REPUBLICA DEL PERU

Resolución Ministerial

N° 304 -2018-PCM

Lima, 21 NOV. 2018

CONSIDERANDO:

Que, de conformidad con lo establecido en el artículo 32 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, compete a la Oficina de Tecnologías de la Información, entre otros, formular, proponer y ejecutar el plan estratégico de tecnología de la información en concordancia con los objetivos estratégicos institucionales y las necesidades de los órganos de la entidad;

Que, mediante Decreto Supremo N° 081-2017-PCM, se aprobó la formulación de un Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública, con el objetivo de disponer la formulación de un Plan de Transición, a implementarse de manera progresiva en toda la infraestructura tecnológica: software, hardware, servicios, entre otros, en las entidades de la Administración Pública;

Que, a través de los Informes N° D000041-2018-PCM-OTI-LGT, N° D000047-2018-PCM-OTI-LGT y N° D000052-2018-PCM-OTI-LGT elaborados por la Oficina de Tecnologías de la Información de la Presidencia del Consejo de Ministros, se sustenta la propuesta del Plan de Transición al Protocolo IPv6 de la PCM;

Que, el Plan de Transición al Protocolo IPv6 de la Presidencia del Consejo de Ministros, propuesto por la Oficina de Tecnologías de la Información, tiene como objetivo mejorar la seguridad y calidad de los servicios informáticos que la PCM brinda a la ciudadanía y público en general, incorporando nuevas tecnologías compatibles con el protocolo de comunicación en la Internet IPv6;

Que, en ese sentido, al considerarse necesario propiciar un entorno que garantice la adopción del Protocolo IPv6, y ante el inminente agotamiento de las direcciones IPv4, resulta necesario aprobar el Plan de Transición al Protocolo IPv6 de la Presidencia del Consejo de Ministros;

De conformidad con lo establecido en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; el 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; y, el Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros;

SE RESUELVE:

Artículo 1.- Aprobar el Plan de Transición al Protocolo IPv6 de la Presidencia del Consejo de Ministros, el cual forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Disponer la publicación de la presente resolución ministerial en el Portal Institucional de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) conforme a lo establecido en la Resolución Ministerial N° 153-2015-PCM de fecha 12 de junio de 2015.

Regístrese, comuníquese y publíquese.

CESAR VILLANUEVA ARÉVALO
Presidente del Consejo de Ministros

Plan de Transición al Protocolo IPv6 de la Presidencia del Consejo de Ministros

ÍNDICE

I. INTRODUCCIÓN

En la actualidad se ha podido observar que las comunicaciones e información publicadas en la Internet se han convertido en parte fundamental para la atención al ciudadano. Siendo las tecnologías y servicios desarrollados en los últimos años los que facilitan los medios para comunicarnos con los ciudadanos, instituciones y entidades públicas.

Estas tecnologías y servicios de la Internet basan su funcionamiento sobre un estándar de comunicación denominada Protocolo de Internet (IP - Internet Protocol), siendo la versión número cuatro de dicho protocolo (IPv4) la más utilizada actualmente en el mundo, y la que viene también empleando la Presidencia del Consejo de Ministros (PCM).

Cuando se diseñó el IPV4 como un estándar para facilitar las comunicaciones en la Internet, no se proyectó el rápido crecimiento que tendría esta red, ni la diversidad de servicios y dispositivos que lo utilizarían. Hoy en día existen además de las computadoras: videocámaras, sistemas de seguridad, drones, lavadoras, cocinas, refrigeradoras, equipos médicos, entre muchos otros dispositivos que basan su funcionamiento en este protocolo. Esta alta diversidad y explosivo crecimiento de los servicios a través de la Internet, ha generado que las capacidades del IPv4 de asignación de direcciones este muy cerca de colapsar.

Por este motivo, y previendo la situación, el organismo que se encarga de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), ha trabajado en los últimos años en una nueva versión del Protocolo de Internet, concretamente la versión 6 (IPv6), que posee direcciones suficientes para abastecer la demanda de comunicaciones por Internet para los próximos 480 años.

El despliegue de IPv6 se viene realizando gradualmente, en una coexistencia ordenada con IPv4, al que se irá desplazando a medida que dispositivos de cliente, equipos de red, aplicaciones, contenidos y servicios se vayan adaptando a la nueva versión del protocolo de Internet.

Por ello, es importante, conocer cómo se realiza el despliegue del nuevo protocolo de Internet, tanto si somos usuarios residenciales, como corporativos, proveedores de contenidos, proveedores de servicios de Internet, así como la propia administración pública.

