Resolución Ministerial

Lima, 09 AGO. 2018

VISTOS:

La Memoranda (OGI) N° OGI03072018 y OGI03162018, de la Oficina General de Apoyo a la Gestión Institucional, así como el Memorándum (OPP) N° OPP10372018 de la Oficina General de Planeamiento y Presupuesto;

CONSIDERANDO:

Que, mediante Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, se 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 democrático, descentralizado y al servicio del ciudadano;

Que, mediante Decreto Supremo N° 081-2017-PCM, se aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública, con el objeto de disponer la formulación de un Plan de Transición al Protocolo IPV6, a implementarse de manera progresiva en toda la infraestructura tecnológica, programas informáticos, servicios, entre otros, en las entidades de la Administración Pública;

Que, mediante la Resolución Ministerial N° 0895-2017-RE, se aprueba el Plan Estratégico de Gobierno Electrónico del Ministerio de Relaciones Exteriores 2017-2019 y como parte de la adopción de estándares, se enuncia el impulsar la transición del protocolo IPv4 hacia IPv6, en los servicios disponibles en Internet por parte de la institución;

Que, de conformidad con lo establecido en el inciso n) del artículo 46 del Reglamento de Organización y Funciones del Ministerio de Relaciones Exteriores, aprobado mediante Decreto Supremo N° 135-2010-RE, la Oficina General de Apoyo a la Gestión Institucional, tiene como una de sus funciones, normar, coordinar y evaluar la implementación de las disposiciones emitidas por el sector encargado del gobierno electrónico e informática;

Que, asimismo, el referido Reglamento señala en el inciso g) del artículo 48, que la Oficina de Tecnologías de la Información tiene por función planificar, dirigir y supervisar la operatividad y calidad del servicio de telecomunicaciones de la entidad;

Que, la Oficina de Tecnologías de la Información de la Oficina General de Apoyo a la Gestión Institucional, como integrante del Sistema Nacional de Informática de acuerdo a lo establecido en el Decreto Legislativo N° 604 – Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, ha elaborado el Plan de Transición al Protocolo IPv6 del Ministerio de Relaciones Exteriores del Perú, cuyo alcance son los servicios que la institución expone en Internet;

Que, en consecuencia, conforme a lo dispuesto en el artículo 3 del Decreto Supremo N° 081-2017-PCM, es necesario expedir la Resolución Ministerial que apruebe el Plan de Transición al Protocolo IPV6 del Ministerio de Relaciones Exteriores.

0450

Resolución Ministerial

Con los visados de la Oficina de Tecnologías de la Información, la Oficina General de Apoyo a la Gestión Institucional, la Oficina General de Planeamiento y Presupuesto, y la Oficina General de Asuntos Legales;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 27658, Ley Marco de Modernización de la Gestión Pública, Ley N° 29357, Ley de Organización y Funciones del Ministerio de Relaciones Exteriores, y su Reglamento aprobado mediante Decreto Supremo N° 135-2010-RE; y en ejercicio de la facultad delegada mediante Resolución Ministerial N° 0065-2018/RE;

SE RESUELVE:

Artículo 1°.- Aprobar el "Plan de Transición al Protocolo IPV6 del Ministerio de Relaciones Exteriores", que como anexo forma parte integrante de la presente resolución.

Artículo 2°.- Remitir a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros el "Plan de Transición al Protocolo IPV6 del Ministerio de Relaciones Exteriores", que se aprueba en el artículo 1 de la presente resolución.

Artículo 3°.- Disponer que la presente Resolución y su anexo se publique en el Portal de Transparencia Estándar del Ministerio de Relaciones Exteriores.

Regístrese y comuníquese.

Registrado en la Fecha
09 AGO 2018
RM No. 0450 /RE

Néstor Popolizio Bardales
Ministro de Relaciones Exteriores

Oficina General de Apoyo a la Gestión Institucional

Oficina de Tecnologías de la Información

Plan de Transición al Protocolo IPv6 del Ministerio de Relaciones Exteriores

0450

ÍNDICE

I. Introducción

La ciudadanía y las instituciones, utilizan Internet como un medio que facilita una serie de actividades del día a día, donde se encuentran el correo electrónico, las búsquedas de sitios web, descarga y subida de archivos digitales, acceso a sistemas y aplicativos de atención en línea, comunicación entre Sedes, entre otros más, para lo cual es necesario la interconexión de una serie de componentes de red con los dispositivos tecnológicos utilizados por el ciudadano y/o funcionario público, lo cual se logra con la utilización de protocolos estándares como el Protocolo de Internet (IP).

