

# SERVICIO DE ADMINISTRACIÓN TRIBUTARIA – SAT

## RESOLUCIÓN DE GERENCIA GENERAL N.º 286-004-00000147

Lima, 1 de julio de 2025.

### CONSIDERANDO:

Que, mediante Edicto N.º 225 se crea el Servicio de Administración Tributaria - SAT como un organismo público descentralizado de la Municipalidad Metropolitana de Lima, con personería jurídica de Derecho Público Interno y con autonomía administrativa, económica, presupuestaria y financiera;

Que, mediante Decreto de Alcaldía N.º 015 publicado en el Diario Oficial El Peruano el 29 de septiembre de 2024 y vigente a partir del 1 de diciembre de 2024, se aprobó el Manual de Operaciones – MOP del SAT;

Que, el citado Manual de Operaciones, de conformidad con lo establecido en el literal c) de su artículo 11º, establece que es función de la Gerencia General, aprobar los planes y políticas institucionales;

Que, la Ley N.º 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; por lo que deviene en necesario mejorar la gestión pública a través del uso de nuevas tecnologías que permitan brindar mejores servicios a los ciudadanos;

Que, la Política Nacional de Gobierno Electrónico, aprobada con Decreto Supremo N.º 081-2013-PCM, prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Infraestructura, el mismo que busca contar con una red informática que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, bases de datos, entre otros;

Que, a través de los artículos 1º y 3º del Decreto Supremo N.º 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 dispone la formulación de un Plan de Transición al Protocolo IPV6, a implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública, el mismo que será aprobado por el Titular de cada entidad;



Que, en dicho contexto normativo, con Informe N.º D000061-2025-SAT-OTI, y correo de fecha 30 de junio de 2025, la Oficina de Tecnologías de la Información remite el proyecto del Plan de Transición al Protocolo IPv6; asimismo, con Informe N.º D000011-2025-SAT-OGI de fecha 17 de junio de 2025, la Oficina General de Innovación y Desarrollo Tecnológico solicita su respectiva aprobación;

Que, el referido Plan de Transición al Protocolo IPv6, es una proyección o marco base de las actividades significativas que permite adaptar los recursos tecnológicos, humanos y económicos del SAT, para progresivamente pasar a una arquitectura de red IPv6, mediante las siguientes actividades: a) Identificar los componentes claves que determinan la transición al protocolo IPv6; b) Garantizar la continuidad de los servicios digitales que ofrece el SAT durante la etapa de implementación del protocolo IPv6 sobre la red del SAT y posterior a ella; c) Definir las actividades, recursos y cronograma para la transición al protocolo IPv6;

Que, en atención a lo informado, con Proveído N.º D000798-2025-SAT-GGE del 23 de junio de 2025, la Gerencia General del SAT solicita la elaboración de la Resolución de Gerencia General correspondiente;

Estando a lo dispuesto en el artículo 10 y el inciso c) del artículo 11 del Manual de Operaciones – MOP del SAT, aprobado mediante Decreto de Alcaldía N.º 015;

### SE RESUELVE:

**Artículo 1º.** - Aprobar el Plan de Transición al Protocolo IPv6 del Servicio de Administración Tributaria de Lima, y su cronograma, que en anexo forman parte integrante de la presente resolución.

**Artículo 2º.** - Remitir la presente resolución, así como el plan y cronograma aprobados a la Secretaría de Gobierno Digital (SEGDI), de la Presidencia del Consejo de Ministros; de conformidad con lo dispuesto en el artículo 5º del Decreto Supremo N.º 081-2017-PCM.

**Artículo 3º.** - Encárguese al responsable del Portal de Transparencia del SAT la publicación de la presente resolución en la página web de la entidad: [www.sat.gob.pe](http://www.sat.gob.pe).

Regístrese, comuníquese y cúmplase.



**María del Pilar Caballero Estella**  
Gerente General  
Servicio de Administración Tributaria



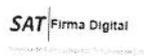
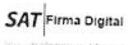
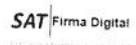
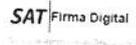


**SAT** *SERVICIO DE  
ADMINISTRACIÓN  
TRIBUTARIA DE LIMA*

PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

**2025**

REVISIÓN Y APROBACIÓN:

Elaborado por: Cesar Edilberto Terry Ramos	Firma:
Cargo/Rol: Especialista de Gestión de Operaciones de TI III	 Firmado digitalmente por TERRY RAMOS Cesar Edilberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:29:19 -05:00
Revisado por: Edwin Turín Avila	Firma:
Cargo/Rol: Especialista de Gestión de Operaciones de TI II	 Firmado digitalmente por TURIN AVILA Edwin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:37:57 -05:00
Revisado por: Carlos Alberto Sanz Diaz	Firma:
Cargo/Rol: Especialista de Gestión de Operaciones de TI II	 Firmado digitalmente por SANZ DIAZ Carlos Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:40:03 -05:00
Revisado por: Dayana Erika Quispe Reyes	Firma:
Cargo/Rol: Analista de Control de Calidad de TI II	 Firmado digitalmente por QUISPE REYES Dayana Erika FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:43:45 -05:00
Revisado por: Juan Martin Camino León	Firma:
Cargo/Rol: Oficial de Seguridad de la Información y Confianza Digital	 Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:46:02 -05:00
Revisado por: Genaro Torres Armas	Firma:
Cargo/Rol: Especialista de Gestión de Soluciones de TI I	 Firmado digitalmente por TORRES ARMAS Genaro FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:47:24 -05:00
Revisado por: Edson Owerland Leon De La Sota	Firma:
Cargo/Rol: Especialista de Gestión de Servicios de TI I	 Firmado digitalmente por LEON DE LA SOTA Edson Owerland FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:55:47 -05:00
Revisado por: Sandro Ivan Rodriguez Romero	Firma:
Cargo/Rol: Jefe de la Oficina de Tecnologías de la Información	 Firmado digitalmente por RODRIGUEZ ROMERO Sandro Ivan FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:12:23 -05:00
Revisado por: Ottoniel Waldir Tume Ledesma	Firma:
Cargo/Rol: Jefe de la Oficina General de Innovación y Desarrollo Tecnológico	 Firmado digitalmente por TUME LEDESMA Ottoniel Waldir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:26:14 -05:00
Aprobado por: Maria Del Pilar Caballero Estella	Firma:
Cargo/Rol: Gerente General del SAT	 Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 01.07.2025 19:11:29 -05:00