Es así, que el objetivo del presente documento tiene como fin establecer el plan de transición al protocolo IPv6 para la PCM, el cual incluye las tareas de definición del alcance, establecer el diagnóstico de la infraestructura tecnológica, analizar el modo de implementación, definir las pruebas previas y su posterior pase a producción, establecer los parámetros de capacitación y sensibilización a los usuarios.

II. BASE LEGAL

- Decreto Supremo N°054-2011-PCM, que aprueba el Plan Estratégico de Desarrollo Nacional denominado Plan Bicentenario: El Perú hacia el 2021.
- Decreto Supremo N°066-2011-PCM, aprueba el "Plan de Desarrollo de la Sociedad de Información del Perú – La Agenda Digital Peruana 2.0".
- Decreto Supremo N°081-2013-PCM, Aprueba la Política Nacional de Gobierno Electrónico.
- Resolución Ministerial N°004-2016-PCM, que aprueba el 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.
- Decreto Supremo N°081-2017-PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las Entidades Públicas.
- Decreto Supremo N°006-2017-JUS, aprueban Texto Único Ordenado de la Ley N°27444 – Ley del Procedimiento Administrativo General.
- Decreto Supremo N°022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Ley N°27658, Ley Marco de Modernización de la Gestión del Estado
- Ley N°29158, Ley Orgánica del Poder Ejecutivo.
- Las demás normas relacionadas con el ámbito funcional de la PCM.

III. OBJETIVO

Mejorar la seguridad y calidad de los servicios informáticos públicos que la PCM brinda a la ciudadanía y público en general, incorporando nuevas tecnologías compatibles con el protocolo de comunicación en la Internet IPv6.

IV. ALCANCE

El presente plan de transición al protocolo IPv6 contempla la migración de todos los servicios informáticos publicados por la PCM en la Internet.

V. FASES DE TRANSICIÓN AL PROTOCOLO IPv6

5.1. FASE I. PLANIFICACIÓN

La fase de planificación es importante para realizar la transición al protocolo IPv6, ya que determinará la realización de la evaluación de las capacidades técnicas y compatibilidades de la infraestructura tecnológica con el referido protocolo IPv6, detectar las oportunidades de mejora tecnológica, y diseñar una configuración óptima para su implementación y posterior funcionamiento bajo esta nueva versión del protocolo.

Dado el alcance formulado, el equipamiento de la infraestructura tecnológica está comprendido por el hardware, software, sistemas informáticos y servicios informáticos (brindados estos últimos por empresas privadas) de la PCM en la Internet.

Para tal fin, se realizarán las actividades de inventario de la infraestructura tecnológica, consolidación del diagnóstico y posteriormente realizar el respectivo análisis de riesgos.

5.1.1 Inventario

A fin de tener conocimiento de la cantidad de componentes en la infraestructura tecnológica para la transición al protocolo IPv6, se realizará un inventario que nos brindará el universo de componentes considerados según el alcance propuesto. Los componentes de infraestructura tecnológica a considerar son los siguientes:

- Hardware
- Software
- Sistemas Informáticos
- Servicios Informáticos

5.1.1.1. Hardware

Es la parte tangible de un dispositivo informático, de acuerdo al alcance, se refiere al equipamiento de seguridad perimetral de la red (equipos que protegen la red de accesos no autorizados desde la Internet), de los servidores (aquellos que publican información o sistemas hacia la Internet), y equipos de videoconferencia (dispositivos para realizar conferencias entre puntos geográficamente distantes a través de la Internet).

En la siguiente tabla se resume el hardware de la entidad:

Tabla N°01. Hardware

N°	Hardware	Cantidad
1	Seguridad perimetral	5
2	Servidores	9
3	Videoconferencia	4

5.1.1.2. Software

Es la parte digital de un dispositivo informático; es decir, el conjunto de instrucciones, programas y reglas informáticas que requiere un sistema o servicio para funcionar. De acuerdo al alcance, se refiere a los sistemas operativos (sistema básico que requiere todo computador para poder operar), software de programación (software especializado que nos permite desarrollar nuevos softwares personalizados para atender las necesidades de las áreas usuarias) y gestores de base de datos (soporte de almacenamiento de información de manera estructurada y de gran capacidad).