El Decreto Supremo Nº 081-2017-PCM, señala que el Protocolo IP "*es utilizado para el intercambio de información entre redes o dispositivos conectados a la Internet, existiendo dos versiones de este protocolo, la versión 4 (IPv4) y la versión 6 (IPv6)*". Además el mencionado Decreto señala que "*una dirección IP identifica a un dispositivo dentro de una red IP, siendo su uso imprescindible para la comunicación entre dispositivos, acceso a servicios a través de Internet u otros, y conforme a lo manifestado por el Registro de Direcciones de Internet para América Latina y el Caribe- (LACNIC por sus siglas en inglés) sobre el agotamiento de la cantidad de direcciones de IPv4, emerge el uso de las direcciones basadas en el protocolo IPv6, como mecanismo para asegurar la provisión y acceso a servicios digitales basados en IPv6;*".
Las organizaciones de manera paulatina vienen trabajando en redes donde IPv4 e IPv6 conviven de manera independiente, ya que ambas constituyen protocolos diferentes, siendo IPv6 un protocolo "sucesor" de IPv4, para ello se debe tomar las medidas necesarias para una adecuada transición.
Los fundamentos para la creación de un protocolo como el IPv6 se pueden resumir en el siguiente ejemplo:

> Cada PC, Mac, Laptop, Smartphone, Servidor, Router, entre otros, que es conectado a internet tiene una dirección IP de cuatro grupos de números, con valores entre 0 y 255. Así, por ejemplo, una PC puede tener el IP 88.251.111.56. Si es una página web, puede tener otra dirección IP al cual se accede a través de un nombre, por ejemplo rree.gob.pe.
>
> Esta necesidad de direcciones IP únicas de cada dispositivo y páginas web, ha traído como consecuencia que actualmente el rango de direcciones disponibles con el protocolo IPv4 (cuatro grupos de números, con valores entre 0 y 255: 255.255.255.255) se haya agotado.
> En este mismo ejemplo, es necesario precisar que el protocolo IPv6 permite disponer de 4028236692093846346337460743176821145 6 conexiones en todo el planeta, a diferencia del IPv4, limitado a solo 4294967296 conexiones.

Además, el protocolo IPv6 ofrece mejores características en cuanto a escalabilidad, enrutamiento, seguridad, auto-configuración y rendimiento en comparación con el IPv4.

Es así, que el proceso de transición al nuevo protocolo IPv6 por parte del Ministerio de Relaciones Exteriores requiere la identificación de la infraestructura de redes y comunicaciones actual, con la finalidad de determinar que componentes (software, hardware y conectividad) ya cuentan con la compatibilidad con el nuevo protocolo IPv6 y los costos estimados que significará la transición al nuevo protocolo.

Adicionalmente a lo expuesto en el párrafo precedente, el Ministerio de Relaciones Exteriores requiere de especialistas, técnicos, ingenieros y usuarios que se encuentren debidamente capacitados en el nuevo protocolo IPv6, con miras a planificar un proceso óptimo de transición, puesta en marcha y operaciones con el nuevo protocolo, así como la selección de proveedores que brinden servicios de internet mediante el nuevo protocolo.

II. Base Legal

- Decreto Supremo 081-2017-PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Legislativo N° 1017, Decreto Legislativo que aprueba la Ley de Contrataciones del Estado, y su Reglamento, aprobado con Decreto Supremo N° 184-2008-EF, de aplicación hasta la entrada en vigencia de la Ley N° 30225.
- Resolución de Contraloría N° 163-2015-CG, aprueba la Directiva N° 007-2015CG/PROCAL, Directiva de los Órganos de Control Institucional.
- Decreto Supremo N° 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información - La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico.

III. Objetivos del Plan de Transición

- Definir las actividades que permitan, de manera progresiva, adaptar la infraestructura, plataforma y servicios públicos digitales [1] del Ministerio de Relaciones Exteriores al Protocolo IPV6.
- Identificar la situación actual de la infraestructura, plataformas y servicios públicos digitales en relación al protocolo Ipv4 y/o Ipv6.

IV. Alcance del Plan de Transición

El presente plan de transición contempla como alcance los servicios que el Ministerio de Relaciones Exteriores expone en Internet.

V. Riesgos de no adopción del Protocolo IPv6

5.1. Riesgos Identificados

La Gestión de Riesgos es un proceso continuo, para ello es necesario usar un plan de tratamiento de riesgos con finalidad de implementar las recomendaciones y mejorar la toma de decisiones. Al respecto, el Ministerio de Relaciones Exteriores teniendo en cuenta las buenas prácticas toma como referencia la ISO 31000 Gestión del Riesgo – Directrices y la ISO/IEC 27005 Gestión del Riesgo en Seguridad de la Información para su tratamiento de riesgos. En consecuencia, los riesgos son valorados en función del **impacto** que podría genera al logro de los objetivos del Ministerio de Relaciones Exteriores y su **probabilidad** de ocurrencia.