## ÍNDICE

1.	INTRODUCCIÓN	4
2.	BASE LEGAL	5
3.	OBJETIVO DEL PLAN DE TRANSICIÓN	5
4.	TERMINOS Y DEFINICIONES	5
5.	ALCANCE DEL PLAN DE TRANSICIÓN	6
6.	DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA	7
7.	IMPLEMENTACIÓN DEL PROTOCOLO IPV6	11
8.	REALIZACIÓN DE PRUEBAS	12
9.	CAPACITACIÓN Y SENSIBILIZACIÓN	13
10.	PRESUPUESTO ESTIMADO	13
11.	ANEXOS	14

## 1. INTRODUCCIÓN

El protocolo de Internet o protocolo IP en su versión 4 (IPv4), es el que actualmente y globalmente se ha venido empleando para identificar los dispositivos que se conectan a Internet. Mediante el uso de IPv4 existe un aproximado de 4,300 millones de direcciones IP que pueden ser asignadas; sin embargo, debido a la cada vez más creciente demanda para interconectar diversos dispositivos tecnológicos a Internet (telefonía móvil, Internet de las Cosas (IoT), computación en la nube, entre otros), estas direcciones IP ya no resultan suficientes para abastecer la demanda actual.

En el 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 desarrolló un nuevo protocolo de Internet, denominado IPv6, el cual tiene la capacidad de asignar 340 sextillones de direcciones IP.

A nivel mundial, para la asignación de direcciones IP existen organismos jerárquicos siendo el principal de ellos la IANA (Internet Assigned Numbers Authority), 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 a los Registros Regionales de Internet (RIR), los cuales realizan una posterior subdelegación de recursos a sus clientes principales que incluyen a los proveedores de servicios de Internet (ISP).

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.

Se debe tener en cuenta, que el protocolo IPv4 es predominante en internet y no es posible su sustitución a mediano plazo, por tal razón la utilización del protocolo IPv6, debe realizarse mediante una estrategia de "transición o adaptación" que resulta de un estudio específico o personalizado de la arquitectura tecnológica para que ambos protocolos convivan.

El mismo 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 se gestiona, será complicado. Es por ello que será necesario realizar servicios especializados, con el fin de ejecutar un Plan de Transición al protocolo IPv6 en el SAT.

En el periodo 2024, el Servicio de Administración Tributaria SAT de Lima, contrató el servicio especializado para que elabore el Plan de Transición al protocolo IPv6 y ejecute la primera etapa que corresponde al "**Diagnóstico de la Infraestructura Tecnológica**", que incluye el inventario del software, hardware, infraestructura tecnológica, aplicaciones y servicios que no soportan IPv6, y la evaluación del riesgo.

En ese sentido, el presente documento tiene por finalidad proyectar un marco de trabajo, fases, etapa y/o actividades e instrumentos que faciliten la adopción del protocolo IPv6, teniendo presente lo dispuesto en el Decreto Supremo N°081-2017-PCM que aprobó la formulación del Plan de Transición al Protocolo IPv6 en las entidades públicas.

## 2. BASE LEGAL

1. Ley N°27444, Ley del Procedimiento Administrativo General.
2. Ley N°27658, Ley Marco de Modernización de la Gestión del Estado.
3. Ley N°29158, Ley Orgánica del Poder Ejecutivo.
4. Decreto Supremo N°004-2013-PCM, Política Nacional de Modernización de la Gestión Pública.
5. Decreto Supremo 081-2017-PCM, Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública.
6. Decreto Supremo N°033-2018-PCM, Plataforma Digital Única del Estado Peruano y establece disposiciones adicionales para el desarrollo del Gobierno Digital.
7. Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N°129-2014, Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI. Tecnología de la información, Técnicas de seguridad, Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición.
8. Resolución Ministerial N°004-2016-PCM, uso obligatorio de la Norma Técnica Peruana NTP-ISO/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.

## 3. OBJETIVO DEL PLAN DE TRANSICIÓN

Ante el agotamiento de las direcciones del protocolo IPv4, se define una proyección o marco base de las actividades significativas que permita adaptar los recursos tecnológicos, humanos y económicos del SAT, para progresivamente pasar a una arquitectura de red IPv6, mediante las siguientes actividades:

- a. Identificar los componentes claves que determinan la transición al protocolo IPv6.
- b. Garantizar la continuidad de los servicios digitales que ofrece el SAT durante la etapa de implementación del protocolo IPv6 sobre la red del SAT y posterior a ella.
- c. Definir las actividades, recursos y cronograma para la transición al protocolo IPv6.