En la siguiente tabla se resume el software de la entidad:

Tabla N°02. Software

N°	Software	Cantidad
1	Sistema Operativo	2
2	Software de Programación	3
3	Gestor de Base de Datos	3

5.1.1.3. Sistemas Informáticos

Son elementos de hardware y software que interactúan entre sí para procesar información y facilitarla según las necesidades de la entidad. De acuerdo al alcance, se refiere a los portales (información institucional de acceso público para toda la ciudadanía desde cualquier navegador) y las aplicaciones web (aplicaciones informáticas para atender necesidades y/o usuarios específicos, también accesibles desde cualquier navegador).

En la siguiente tabla se resumen los sistemas informáticos de la entidad:

Tabla N°03. Sistemas informáticos

N°	Sistemas Informáticos	Cantidad
1	Portales	15
2	Aplicaciones Web	31

5.1.1.4. Servicios Informáticos

Son aquellas soluciones que permiten utilizar los servicios de la Internet de manera eficiente y oportuna. Estos servicios son usualmente brindados por empresas privadas e implican un costo por uso de los mismos.

Se resume a continuación los servicios que actualmente recibe la PCM:

Tabla N°04. Servicios informáticos

N°	Servicios informáticos	Cantidad
1	Acceso de Internet	1
2	Interconexión de sedes de la PCM (sede central)	7
3	Seguridad perimetral gestionada	1
4	Dominios de Internet	27
5	Servicio de telefonía fija	1

5.1.2 Diagnóstico

Proporcionará el conocimiento técnico de las capacidades del protocolo IPv6 disponibles en la actual infraestructura tecnológica de la PCM, de manera que nos permita evaluar y proyectar diferentes estrategias para la transición hacia el protocolo IPv6.

Esta evaluación tendrá la siguiente información:

- Verificación de las características específicas del IPv6 que existan o estén habilitadas en la infraestructura tecnológica de la PCM identificada en el inventario realizado.
- Contrastar la información verificada en el ítem anterior, con las características específicas del IPv6 disponibles que pueden ser adquiridos o contratados por la entidad como mejora a la actual infraestructura tecnológica.

Para el diagnóstico se utilizará el formato del Anexo 1.

5.1.3 Análisis de Riesgos:

Previo a las etapas de implementación y pruebas; se debe identificar la posible ocurrencia de eventos que podrían impactar las evaluaciones y/o resultados de la presente planificación, definiendo estos eventos como riesgos, siendo parte del presente plan su identificación, valoración y mitigación.

5.1.3.1 Identificación de riesgos:

Realizado el diagnóstico del equipamiento de la infraestructura tecnológica identificada en el punto 5.1.2, dando como resultado que algunos componentes necesiten alguna mejora para la transición al Protocolo IPv6, se aplicarán técnicas de lluvia de ideas y juicio de personal experto para determinar los potenciales riesgos, mismos que serán listados en una relación para su posterior valoración.

5.1.3.2 Valoración de Riesgos:

Una vez identificado los riesgos, se aplicará el método de Valoración de Riesgos por Probabilidad e Impacto, el cual se basa en cuantificar la probabilidad de ocurrencia del riesgo identificado, multiplicada por el valor establecido como impacto, siendo el número resultante el Valor del Riesgo. Mientras más alto el valor, mayor el riesgo.
Para esta escala de valoración se definen los siguientes parámetros para las probabilidades de ocurrencia del riesgo:

Tabla N°05 Valoración de la Probabilidad de Ocurrencia

Valor	Clasificación	Definición
5	Muy Alta (MA)	El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta. 13 a más veces al año (proporcional a una (1) vez a la semana o más).

Valor	Clasificación	Definición
4	Alta (A)	Existen antecedentes de que el evento ocurrirá, dentro de un plazo de tiempo que implique una acción para enfrentarlo, pero la frecuencia no es alta. 5 a 12 veces al año (proporcional a una vez al mes).
3	Moderada (M)	Es posible que ocurra el evento con una frecuencia baja. 3 o 4 veces al año.
2	Baja (B)	Si bien el evento puede ocurrir el periodo entre uno y otro evento puede ser muy grande. Al menos 2 veces al año.
1	Muy Baja (MB)	El evento no ocurre nunca o casi nunca. Ha ocurrido al menos una (1) vez al año.

Para la escala de valoración del impacto se define lo siguiente:

Tabla N°06 Valoración del Impacto del Riesgo

Nivel	Descripción	Impacto
5	Extremo	Impacta en forma severa en la Institución al punto de comprometer la confidencialidad o integridad de información crítica y/o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a toda la Institución y su efecto repercute en todo el personal involucrado.
4	Alto	Impacta en forma grave a un área o servicio específico de la Institución, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable. Su efecto está limitado dentro de la Institución.
3	Mediano	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Bajo	El impacto es leve y se puede prescindir del mismo en un tiempo limitado.
1	No Significativo	No representa un impacto importante para la Institución.