N°	Riesgo	Impacto	Probabilidad	Valoración		
				Alto	Medio	Bajo
1	Perdida de información	Alto	Bajo			
2	Daños físicos en los equipos	Alto	Medio			

[1] Aquel servicio público ofrecido de forma total o parcial a través de Internet u otra red equivalente que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales (teléfonos inteligentes plataformas no presenciales, etc.), para la producción y acceso a datos servicios y contenidos que generen valor público para los ciudadanos y personas en general Fuente. Decreto Supremo N° 033-2017-PCM, el documento puede ser consultado en:

N°	Riesgo	Impacto	Probabilidad	Valoración		
				Alto	Medio	Bajo
3	No disponibilidad de repuestos	Medio	Bajo			
4	Incompatibilidad de hardware	Medio	Bajo			
5	Inestabilidad de las aplicaciones	Alto	Medio			
6	Problemas de funcionamiento del S.O.	Alto	Medio			
7	Falta de compatibilidad ipv6 en los proveedores que brindan el servicio de Internet	Alto	Medio			
8	Cortes de energía eléctrica inesperados no superados	Alto	Alto			
9	Incompatibilidad de aplicaciones con el S.O.	Alto	Bajo			
10	Falta de conocimiento / capacitación / educación en seguridad IPv6	Alto	Medio			
11	Falta de compatibilidad ipv6 con las partes interesadas	Medio	Medio			

Leyenda:
Riesgos: Para la definición de los riesgos se toma como referencia los siguientes
Perdida de información | Daños físicos en los equipos | No disponibilidad de repuestos | Incompatibilidad de hardware | Inestabilidad de las aplicaciones | Problemas de funcionamiento del S.O. | Falta de compatibilidad ipv6 en los proveedores que brindan el servicio de Internet | Cortes de energía eléctrica inesperados no superados | Incompatibilidad de aplicaciones con el S.O. | Otros
Impacto: Alto, Medio y Bajo
Probabilidad: Alta, Media y Baja
Cuadro de Valoración:

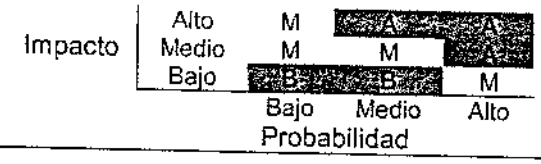

Tabla N° 01: Valoración de riesgos

VI. Diagnóstico de la Infraestructura Tecnológica

6.1. Hardware

El hardware que tiene el Ministerio de Relaciones Exteriores según el alcance, está conformado por equipamiento de comunicaciones, video conferencia, servidores físicos y virtualizados con niveles de capacidad en alta disponibilidad, para atender adecuadamente los servicios que se exponen en Internet.

6.1.1 Equipamiento de Comunicaciones:

Corresponde a los switches y routers que interactúan con las aplicaciones según el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Switches administrables WS-C2960-24TT-L (Cantidad 1)	X	X	
2	Switch administrable WS-C2960X-24TS-L (Cantidad 3)	X	X	

3	Switch administrable WS-C2960X-48FPD-L (Cantidad 2)	X	X	
4	Switch administrable NEXUS 5672UP (Cantidad 02)	X	X	
5	Switch administrable NEXUS 2248PQ (Cantidad 4)	X	X	
6	Switch administrable NEXUS 3048 Chassis (Cantidad 1)	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Equipo de Comunicaciones soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 02: Equipamiento de comunicaciones

6.1.2 Equipamiento de Video Conferencia

Corresponde a los equipos de video conferencia que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	CMA 4000	X	X	
2	FIREWALL POLYCOM VBP 5300 E25	X	X	
3	FIREWALL POLYCOM VBP 5300 ST25	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Equipo de Video Conferencia soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 03: Equipamiento de Videoconferencia

6.1.3 Equipamiento de Servidores – Físicos:

Corresponde a los servidores físicos que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Servidores dedicados HP Proliant BL 460c Gen 8 (Cantidad 16)	X	X	
2	Servidores dedicados HP Proliant BL 460c Gen 9 (Cantidad 02)	X	X	
3	Servidores dedicados HP Proliant DL 380 G7 (Cantidad 04)	X	X	
4	Servidores dedicados HP Proliant DL 380 Gen 8 (Cantidad 02)	X	X	
5	Servidor dedicado IBM System X 3650 (Cantidad 01)	X	X	