## 4. TERMINOS Y DEFINICIONES

Para efectos de una correcta interpretación y mejor entendimiento de los contenidos del presente documento, se deben considerar los siguientes términos y definiciones:

- a. **PROTOCOLO IP:** El protocolo IP (Internet Protocol) es utilizado para el intercambio de datos e información entre redes o dispositivos conectados a Internet, existiendo a la fecha dos versiones, la versión 4 y versión 6 (IPv4 e IPv6 respectivamente). IPv6 es el protocolo joven de internet y nace para solucionar el actual agotamiento de las direcciones IPv4.
- b. **RIR:** (Registro Regional de Internet), es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo.
- c. **LACNIC:** (Registro de Direcciones de Internet para América Latina y Caribe), es una organización no gubernamental internacional, establecida en Uruguay en el año 2002. Su función es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región.
- d. **ASN:** (Autonomous System Number, o Número de Sistema Autónomo) es un identificador único que se asigna a cada Sistema Autónomo (AS) que opera en Internet.

- e. **BGP:** (Border Gateway Protocol o Protocolo de Puerta de Enlace Fronteriza). Es el protocolo de enrutamiento que permite a Internet enviar datos entre diferentes redes independientes, llamadas Sistemas Autónomos (AS).
- f. **ISP:** (Internet Service Provider), es un Proveedor de Servicios de Internet. Es una empresa u organización que proporciona a los usuarios (personas, empresas u otras entidades) acceso a Internet y, a menudo, otros servicios relacionados.
- g. **Dual Stack:** es una técnica de transición que permite que un dispositivo o red utilice simultáneamente IPv4 e IPv6, es decir, que funcione con ambos protocolos de Internet a la vez.
- h. **Direccionamiento no asignado:** (Provider Independent), se refiere, en términos generales, a bloques de direcciones IP que aún no han sido asignados oficialmente por una autoridad competente (como IANA, LACNIC, etc.) a un proveedor, una organización o un dispositivo. Permiten mantener el mismo prefijo IPv6 sin importar el ISP, por lo que se evita la re numeración.
- i. **Direccionamiento asignado:** (Provider Aggregatable), direcciones IP que el ISP (Proveedor de Servicios de Internet) asigna temporal o permanentemente. El ISP controla ese direccionamiento y solo se puede usar mientras se tenga contrato con ese proveedor.

## 5. ALCANCE DEL PLAN DE TRANSICIÓN

Contempla toda la infraestructura tecnológica del SAT, plataforma y servicios TI que estén bajo la dirección de la Oficina de Tecnologías de la Información susceptible a una configuración IP.

En el siguiente cuadro, se indican los recursos y componentes que están dentro del alcance del Plan de Transición al Protocolo Pv6 en el SAT:

**Cuadro N° 01 – Recursos y Componentes transición al Protocolo Pv6 en el SAT**

Recurso / Componente	Plataforma
Servidores de Base de Datos	MySQL, PostgreSQL, Oracle, MSSQL, DBx
Servidores de red	AD, DNS, DHCP, Correo
Equipo de Comunicaciones y Seguridad	Switch CORE, Switch de Borde, Firewall, Antispam, Balanceador, Controladores y equipos de accesos inalámbricos, equipos de ruteo, Telefonía IP, Almacenamiento, Equipos de Control UPS y Climatización de Precisión.
Plataformas web	IIS, Jboss, Apache
Software y aplicaciones	Diferentes fabricantes y desarrollos propios.
Estaciones de usuario	PC, Laptop, Impresora, anexos IP, Cámaras IP, lectoras de marcación y escáner de usuarios

El grupo de recursos y componentes son los motores de base de datos, servidores de red (controlador de dominio, DHCP, Correo y DNS privado y público), equipos de comunicaciones y seguridad, plataformas del perímetro y web, Software y aplicaciones, y estaciones de usuario final (PC, Laptop, Impresora, Anexos y Escáner).

Para lograr una transición progresiva, sostenible y con valor, el recurso esencial es el conocimiento de la arquitectura de red, servicios de red y el diseño de la arquitectura de transición de IPv4 a IPv6, junto a la capacitación y sensibilización. La generación de valor deberá ser progresiva e inmediata al finalizar la puesta en

producción de la arquitectura de transición de IPv4 a IPv6, y deberá poder permitir publicar servicios del SAT a Internet IPv6, superando de esta manera los contratiempos generados por la actual restricción de direcciones IPv4 que nuestro Register Internet Regional (RIR) y LACNIC, vienen comunicando, y de no poner en marcha, pondría en riesgo el crecimiento, competitividad y continuidad de los servicios que brinda el SAT.

## 6. DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

Para el diagnóstico, se relevó y analizó la información necesaria respecto a la infraestructura tecnológica del SAT, y su operación, compatibilidad y adecuación con el protocolo IPv6: para ello se analizó información relacionada con:

- a. Capacidad del servicio de acceso a Internet.
- b. Equipos de redes y comunicaciones.
- c. Sistemas operativos.
- d. Equipos de seguridad.
- e. Aplicaciones de los servicios.

Se consultó con los representantes de fabricantes con quienes se tiene contratos de soporte de la plataforma tecnológica del SAT, a fin de obtener información técnica específica relacionada con la compatibilidad con el protocolo IPv6 y de ser necesario, incluir acciones en el Plan de Transición al Protocolo Pv6 en el SAT.