Considerando la probabilidad de ocurrencia por el impacto se define la valoración de los riesgos:

Tabla N°07 Valorización de Riesgos

Impacto	Valor	Probabilidad	Valor	Nivel de Riesgo	Valor Total
Extremo	5	Muy Alta	5	Extremo	25
Alto	4	Muy Alta	5	Extremo	20
Mediano	3	Muy Alta	5	Extremo	15
Bajo	2	Muy Alta	5	Alto	10
No Significativo	1	Muy Alta	5	Mediano	5
Extremo	5	Alta	4	Extremo	20
Alto	4	Alta	4	Extremo	16
Mediano	3	Alta	4	Alto	12
Bajo	2	Alta	4	Mediano	8
No Significativo	1	Alta	4	Bajo	4
Extremo	5	Moderada	3	Extremo	15
Alto	4	Moderada	3	Alto	12
Mediano	3	Moderada	3	Alto	9
Bajo	2	Moderada	3	Mediano	6
No Significativo	1	Moderada	3	Bajo	3
Extremo	5	Baja	2	Alto	10
Alto	4	Baja	2	Mediano	8
Mediano	3	Baja	2	Mediano	6
Bajo	2	Baja	2	Bajo	4
No Significativo	1	Baja	2	No Significativo	2
Extremo	5	Muy Baja	1	Mediano	5
Alto	4	Muy Baja	1	Bajo	4
Mediano	3	Muy Baja	1	Bajo	3
Bajo	2	Muy Baja	1	No significativo	2
No Significativo	1	Muy Baja	1	No significativo	1

Estos riesgos se clasificarán de acuerdo a niveles, en el cual se muestra en la siguiente tabla:

Tabla N°08 Nivel de Riesgo

Rango de Riesgo	Nivel de Riesgo	Descripción de las consecuencias
De 15 a 25	Extremo	Puede afectar seriamente a la Entidad, en términos de paralización de las operaciones. Requiere acción correctiva inmediata más allá del tiempo tolerable, pérdidas considerables o demandas legales y daño considerable.
De 9 a 12	Alto	Puede afectar los niveles de operación y servicios de la Entidad, incumplimiento de metas, y divulgación no autorizada de información fuera de la Entidad. Requiere una acción correctiva sujeta a la discreción de los Propietarios del Riesgo en términos de plazos y compromisos.
De 5 a 8	Mediano	Afecta a los activos de información de soporte a los activos principales, puede afectar la disponibilidad en áreas específicas de la Entidad. La divulgación no autorizada no representa perjuicio importante para la Entidad. Su aceptación está sujeta a la revisión de los Propietarios del Riesgo.
De 3 a 4	Bajo	No causa un efecto considerable en la Entidad. Usualmente son aceptados sin revisión.
De 1 a 2	No Significativo	El efecto para la Entidad es insignificante. Usualmente no se les considera para la gestión de riesgos.

5.1.3.3 Tratamiento del Riesgo:

Determinada la importancia y el impacto del riesgo, el cual dará como resultado la valoración del riesgo, y de acuerdo a ello se realizarán las acciones de mitigación correspondiente, se reconoce en la siguiente tabla los niveles de tratamiento del riesgo:

Tabla N°09 Nivel del Tratamiento del Riesgo

Tratamiento	Detalles del Tratamiento de Riesgos
Reducir	Realizar la acción que corresponda para disminuir la probabilidad de ocurrencia de un riesgo y/o disminuir el impacto si se concreta a un umbral aceptable.
Aceptar	No realizar ninguna acción consciente o intencionadamente para hacer frente a un riesgo.
Evitar	Hacer desaparecer el riesgo, eliminar cualquier probabilidad de ocurrencia.
Transferir	Entregarle la administración de un riesgo a un tercero que lo pueda manejar mejor que la Institución.