0450

6	Servidores dedicados IBM System X 3650 M3 (Cantidad 06)	X	X	
7	Servidores dedicados DELL Power Edge R720 (Cantidad 10)	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Servidores – Físicos soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 04: Equipamiento de Servidores –Físicos

6.1.4 Equipamiento de Servidores – Hypervisores:

Corresponde a los Hypervisores que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Servidores VMware ESXi 6.5 (Cantidad 12)	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Servidores – Hypervisores soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 05: Equipamiento de Servidores – Hypervisores

6.1.5 Equipamiento de Servidores – Sistema Operativo:

Corresponde al Sistema Operativo de los servidores que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	Servidor Virtual de Consulta de Apostilla	Windows Server 2012 R2 Standard	X	X	
2	Servidor Virtual de Sametime, DB2, Sametime Proxy Server, Wesphere, System Console	Windows Server 2012 Standard	X	X	
3	Servidor Virtual del Sistema de Gestión de Historias Médicas y acreditaciones	Windows Server 2012 R2 Standard	X	X	
4	Servidor Virtual de Base de Datos SQL 2005 y Aplicación de CEP	Windows Server 2003 R2 Standard Edition SP2	X	X	

5	Servidor Virtual de Correo Institucional; Servidor de Correo WEB	Windows Server 2012 R2 Standard	X	X	
6	Servidor Virtual de Portales Joomla	Debian GNU/Linux 8	X	X	
7	Servidor Virtual de Controlador de Dominio, DNS, DHCP Primario	Windows Server 2012 R2 Standard	X	X	
8	Servidor Virtual de Controlador de Dominio, DNS, DHCP Secundario	Windows Server 2012 R2 Standard	X	X	
9	Servidor Virtual de Aplicaciones Lotus	Windows Server 2012 R2 Standard	X	X	
10	Servidor Virtual Vcenter Ambiente de Virtualizacion	VMWare Vcenter Applicance Linux modificado	X	X	
11	Servidor Virtual de Base de Datos SQL 2005	Windows Server 2003 Standard Edition SP2	X	X	
12	Servidor Virtual de Aplicación Web Externas del MRE	Windows Server 2012 R2 Standard	X	X	
13	Servidor Virtual de Intranet Institucional	Windows Server 2016 Standard	X	X	
14	Servidor Virtual de Reportes SQL Server 2012	Windows Server 2016 Standard	X	X	

15	Servidor Virtual de aplicación de Portal Institucional Primario	Windows Server 2012 R2 Standard	X	X	
16	Servidor Virtual de Base de Datos de Portal Institucional Primario	Windows Server 2012 R2 Standard	X	X	
17	Servidor Virtual para Aplicaciones Web Internet	Windows Server 2008 R2 Enterprise SP1	X	X	
18	Servidor Virtual de Domino Server, Domino Directory	Windows Server 2012 R2 Standard	X	X	
19	Servidor Virtual de Base de Datos y Aplicación para SAM	Windows Server 2012 R2 Standard	X	X	
20	Servidor Virtual de Aplicaciones Sharepoint 2010	Windows Server 2003 R2 Standard Edition SP2	X	X	
21	Servidor Virtual de Base de Datos Sharepoint 2010	Windows Server 2008 R2 Enterprise SP1	X	X	
22	Servidor Virtual de IBM DB2	Windows Server 2012 R2 Standard	X	X	
23	Servidor Virtual de Lotus Traveler, Gateway de Mensajeria Dispositivos mobiles, Lotus Domino Server	Windows Server 2008 R2 Standard SP1	X	X	
24	Servidor Virtual ESRS Alertas de la solucion de	Windows Server 2008 R2	X	X	

	Almacenamiento de Virtualización	Standard SP1			
25	Servidor Virtual de Aplicaciones, Lotus Domino	Windows Server 2008 R2 Standard SP1	X	X	
26	Servidor Virtual Web, Lotus Domino	Windows Server Standard SP2	X	X	
27	Servidor Virtual de Base de Datos SQL 2005 y Aplicación de CEP	Windows Server 2003 R2 Standard Edition SP2	X	X	
28	Servidor Virtual de aplicación de Portal Institucional Secundario	Windows Server 2016 Standard	X	X	
29	Servidor Virtual de Base de Datos SQL Server, DB2	Windows Server 2012 R2 Standard	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Servidores – Sistema Operativo soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N°06: Equipamiento de Servidores – Sistema Operativo

6.2. Servicios

El Ministerio de Relaciones Exteriores tiene una serie de servicios informáticos contratados y que dan soporte a los procesos de la institución en el marco del alcance, como son el servicio de internet, alojamiento de dominio, correo electrónico y hosting.