Para los casos de plataformas tercerizadas que están brindando servicios al SAT, se coordinó con los contratistas, la verificación de las características técnicas y compatibilidad del servicio con IPv6.

### Manejo del riesgo

Agregar en la infraestructura de red actual el protocolo IPv6 puede conllevar algunos riesgos, los cuales de materializarse pueden desencadenar en un incidente. Un incidente es una serie de eventos negativos no deseados o inesperados que puede comprometer el desarrollo normal del sistema y generar un impacto en las operaciones de la entidad. Para identificar y gestionar los riesgos nos vamos a apoyar en la siguiente matriz:

Gráfico N° 01 – Mapa de Riesgo

PROBABILIDAD	4	Moderado	Alto	Muy Alto	Muy Alto
	3	Moderado	Moderado	Alto	Muy Alto
	2	Bajo	Moderado	Moderado	Alto
	1	Bajo	Bajo	Moderado	Moderado
		1	2	3	4
CONSECUENCIAS					

Cuadro N° 02 - Identificación y cálculo del riesgo inherente

N°	Riesgo	Descripción	Probabilidad	Consecuencia	Valoración		
					Muy Alto	Alto	Medio
1	Interrupción de servicios críticos	Cambios en la configuración de red pueden interrumpir servicios (DNS, correo, aplicaciones internas).	3	3		9	
2	Incompatibilidad de sistemas	Aplicaciones o equipos antiguos pueden no soportar IPv6.	3	3		9	
3	Falta de visibilidad y monitoreo	Herramientas SIEM o de monitoreo no están adaptadas a IPv6, lo cual limita la capacidad de detectar incidentes.	3	3		9	
4	Incremento de la superficie de ataque	IPv6 puede abrir nuevos vectores de ataque (ICMPv6, SLAAC, etc.).	3	3		9	
5	Error humano en la configuración dual stack	La coexistencia IPv4/IPv6 puede inducir a errores en ruteo, ACLs, etc.	3	3		9	

Cuadro N° 03 - Estrategias de mitigación y control de riesgos

N°	Medida de control	Descripción
1	Pruebas piloto controladas	Realizar la implementación en entornos limitados (laboratorios, redes segmentadas) antes del despliegue completo.
2	Validación / Actualización de herramientas de seguridad	Validar que firewalls, SIEM y escáneres de vulnerabilidades soportan y monitorean tráfico IPv6.
3	Auditoría de configuración	Validar reglas de seguridad, rutas y políticas en IPv6 en paralelo a IPv4 (especialmente en entornos dual-stack).
4	Análisis de riesgos por etapas	Aplicar una metodología como ISO 27005 para analizar riesgos en cada fase del proyecto de transición.
5	Capacitación técnica específica	Asegurar que el personal de redes y seguridad esté capacitado en temas clave de IPv6: dual-stack, seguridad, troubleshooting.
6 (*)	Validar compatibilidad de las aplicaciones y equipos respecto a protocolo IPV6	Identificar componentes de hardware y software que no tengan compatibilidad con el protocolo IPV6 y proponer acciones correctivas y costos asociados, incorporándose como requisitos del plan de implementación.

Respecto a la **medida de control N° 6** "Validar compatibilidad de las aplicaciones y equipos respecto a protocolo IPV6", producto del diagnóstico realizado se han identificado las siguientes situaciones que contribuyen a incrementar la probabilidad del riesgo N°2 "Incompatibilidad de sistemas":

- **Sistema Administrativo Financiero del SAT (SAF) y software de base de datos Oracle:** El SAF es utilizado por la Oficina de Recursos Humanos (ORH) para la gestión del recurso humano. Asimismo, es utilizado por personal del Área de Presupuesto para consultar la ejecución de los bienes y servicios.

De acuerdo con la información publicada por el fabricante Oracle, la versión Enterprise 10G no soporta IPv6; por lo que resulta muy probable que el sistema no funcione bajo IPv6.

La ORH utiliza dicho sistema para la gestión de la planilla, contratos, asistencia, entre otras actividades, las cuales tendrán que realizarlas de forma manual y retrasarían enormemente la ejecución de actividades de dicha oficina.

- **Aplicativos WEB (auditoría):** Actualmente los aplicativos WEB están desarrollados para guardar la dirección IP del equipo en uso como pista de auditoría.

El especialista de gestión de soluciones de TI ha revisado la programación de las aplicaciones y ha confirmado que esta se encuentra diseñada para obtener la cantidad de caracteres de la dirección IP, pero en la versión 4 y no de la versión 6 (la cual tiene más caracteres), de tal manera que la información en los reportes del sistema WEB no se mostraría completa (IP cortada).

Capturar la información de la dirección IP de los equipos que utilizan los aplicativos WEB, es necesaria e importante para el uso en las auditorías, seguimientos, monitoreo y reportes mensuales de los sistemas WEB del SAT.

- **Equipo Antispam Barracuda:** El equipo protege al correo institucional de los spam y virus, evitando la propagación de virus y saturación del correo (lentitud).

La probabilidad que el equipo no funcione en IPv6 es muy probable, ya que de acuerdo con la información publicada por el fabricante Barracuda, la versión del equipo no soporta IPv6.