5.2.FASE II. IMPLEMENTACIÓN DEL PROTOCOLO IPv6

Realizado el inventario, diagnóstico y análisis de riesgos; se realizarán las siguientes actividades de acuerdo a la siguiente matriz:

Tabla N°10 Matriz de Implementación del Protocolo IPv6

Ítem	Actividades	Objetivo
1	Habilitar el protocolo IPv6 a los componentes de la infraestructura tecnológica de acuerdo al diagnóstico	Tener el direccionamiento IPv6 para cada uno de los componentes de la infraestructura tecnológica de acuerdo al diagnóstico realizado en la Fase I, para la utilización del nuevo protocolo de comunicaciones.
2	Configurar el protocolo IPv6 en los servicios informáticos	Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6, simulando el comportamiento de la red de comunicaciones, agregando carga, servicios y usuarios finales tanto internos como externos, pruebas realizadas sobre el procedimiento de IPv6 usando la metodología en Doble Pila; así mismo revisar dicho comportamiento de la red IPv6 para usuarios finales tanto internos como externos.
3	Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones	Activar las políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posee la PCM, con los RFC de seguridad en IPv6; para la protección del tráfico de la información.
4	Coordinar con el (los) proveedor (es) de servicios ISP, para establecer la conectividad en IPv6 hacia el exterior	Trabajar en coordinación con el (los) proveedor (es) de servicios de Internet –ISP, para establecer el enrutamiento necesario del segmento de IPv6 y la conectividad integral, desde el interior de la red LAN de la PCM, hacia el exterior de las redes WAN a fin de garantizar que la generación de tráfico IPv6 nativo ante la comunidad de Internet.

5.3.FASE III. REALIZACION DE PRUEBAS

La realización de las pruebas permitirá determinar que los componentes de la infraestructura tecnológica funcionan adecuadamente y cumplen con las medidas de seguridad respecto al protocolo IPv6.

Las actividades determinadas para la realización de las pruebas será responsabilidad de la Oficina de Tecnologías de la Información, en coordinación con la Oficina General de Administración.

Dichas actividades se describen en la siguiente matriz:

Tabla N°11 Matriz de la realización de pruebas

Ítem	Actividades	Objetivo
1	Probar la funcionabilidad y monitoreo del IPv6	Establecer las pruebas y el monitoreo de la funcionalidad del Protocolo IPv6 de los componentes de la infraestructura tecnológica en un ambiente que permita empezar a generar tráfico de la PCM hacia Internet y viceversa.
2	Analizar la información y probar la funcionabilidad frente a las políticas de seguridad	Establecer las pruebas de funcionalidad del nuevo protocolo frente a las políticas de seguridad de la infraestructura tecnológica y sustentando las pruebas realizadas.
3	Afinamiento de las configuraciones realizadas a la infraestructura tecnológica	Establecer las acciones para el afinamiento de las configuraciones realizadas a la infraestructura tecnológica para obtener su optimización respecto al Protocolo IPv6. Dicho afinamiento compete tanto a los proveedores ISP, como a la PCM, para que la totalidad de la infraestructura tecnológica, que son publicados en Internet y queden operativos a IPv6.

VI. CAPACITACIÓN

Para la adecuada transición del protocolo IPv4 al IPv6, todo el personal de la Oficina de Tecnología de Información recibirá una charla de inducción del protocolo IPv6. Además, se realizarán capacitaciones necesarias referente al protocolo IPv6, teniendo énfasis, para el desarrollo de Sistemas Informáticos y para la configuración y administración de los equipos de comunicación y seguridad de la PCM.

La capacitación se realizará de manera previa al diagnóstico de la infraestructura tecnológica.

VII. PRESUPUESTO ESTIMADO

El presupuesto estimado está detallado de acuerdo a las fases definidas en el punto 5 del presente documento, y categorizadas según el tipo de gasto en: adquisiciones, servicios y consultorías, además de las fechas estimadas para su realización.

VIII. ANEXOS

Anexo 1: Diagnóstico de la Infraestructura Tecnológica

Anexo 2: Cronograma y Presupuesto Estimado del Plan de Transición al protocolo IPv6

IX. CONCLUSIONES

- La transición al protocolo IPV6 debe realizarse de manera gradual.
- Existe equipamiento a nivel de infraestructura tecnológica que no soporta el protocolo IPv6 y deberá ser adquirido o contratado, según corresponda.
- Los servicios externos deben ser revisados en entornos de prueba previo a la migración al protocolo IPv6.