6.2.1. Servicio de Internet

El servicio de Internet comprende también una sección de seguridad perimetral gestionada por lo cual es importante incluir los equipos de seguridad que el proveedor América Móvil Perú S.A.C. actualmente brinda como parte del servicio en este rubro para el 2018.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Routers Cisco 1900 series (Cantidad 02)	x	x	
2	Switch Catalyst 2960-S series (Cantidad 02)	x	x	

3	Firewall Fortinet 800D (Cantidad 04)	x	x	
4	Firewall Fortinet 500D (Cantidad 02)	x	x	
5	Fortisandbox 1000D (Cantidad 01)	x	x	
6	Anti-DDoS ARBOR (Cantidad 01)	x	x	
7	Fortimanager 200D (Cantidad 01)	x	x	
8	Fortianalyzer 400E (Cantidad 01)	x	x	
9	Fortimail 400E (cantidad 02)	x	x	
10	Appliance Imperva WAF x2010 (Cantidad 02)	x	x	
11	Appliance Imperva WAF M110	x	x	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de Internet soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 07: Servicio de internet

6.2.2. Servicio de alojamiento de dominio

Corresponde a los servicios de alojamiento de dominio que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	rree.gob.pe - NIC.pe	X	X	
2	consulado.pe - NIC.pe	X	X	
3	embajada.pe - NIC.pe	X	X	
4	adp.edu.pe - NIC.pe	X	X	
5	citasrefugiados.gob.pe - NIC.pe	X	X	
6	plataformavirtual.net.pe - NIC.pe	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de alojamiento de dominio soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 08: Servicio de dominio

6.2.3. Servicio de correo electrónico:

Corresponde a los servicios de correo electrónico que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Servicio de correo electrónico IBM Lotus Notes On Premise	X	X	
2	Servicio de correo electrónico Smart Cloud Notes Web	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de correo electrónico soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 09: Servicio de correo electrónico

6.2.4. Servicio de hosting o nube

Corresponde a los servicios de hosting que interactúan con las aplicaciones señaladas en el alcance.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	www.citasrefugiados.gob.pe	X	X	
2	www.plataformavirtual.net.pe	X	X	
3	www.adp.edu.pe	X	X	

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de hosting o nube soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 10: Servicio de hosting [Nube]

6.3. Aplicaciones

Las aplicaciones que brindan servicios corporativos hacia el ciudadano, se detallan en el siguiente cuadro. Cabe precisar que las aplicaciones descritas vienen funcionando con configuración 100% en ipv4.

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Academia Diplomática del Perú http://www.adp.edu.pe/	X		Alto
2	Apostilla Consulta http://apostillaconsulta.rree.gob.pe/consulta/	X		Alto
3	Chat Corporativo (Sametime) http://webchat.rree.gob.pe/	X		Medio
4	Consulado del Perú http://www.consulado.pe/	X		Alto
5	Consulta de visitas http://visitas.rree.gob.pe/consultavisitas/	X		Alto
6	Consulta Externa de Pasaportes http://cep.rree.gob.pe/cep/	X		Alto
7	Correo Web del MRE http://webmail.rree.gob.pe/	X		Alto
8	Embajada del Perú http://www.embajada.pe/	X		Alto
9	Intranet MRE http://intranet.rree.gob.pe/	X		Alto
10	Ley de Retorno http://leydelretorno.rree.gob.pe/	X		Alto
11	Libro de Reclamaciones http://apps.rree.gob.pe/portal/librecla.nsf	X		Alto
12	Módulo de Evaluación Bianual http://evaluacion.rree.gob.pe/meb/	X		Alto
13	Portal de Transparencia http://transparencia.rree.gob.pe/	X		Alto
14	Portal MRE http://www.rree.gob.pe/	X		Alto
15	Repositorio de la ADP http://repositorio.adp.edu.pe/	X		Alto
16	Sistema de Actividades Migratorias - MRE http://consulares.rree.gob.pe/sismre/	X		Alto
17	Sistema de Consulta de Fojas de Servicio http://mcf.rree.gob.pe/mcf_web	X		Alto
18	Sistema de Mensajería Móvil - Traveler http://traveler.rree.gob.pe/	X		Medio
19	Sistema de Registro de Eventos http://eventos.rree.gob.pe/	X		Alto
20	Visas Online MRE	X		Alto