El correo institucional es un medio de comunicación oficial del SAT, el mismo que es utilizado tanto para los procesos de cobranza como para las comunicaciones con los ciudadanos, otras entidades y personal interno.

- **Sistema de red inalámbrica interna (Red Wi-Fi):** El cual nos sirve para conectarnos de forma segura a la red inalámbrica (Wifi) del SAT, con el fin de obtener acceso a internet o para ingresar a los sistemas de la intranet.

De acuerdo con la información publicada por el fabricante, la versión del equipo ISE (autenticador del sistema inalámbrico) no soporta IPv6, por esta razón es muy probable que el equipo no funcione bajo un entorno IPv6.

No se podría brindar acceso a internet/Intranet a los colaboradores (atención mediante Tablet o laptop) y a Internet al personal del Órgano de Control Institucional y personal de la SOA para que realicen sus actividades.

- **Firewall perimetral Palo Alto:** Equipo que se ubica en el límite entre la red interna del SAT e Internet, y protege la red interna controlando el tráfico que entra y sale según reglas de seguridad establecidas, detectar y mitigar ataques básicos, bloquea accesos no autorizados desde el exterior y filtra paquetes de datos según IP, puerto, protocolo, contenido, etc.

Se ha verificado que el firewall perimetral no soporta el mecanismo de tunneling para conectar a Internet IPv6; este mecanismo permite enviar tráfico IPv6 a través de redes IPv4, y es necesario para evitar la no

reenumeración de direcciones IPv6 cuando se cambia de proveedor y no se cuenta con direccionamiento independiente.

En el siguiente cuadro se establecen las medidas de propuestas para corregir las situaciones que contribuyen a incrementar el riesgo N°2:

Cuadro N° 04 – Situaciones que incrementan los riesgos y medidas de tratamiento

N°	Situaciones que contribuyen al riesgo N° 2	Medida de propuesta
1	<p><u>La probabilidad</u> de que no funcione el sistema SAF (BD Oracle) es muy probable, ya que de acuerdo con la información publicada por el fabricante Oracle, la versión Enterprise 10G no soporta IPv6. El <u>impacto</u> es crítico, debido a que la ORH utiliza dicho sistema para la gestión de la planilla, contratos, asistencia, entre otras actividades, las cuales tendrían que realizarlas de forma manual y retrasarían enormemente la ejecución de actividades de dicha oficina. <u>Riesgo Alto.</u></p>	<p><u>Alternativas de Tratamiento:</u></p> <ol style="list-style-type: none"> <li>1. Adquirir la versión actual del motor de base de datos Oracle (Enterprise) para el sistema SAF, o</li> <li>2. Adquirir una herramienta de software que reporte la auditoría del sistema SAF conjuntamente con la instalación del software Oracle (Standard), o</li> <li>3. Contratar el servicio de desarrollo de software que modifique el sistema SAF para que reporte la auditoría, e implementar el software Oracle (Standard), o</li> <li>4. Adquirir o contratar bajo suscripción, una herramienta de software específica para la gestión de RRHH, la cual sea compatible con IPV6.</li> <li>5. Implementar una herramienta de software público gratuito para entidades del estado, disponible desde la Plataforma Nacional de Software Publico, la cual sea compatible con IPV6.</li> </ol>
2	<p>Aplicativos WEB (auditoría): Actualmente los aplicativos WEB están desarrollados para guardar el número de IP del equipo en uso. <u>La probabilidad</u> que el número de IP en versión 6 no este completo en los reportes de los sistemas WEB es muy probable, ya que el especialista de gestión de soluciones de TI ha revisado la programación de las aplicaciones y ha confirmado que está diseñada para obtener la cantidad de caracteres de la IP, pero en la versión 4 y no de la versión 6 (cuál tiene más caracteres), de tal manera que la información en los reportes del sistema WEB saldría incompleta (IP cortada). El <u>impacto</u> es crítico, debido a que la información de la IP de los equipos que utilizan los aplicativos WEB, es necesaria e importante para el uso en las auditorías, seguimientos, monitoreo y reportes mensuales de los sistemas WEB del SAT. <u>Riesgo Alto.</u></p>	<p><u>Alternativas de Tratamiento:</u></p> <p>Contratar un servicio de desarrollo de software para modificar las aplicaciones WEB, que soporten la cantidad de caracteres en IPV6. Asimismo, las nuevas aplicaciones WEB a desarrollar, deberán incluir el soporte de IPV6.</p>
3	<p>Equipo Antispam Barracuda: El equipo protege al correo institucional de los spam y virus, evitando la propagación de virus y saturación del correo (lentitud). <u>La probabilidad</u> que el equipo no funcione en IPv6 es muy probable, ya que de acuerdo con la información publicada por el fabricante Barracuda, la versión del equipo no soporta IPv6. El <u>impacto</u> es crítico, debido a que el</p>	<p><u>Alternativas de Tratamiento:</u></p> <ol style="list-style-type: none"> <li>1. Adquirir o contratar bajo el modelo de suscripción, un nuevo sistema antispam que soporte el protocolo IPV6, o</li> <li>2. Migrar el servicio de correo electrónico del SAT a la nube</li> </ol>

