefe UITST / SOC ISP	Documentar pruebas de intrusión y throughput aleatorias
	4.2		Optimización Continua	36 semanas	Responsable Soporte IPv6	Reporte de incidencias y documentación de mejoras

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA RECTORADO

Aprobado en Sesión de Consejo Universitario de fecha ____ de abril de 2024.

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA SECRETARÍA GENERAL

Elaborado por Oficina de Tecnologías de la Información-OTI
Revisado y actualizado por Unidad de Modernización-UM.

Arequipa, 2024 marzo 25
MACZ/msbv