0450

	http://visasonline.rree.gob.pe/			
21	Sistema de Consulta de Trámite http://apps.rree.gob.pe/ConsultaMPMRE	X		Medio
22	Servicios Web expuestos en la Plataforma de Interoperabilidad del Estado - PIDE http://pide.rree.gob.pe/WebService_MRE.svc?wsdl	X		Alto

Leyenda:
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de hosting [Nube] soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla 11: Aplicaciones

Conclusiones sobre el Diagnóstico de la Infraestructura Tecnológica

- El alcance definido permitirá al Ministerio de Relaciones Exteriores adoptar el protocolo IPv6 de manera progresiva, contemplado las fases para la transición controlada de los servicios y aplicaciones según en el diagnóstico que se efectúe.
- El plan contempla el cronograma estimado que organiza las actividades, a fin que las aplicaciones y el servicio de Internet del Ministerio de Relaciones Exteriores soporte el protocolo IPv6.
- El proceso de transición del protocolo IPv4 a Ipv6, permitirá que la infraestructura informática de la institución, garantice la coexistencia de ambos protocolos, manteniendo la disponibilidad, integridad y confidencialidad de los servicios informáticos expuestos a los ciudadanos y funcionarios o servidores del Ministerio, dentro y fuera de nuestro país.
- El alcance del plan se espera lograr en un periodo de 2 (dos) años, el mismo que se actualizará para un siguiente periodo, hasta lograr la totalidad del plazo previsto por el Decreto Supremo 081-2017-PCM.
- La implementación del protocolo IPv6 en la institución permitirá cumplir con el Decreto Supremo 081-2017-PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública.

VII. Implementación del Protocolo IPv6

El presente plan es un instrumento para ejecutar y realizar la transición de IPv4 a IPv6, donde se han planteado las fases, los entregables y responsables, de modo que en el plazo establecido por el D.S. N.° 081-2017-PCM, el Ministerio cumpla con la transición al protocolo IPv6.

Fase 1: Formulación de Plan y Políticas vinculadas con la Transición al Protocolo IPV6

Esta fase es muy importante dentro del proceso de transición al protocolo IPv6 y se trata del presente documento en el cual se encuentra el inventario de los activos de información listados en el Capítulo VI Diagnóstico de la Infraestructura Tecnológica los cuales forman parte del alcance del Plan de Transición.
El objetivo de la presente fase es disponer de un plan el cual permitirá migrar a IPv6 la infraestructura de hardware, software y conectividad comprendidas en el Alcance.

Forman parte de esta fase:

- Elaborar el inventario de activos en base al inventario de hardware y software identificando el soporte tanto para IPv4 como para IPv6.
- Afinar el presente plan en base al Alcance y al inventario de activos; el cual servirá la migración futura de toda la infraestructura a IPv6.
- Diagnosticar en base a los riesgos los activos que deben ser atendidos para el cumplimiento de funcionamiento en protocolo IPv6

- Medir el avance de implementación.
- Presentar los equipos de la infraestructura que soportan IPv6, los que requieran actualización y los que no soporten IPv6.
- Definir el proceso de transición de los distintos servicios tecnológicos.
- Revisar las políticas de enrutamiento IPv6 dentro de los segmentos de red definidos en el alcance.
- Definir las pruebas para la validación del funcionamiento de los aplicativos, equipos y servicios comprendidos en el Alcance.

El entregable de esta fase comprende el presente plan.

Los responsables son los siguientes:

- Oficina General de Apoyo a la Gestión Institucional.
- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.
- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

Fase 2: Definición y Diseño

El objetivo de la presente fase es realizar una revisión de la red, definir un nuevo esquema de red para el funcionamiento de IPv6 y elaborar diagramas acordes al Alcance definido.

Forman parte de esta fase:

- Visualizar la topología actual de red del Ministerio.
- En base al alcance proponer un nuevo diseño.
- Actualizar el diagrama de red.

Los responsables son los siguientes:

- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.
- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

Fase 3: Migración de Servicios orientados a Internet

El objetivo de la presente fase es mantener la funcionalidad completa del protocolo IPv4 mientras se estable la presencia del protocolo IPv6 en base al alcance definido; serán considerados aspectos de funcionalidad y seguridad de los equipos perimetrales, los servidores que prestan servicios expuestos a Internet, los ruteadores y el equipamiento de la zona desmilitarizada que permite brindar los servicios expuestos a Internet.

Forman parte de esta fase:

- Evaluación del equipamiento actual y su funcionamiento sobre IPv6.
- Configuraciones de IPv6.
- Seguridad de equipamiento IPv6
- Pruebas de funcionamiento IPv6
- Mejoramiento de configuraciones y aseguramiento de la infraestructura en base a las pruebas de funcionamiento.