	<p>correo institucional es un medio de comunicación oficial del SAT, que lo utilizamos para la cobranza, para comunicarnos con los ciudadanos y personal interno. <u>Riesgo Alto</u></p>	
4	<p>Sistema inalámbrico CISCO: El cual nos sirve para conectarnos de forma segura a la red inalámbrica (Wifi) del SAT, con el fin de obtener acceso a internet o para ingresar a los sistemas de la intranet. <u>La probabilidad</u> de que el sistema Wifi no funcione en IPv6 es muy probable, ya que de acuerdo con la información publicada por el fabricante CISCO, la versión del equipo ISE (autenticador del sistema) no soporta IPv6. El <u>impacto</u> es crítico, porque dejaríamos incomunicado a los equipos inalámbricos del SAT y no se podría brindar acceso a internet/Intranet a los colaboradores (atención mediante Tablet o laptop) y a Internet al personal del Órgano de Control Institucional y personal de la SOA para que realicen sus actividades. <u>Riesgo Alto.</u></p>	<p><u>Alternativas de Tratamiento:</u> Adquirir o contratar un sistema de red inalámbrico.</p>
5	<p>El firewall perimetral Palo Alto no soporta el mecanismo de tunneling para conectar a Internet IPv6, puesto que no puede enviar tráfico IPv6 a través de redes IPv4; además, este mecanismo es necesario para evitar la no reenumeración de direcciones IPv6 cuando se cambia de proveedor y no se cuenta con direccionamiento independiente. El <u>impacto</u> es crítico puesto que no se podría tener salida a Internet IPv6. <u>Riesgo Alto.</u></p>	<p><u>Alternativas de Tratamiento:</u> 1. Adquirir un equipo firewall con soporte de mecanismo de transición tunneling y contratar servicio de tunneling; o 2. Implementar otro mecanismo para conectar a Internet IPv6: a) A través de los recursos proporcionados por LACNIC, con <b>direccionamiento no asignado</b> (recomendado). En este caso se solicita un bloque de direcciones IPv6 PI, el cual resulta independiente y <b>no varía</b> según el ISP que se contrate. b) A través de los recursos del proveedor de Internet, <b>direccionamiento asignado</b> (menos recomendado). En este caso el direccionamiento varía si cambio de ISP.</p>

## 7. 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. En el mediano plazo, el protocolo IPv4 se dejará de utilizar.

El objetivo de la transición, de acuerdo al diagnóstico realizado, es ir reemplazando o implementando alternativas de todos los componentes, identificados en el "Diagnóstico", que no soportan IPv6; y que la migración no impacte en la operatividad y continuidad de los servicios.

## PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

Durante la etapa de implementación y etapa de pruebas, existirá una convivencia del protocolo IPv4 e IPv6, mediante el dual stack.

Esta etapa podría ser realizada con apoyo o recurso externo especializado con experiencia comprobada, de acuerdo a lo que se indica en el cronograma.

En la etapa de implementación de ejecutará las Medidas de Control N° 2, 3, 4 y 6.

Cabe precisar, que el cumplimiento del cronograma de implementación dependerá de la asignación presupuestal para la adquisición o contratación de los bienes y servicios indicados.

**Cuadro N° 05 - Cronograma y responsable de la etapa: Implementación del protocolo IPv6**

PLAN DE TRANSICIÓN AL PROTOCOLO IPV6	Resp	Dic-25	Ene-26	Feb-26	Mar-26	Abr-26	May-26	Jun-26	Jul-26	Ago-26	Set-26	Oct-26	Nov-26	Dic-26
<b>Etapa 1: Implementación del protocolo IPv6</b>														
Elaboración de TDR para el diseño de una arquitectura de transición de IPv4 a IPv6, direccionamiento, configuración de todos los equipos de la red, elaboración de políticas de seguridad para los servicios publicados a IPv6 y navegación de usuarios, elaboración de TDR LACNIC, pruebas y capacitación.	Int													
Tiempo para la contratación del Servicio	Int													
Implementación del protocolo IPv6	Ext													
Elaboración de TDR para la gestión y adquisición de direccionamiento IPv4 e IPv6 independiente vía LACNIC.	Ext													
Tiempo para la contratación del Servicio	Int													
Tiempo para la asignación IPS LACNIC e inicio del servicio	Ext													
Elaboración de TDR para el Servicio de Internet y Seguridad Gestionada, internet vía BGP y con direccionamiento independiente IPv6	Int													
Tiempo para la contratación del servicio.														
Tiempo para la implementación e inicio del servicio.	Int/Ext													
Elaboración de EETT para reemplazar el software que soporte IPv6 o Elaboración de TDR para Servicio de desarrollo de software	Int													
Tiempo para la contratación e implementación del bien o desarrollo del software	Int/Ext													
Elaboración de TDR para modificar los sistemas WEB para que la reporteria y auditoria soporten la cantidad de caracteres que soporte IPv6	Int													
Tiempo para la contratación e implementación del desarrollo del software	Int/Ext													
Elaboración de EETT para reemplazar equipo de seguridad con soporte a IPv6 o TDR para contratar un servicio de antispam que soporte el protocolo IPv6	Int													
Tiempo para la contratación e implementación del bien o inicio del servicio	Int/Ext													
Elaboración de EETT para reemplazar el sistema inalámbrico con soporte a IPv6 o TDR para la contratación del servicio.	Int													
Tiempo para adquisición e implementación del sistema	Int/Ext													

## 8. REALIZACIÓN DE PRUEBAS

Las pruebas con éxito representan la evidencia de la implementación del protocolo IPv6, sin embargo, durante esta etapa existirá una convivencia del protocolo IPv4 e IPv6, mediante el dual stack.