ANEXO 1: DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

Características IPV6	Equipamiento de Infraestructura Tecnológica												Resultado del Diagnóstico (Índices de compatibilidad, rendimiento y seguridad informática)
	Hardware			Software			Sistemas Informáticos			Servicios Informáticos			
	Hw1	Hw2	Hw3	Sw1	Sw2	Sw3	Sist.1	Sist.2	Sist.3	Srv.1	Srv.2	Srv.3	
Atributo 1	*	*	*	*	*	*	*	*	*	*	*	*	
Atributo 2	*	*	*	*	*	*	*	*	*	*	*	*	
Atributo 3	*	*	*	*	*	*	*	*	*	*	*	*	
Atributo 4	*	*	*	*	*	*	*	*	*	*	*	*	
Atributo 5	*	*	*	*	*	*	*	*	*	*	*	*	
Atributo 6	*	*	*	*	*	*	*	*	*	*	*	*	
	1.- Indica la valoración de compatibilidad, rendimiento y seguridad informática.												
	2.- El valor 0 indica que el equipamiento de infraestructura tecnológica NO es compatible con la implementación del Protocolo IPv6												
	3.- El valor 1 indica que el equipamiento de infraestructura tecnológica es compatible, pero no mejora el rendimiento con la implementación del Protocolo IPv6.												
	4.- El valor 2 indica que el equipamiento de infraestructura tecnológica es compatible y mejora el rendimiento con la implementación del Protocolo IPv6.												
	5.- El valor 3 indica que el equipamiento de infraestructura tecnológica es compatible, mejora el rendimiento y seguridad informática con la implementación del Protocolo IPv6.												

ANEXO 2: CRONOGRAMA Y PRESUPUESTO ESTIMADO DEL PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

	ACTIVIDAD	DESCRIPCIÓN	RECURSOS	PRESUPUESTO			CRONOGRAMA							
				ADQUISICIONES	SERVICIOS	CONSULTORIAS	2018	2019		2020		2021		2022
							II-SEM	I-SEM	II-SEM	I-SEM	II-SEM	I-SEM	II-SEM	I-SEM
FASE I: PLANIFICACIÓN	INVENTARIO	Evaluación del Hardware, Software, Sistemas y Servicios Informáticos	Se realizará por personal de la OTI	—	—	—	S/0.00							
	DIAGNÓSTICO	Brecha de paso de IPV4 al IPV6 del Inventario identificado	Se realizará por personal de la OTI	—	—	—		S/0.00						
	ANÁLISIS DE RIESGOS	Análisis, Identificación, Valoración y Tratamiento del Riesgo	Se realizará por personal de la OTI	—	—	—			S/0.00					

FASE II: IMPLEMENTACIÓN		Habilitar el protocolo IPV6 a los componentes de la infraestructura tecnológica de acuerdo al diagnóstico	Se adquirirán los Hardware y/o Software que se requiera para atender la brecha	S/500,000.00	---	---				S/250,000.00	S/250,000.00			
		Configurar el protocolo IPV6 en los servicios informáticos	Se contratará una consultoría para realizar esta tarea	---	---	S/ 50,000.00					S/50,000.00			
		Activar las políticas de seguridad de IPV6 en los equipos de seguridad	Se realizará por personal de la OTI	---	---	---						S/0.00		
		Coordinar con el (los) proveedor (es) de servicios ISP, para establecer la conectividad en IPV6 hacia el exterior	Se contratarán los servicios correspondientes a través de los proveedores locales del Internet	---	S/500,000.00	---						S/250,000.00	S/250,000.00	
FASE III: REALIZACIÓN DE PRUEBAS		Probar la funcionabilidad y monitoreo del IPV6	Se realizará por personal de la OTI	---	---	---							S/0.00	S/0.00
		Analizar la información y probar la funcionabilidad frente a las políticas de seguridad	Se realizará por personal de la OTI	---	---	---							S/0.00	S/0.00
		Afinamiento de las configuraciones realizadas a la infraestructura tecnológica	Se realizará por personal de la OTI	---	---	---							S/0.00	S/0.00

CAPACITACIÓN		Charla e Inducción al Protocolo IPV6	Se coordinará con la Secretaría de Gobierno Digital para brindar esta charla técnica	—	—	—		S/0.00						
		Capacitación para incorporar el IPV6 en el desarrollo de Sistemas Informáticos	Se contratará una consultoría para brindar este servicio de capacitación	—	—	S/12,000.00		S/12,000.00						
		Capacitación para incorporar el IPV6 a nivel de los equipos de comunicación y seguridad de la PCM	Se contratará una consultoría para brindar este servicio de capacitación	—	—	S/50,000.00		S/50,000.00						
				S/500,000.00	S/500,000.00	S/112,000.00	S/0.00	S/62,000.00		S/550,000.00		S/500,000.00		S/0.00
				S/1,112,000.00										