Los responsables son los siguientes:

- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.

- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

Fase 4: Migración de aplicación

El objetivo es determinar el total de módulos dentro de los sistemas de información que forman parte de la plataforma de sistemas de información del Ministerio y que tienen características de estar expuestos hacia internet, que requieran de cambios que aseguren su correcto funcionamiento en ambientes de producción de solo IPv6.

Entregables

- Documentación del Proceso de Migración
- Documentación de los Sistemas de Información Migrados o reemplazados
- Documentación de los elementos de las aplicaciones que han requerido cambios y en que han consistido los cambios realizados.

Los responsables son los siguientes:

- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.
- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

VIII. Realización de Pruebas

Al momento de realizar las pruebas de funcionalidad deben cubrirse las siguientes actividades:

- Realizar las pruebas y el monitoreo de la funcionalidad del protocolo IPv6 en los sistemas de información comprendidos en el alcance, los sistemas de comunicaciones y los distintos servicios, en ambientes que permitan la generación de tráfico IPv6 desde el Ministerio hacia Internet y viceversa.
- Realizar las pruebas de funcionalidad del protocolo IPv6 acorde a las políticas de seguridad perimetral, de los servidores y equipos de comunicaciones, manteniendo un registro de las pruebas realizadas.
- Al realizar las pruebas de funcionalidad es posible ejecutar acciones de afinamiento de las configuraciones de hardware y software con la información que se obtenga de la implementación.
- Finalmente se debe realizar un nuevo inventario de los servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento del protocolo IPv6.

El período de prueba estará comprendido dentro del plazo establecido en el Artículo 5° dada en el D.S. N.° 081-2017-PCM.

8.1. Pruebas de migración de servicios orientados a Internet

Objetivo

Ejecución de pruebas de migración de los servicios orientados a Internet, monitoreo de la funcionabilidad de IPv6 y registros de las pruebas de funcionalidad de cada equipo.

Entregables

0450

Documentación y registro de los casos de prueba ejecutados (antes y después de los cambios realizados).

Responsables y Áreas involucradas

- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.
- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

8.2. Pruebas de Migración de las aplicaciones

Objetivo

Ejecución de pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento y servicios web de la entidad.

Entregables

Documentación de los casos de prueba ejecutados (antes y después de los cambios realizados)

Responsables y Áreas involucradas

- Oficina de Tecnologías de la Información.
- Unidad de Redes e Infraestructura.
- Unidad de Desarrollo de Sistemas.
- Oficial de Seguridad de la Información.

IX. Capacitación y Sensibilización

La capacitación en IPv6 es fundamental, no sólo la parte técnica del protocolo IPv6 sino también la concientización y los beneficios de la transición.

La recomendación académica para la capacitación a brindar, puede tomar como referencia los siguientes módulos:

- Módulo 1: Introducción y aspectos básicos de IPv6.
- Módulo 2: Agotamiento de direcciones IPv4, transición a IPv6 y coexistencia.
- Módulo 3: IPv6 Operaciones.
- Módulo 4: IPv6 Servicios.
- Módulo 5: IPv6 Habilitando protocolos de enrutamiento.
- Módulo 6: IPv6 Multicast Services.
- Módulo 7: IPv6 Mecanismos de Transición.
- Módulo 8: IPv6 Seguridad
- Módulo 9: Implementación de IPv6
- Módulo 10: IPv6 y Proveedores de Servicio

Se recomienda que la capacitación esté dirigida a los colaboradores de la Oficina de Tecnologías de la Información del Ministerio con especial énfasis a colaboradores de la Unidad de Redes e Infraestructura y la Unidad de Desarrollo de Sistemas; asimismo es recomendable también la participación de los Especialistas de Seguridad de la Información. Los participantes deben adquirir los conocimientos que describan la funcionalidad, aplicabilidad y todos los componentes técnicos del nuevo protocolo IPv6 a través de prácticas y procedimientos de configuración en laboratorios. Los cursos de preferencia deben ser presenciales de mínimo 32 horas en los cuales puedan desarrollarse los Módulos indicados.

Es importante sensibilizar a la Alta Dirección sobre la importancia de implementar IPv6, el impacto que tendrá dentro de la infraestructura de tecnologías de la información del Ministerio y como la implementación afectará las operaciones del Ministerio.