Esta etapa podrá ser desarrollada con apoyo o recurso externo con experiencia especializada. El siguiente cronograma evidenciará los resultados de la implementación. En esta etapa se ejecutará Medida de Control N° 1.

**Cuadro N° 06 - Cronograma y responsable de la etapa: Realización de pruebas**

PLAN DE TRANSICIÓN AL PROTOCOLO IPV6	Resp	Ene-27	Feb-27	Mar-27	Abr-27	May-27	Jun-27	Jul-27	Ago-27
<b>Etapa 2: Realización de pruebas</b>									
Pruebas de conectividad IPv6 de extremo a extremo (funcionalidad y compatibilidad de los equipos, software y sistemas)	Int/Ext								
Pruebas de rendimiento (calidad de servicio)	Int/Ext								
Pruebas de efectividad de las políticas de seguridad IPv6	Int/Ext								
Documentación de resultados y afinamiento de las configuraciones de ser necesario	Int/Ext								

### 9. CAPACITACIÓN Y SENSIBILIZACIÓN

La capacitación del personal técnico que se encargará de la implementación, es fundamental, ya que tiene el propósito de familiarizar al personal con los conceptos y lógica de funcionamiento del protocolo.

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 Gerencia General a fin de garantizar los recursos y el apoyo institucional que permitirá:

- a. Desplegar la transición al IPv6 en la entidad y estar preparados a la integración global del protocolo hacia nuevas tecnologías.
- b. Convocar el compromiso de participación para las próximas tareas que involucran el proceso de migración.

Esta etapa se podrá desarrollar en conjunto con recursos externos especializados en capacitación técnica sobre el protocolo IPv6. También deberá desarrollarse la sensibilización sobre el protocolo IPv6 al usuario final. Asimismo, en esta etapa se ejecutará la Medida de Control N° 5.

**Cuadro N° 07 - Cronograma y responsable de la etapa: Capacitación y sensibilización**

PLAN DE TRANSICIÓN AL PROTOCOLO IPV6	Resp	Ene-27	Feb-27	Mar-27	Abr-27	May-27	Jun-27	Jul-27	Ago-27
<b>Etapa 3: Capacitación y sensibilización</b>									
Capacitación sobre temas técnicos IPv6 para especialistas	Ext								
Sensibilización para funcionarios sobre el protocolo IPv6	Ext								

### 10. PRESUPUESTO ESTIMADO

Luego de realizada una indagación de mercado, se tendrá un monto preciso del presupuesto para la ejecución de todas las etapas. Sin embargo, se han proyectado costos aproximados de inversión, asociados a los bienes y servicios que se han considerado dentro de las alternativas de tratamiento presentadas en el Cuadro N° 04.

En cuanto a las medidas de tratamiento identificadas en el punto 5 del Cuadro N° 04; se ha optado por implementar la conexión a Internet IPv6 a través de los recursos proporcionados por LACNIC, con direccionamiento no asignado (Provider Independent). Se precisa que, al optar por esta alternativa, ya no será necesario adquirir un Firewall con soporte de mecanismo de transición tunneling, además, el bloque de direcciones IPv6 PI que se reciben, son independientes del ISP que se contrate; con lo cual se evita la enumeración.

En el punto N° 5 se detallan los costos de todas las alternativas de tratamiento identificadas en el punto 1 del Cuadro N° 04; la decisión de cuál será la alternativa a implementar debe ser tomada de manera coordinada entre la Oficina de Tecnologías de la Información y el área usuaria (la Oficina de Recursos Humanos), tomando en consideración las funcionalidades que cada alternativa provea y el costo-beneficio final de la solución.

Cuadro N° 07 – Costos estimados asociados a los bienes y servicios considerados en las alternativas de tratamiento del Cuadro N° 04

N°	Descripción del bien o servicio	Valor S/
1	Servicio de elaboración y diseño, incluidos los TDR para la implementación de una arquitectura de transición de IPv4 a IPv6 (Medida de control N°1, 2, 3, 4 y 5).	150,000.00
	Implementación de una arquitectura de transición de IPv4 a IPv6, direccionamiento, configuración de todos los equipos de la red, elaboración de políticas de seguridad para los servicios publicados a IPv6 y navegación de usuarios, ejecución de pruebas, servicio de capacitación y sensibilización (Medida de control N°1, 2, 3, 4 y 5).	
	Servicio de elaboración y diseño incluido TDR para la adquisición y gestión de direccionamiento IPv4 a IPv6 independiente vía LACNIC (Medida de control N°6).	
	Servicio de elaboración y diseño incluido TDR para conexión a Internet vía BGP con direccionamiento no asignado.	
2	Pago único LACNIC por los recursos IPv4, IPv6 y ASN (Medida de control N°6).	20,000.00
3	Pago anual LACNIC por los recursos IPv4, IPv6 y ASN (Medida de control N°6).	13,000.00
4	Desarrollo de software para la modificación de la auditoría de los sistemas WEB, que soporte la cantidad de caracteres de IPv6 (Medida de control N°6).	108,000.00
5	Adquisición e implementación del motor de base Oracle (Enterprise) (Medida de control N°6).	350,000.00
	Servicio de desarrollo de software para auditoría del sistema administrativo financiero (SAF) (Medida de control N°6).	100,000.00
	Adquirir una herramienta de software que reporte la auditoría del sistema SAF conjuntamente con el software Oracle Standard (Medida de control N°6).	100,000.00
	Adquirir o contratar bajo suscripción, una herramienta de software específica para la gestión de RRHH, la cual sea compatible con IPV6 (Medida de control N°6).	200,000.00
	Implementar una herramienta de software público gratuito para entidades del estado, disponible desde la Plataforma Nacional de Software Publico, la cual sea compatible con IPV6 (Medida de control N°6).	30,000.00
6	Adquisición e implementación de equipo Antispam o contratación del servicio Antispam (Medida de control N°6).	100,000.00
7	Adquisición de equipos de la red inalámbrica o contratación del servicio (Medida de control N°6).	150,000.00
8	Imprevistos por retrasos administrativos y/o técnicos	10 a 15 % costo proyecto

## 11. ANEXO

Cronograma general de actividades detalladas de cada etapa (Implementación, Pruebas, Capacitación y Sensibilización), que incluye plazos y responsables, y entregables.

**Cronograma General del Plan de Transición al Protocolo IPv6 del SAT**

	Resp	Dic-25	Ene-26	Feb-26	Mar-26	Abr-26	May-26	Jun-26	Jul-26	Ago-26	Set-26	Oct-26	Nov-26	Dic-26	Ene-27	Feb-27	Mar-27	Abr-27	May-27	Jun-27	Jul-27	Ago-27		
<b>PLAN DE TRANSICIÓN AL PROTOCOLO IPV6</b>																								
<b>Etap 1: Implementación del protocolo IPv6</b>																								
Elaboración de TDR para el diseño de una arquitectura de transición de la IPv4 a IPv6, direccionamiento, configuración de todos los equipos de la red, elaboración de políticas de seguridad para los servicios publicados a IPv6 y navegación de usuarios, elaboración de TDR LACNIC, pruebas y tiempo para la contratación del Servicio	Int																							
Implementación del protocolo IPv6	Ext																							
Elaboración de TDR para la gestión y adquisición de direccionamiento IPv4 e IPv6 independiente vía LACNIC.	Ext																							
Tiempo para la contratación del Servicio	Int																							
Tiempo para la asignación IPS LACNIC e inicio del servicio	Ext																							
Elaboración de TDR para el Servicio de Internet y Seguridad Gestionada, Internet vía BGP y con direccionamiento independiente IPv6	Int																							
Tiempo para la contratación del servicio.																								
Tiempo para la implementación e inicio del servicio.	Int/Ext																							
Elaboración de EETT para reemplazar el software que soporte IPv6 o Elaboración de TDR para Servicio de desarrollo de software.	Int																							
Tiempo para la contratación e implementación del bien o desarrollo del software	Int/Ext																							
Elaboración de TDR para modificar los sistemas WEB para que la reportería y auditoría que soporte la cantidad de caracteres que soporte IPv6	Int																							
Tiempo para la contratación e implementación del desarrollo del software	Int/Ext																							
Elaboración de EETT para reemplazar equipo de seguridad con soporte a IPv6 o TDR para contratar un servicio de antispam que soporte el protocolo	Int																							
Tiempo para la contratación e implementación del bien o inicio del servicio	Int/Ext																							
Elaboración de EETT para reemplazar el sistema inalámbrico con soporte a IPv6 o TDR para la contratación del servicio.	Int																							
Tiempo para adquisición e implementación del sistema	Int/Ext																							
<b>Etap 2: Realización de pruebas</b>																								
Pruebas de conectividad IPv6 de extremo a extremo (funcionalidad y compatibilidad de los equipos, software y sistemas)	Int/Ext																							
Pruebas de rendimiento (calidad de servicio)	Int/Ext																							
Pruebas de efectividad de las políticas de seguridad IPv6	Int/Ext																							
Documentación de resultados y afinamiento de las configuraciones de ser necesario	Int/Ext																							
<b>Etap 3: Capacitación y sensibilización</b>																								
Capacitación sobre temas técnicos IPv6 para especialistas	Ext																							
Sensibilización para funcionarios sobre el protocolo IPv6	Ext																							

Int= Interno / Ext= Externo

Firmado digitalmente por TERRY RIVERA CABALLERO FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:29:01 -05:00

Firmado digitalmente por SANZ DIAZ Carlos Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:39:14 -05:00

Firmado digitalmente por TORRES ARMAS Genaro FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:48:44 -05:00

Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:46:28 -05:00

Firmado digitalmente por REYES Dayana Erka FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:42:30 -05:00

Firmado digitalmente por TUME LEDESMA Obtoniel Wladir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:26:34 -05:00

Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 01.07.2025 19:14:37 -05:00

Firmado digitalmente por QUISPE REYES Dayana Erka FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:42:30 -05:00

Firmado digitalmente por TUME LEDESMA Obtoniel Wladir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:26:34 -05:00

Firmado digitalmente por SANZ DIAZ Carlos Alberto FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:39:14 -05:00

Firmado digitalmente por TORRES ARMAS Genaro FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:48:44 -05:00

Firmado digitalmente por CAMINO LEON Juan Martin FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:46:28 -05:00

Firmado digitalmente por REYES Dayana Erka FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 15:42:30 -05:00

Firmado digitalmente por TUME LEDESMA Obtoniel Wladir FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 30.06.2025 16:26:34 -05:00

Firmado digitalmente por CABALLERO ESTELLA Maria Del Pilar FAU 20337101276 soft Motivo: Soy el autor del documento Fecha: 01.07.2025 19:14:37 -05:00