Algunas recomendaciones para el proceso de capacitación:

- Capacitar al personal de tecnologías de la información que se designe, de modo que dispongan de un nivel adecuado sobre el protocolo IPv6.
- La capacitación no debe describir solamente el componente técnico, sino la forma como se debe orientar la transición de IPv4 a IPv6.
- La capacitación debe incluir todo el material necesario, los temarios de cada Módulo, las guías de laboratorio, con el propósito de aclarar suficientemente los aspectos técnicos teóricos y prácticos sobre IPv6.

X. Presupuesto Estimado

Con la finalidad de realizar la migración establecida en el alcance, la Oficina de Tecnologías de la Información estima los siguientes servicios al año 2020, los mismos que en lo posible se gestionarán según la disponibilidad presupuestal prevista para la programación multianual 2020 al 2022. Adicionalmente considerar que, a raíz de los entregables del servicio de diseño en la arquitectura, podrían surgir equipamientos e insumos no contemplados en el presente presupuesto.

No	Equipamiento/Servicio	Tipo	Precio	Cantidad	Subtotal
1	Servicio de Internet IPv6 para ejecución de pruebas y test	Servicio	48,000.00	1	48,000.00
2	Servicio de Diseño de la Arquitectura de Red IPv6	Servicio	40,000.00	1	40,000.00
3	Servicio de capacitación en IPv6 integral personal técnico del MRE	Servicio	32,000.00	1	32,000.00
4	Servicio de soporte técnico para la migración de los servicios publicados a IPv6	Servicio	60,000.00	1	60,000.00
				Total	180,000.00

Leyenda:
Tipo: Servicios | Hardware | Licencias | (...)
Precio: Monto del Servicios | Hardware | Licencias | (...) expresados en (Soles)
Cantidad: Cantidad de equipos licencias que se planea adquirir | Costo estimados que puede conllevar la prestación del servicio.
Subtotal: Precio * Cantidad
Total = Sumatoria de los subtotales

Tabla 12: Presupuesto estimado

XI. Anexos

1. ANEXO: Cronograma de diagnóstico de la infraestructura

Ítem	Responsable	Actividad	Producto	Fecha inicio	Duración	Fecha fin
1	Unidad de Redes e Infraestructura - OTI	Inventario	Inventario de comunicaciones	3/09/2018	30	2/10/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de video conferencia	3/09/2018	30	2/10/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servidores - hardware	01/11/2018	30	30/11/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servidores - hypervisores	01/11/2018	30	30/11/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servidores - sistema operativos físicos y virtuales	01/11/2018	30	30/11/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servicios - Internet	3/09/2018	88	29/11/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servicios - Dominio	01/10/2018	10	10/10/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servicios - Correo electrónico	01/10/2018	10	10/10/2018
	Unidad de Redes e Infraestructura - OTI		Inventario de servicios - Hosting	10/10/2018	11	20/10/2018
	Unidad de Desarrollo de Sistemas - OTI		Inventario de aplicaciones	03/12/2018	28	30/12/2018
	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas - OTI		Entregable de Inventario	31/01/2018	6	05/01/2019
2	Unidad de Redes e Infraestructura - OTI	Diagnostico	Diagnóstico de comunicaciones	18/12/2018	90	17/03/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de video conferencia	30/11/2018	90	27/02/2019

	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servidores - hardware	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servidores - hypervisores	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servidores - sistema operativos físicos y virtuales	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servicios - Internet	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servicios - Dominio	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servicios - Correo electrónico	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de servicios - Hosting	30/11/2018	90	27/02/2019
	Unidad de Redes e Infraestructura - OTI		Diagnóstico de aplicaciones	14/01/2019	38	20/02/2019
	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas - OTI		Entregable de diagnostico	20/02/2019	10	1/03/2019
3	Unidad de Redes e Infraestructura - OTI	Evaluación de Riesgo	Medición de Riesgo - Infraestructura Tecnológica	1/03/2019	60	29/04/2019
	Unidad de Redes e Infraestructura - OTI		Medición de Riesgo - Servicios	1/03/2019	60	29/04/2019
	Unidad de Desarrollo de Sistemas - OTI		Medición de Riesgo - Aplicaciones	1/03/2019	26	29/04/2019
	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas - OTI		Entregable de Medición de Riesgo	30/04/2019	15	14/05/2019

0450

2. ANEXO: Cronograma de implementación del protocolo IPv6

Item	Responsable	Actividad	Fecha Inicio	Duración	Fecha Fin
1	Oficial de Seguridad de la Información - OTI	Formulación de política de seguridad	15/05/2019	35	18/06/2019
2	Unidad de Redes e Infraestructura – OTI / Oficial de Seguridad - OTI	Definición y diseño	19/06/2019	60	17/08/2019
3	Unidad de Redes e Infraestructura – OTI	Migración de Servicios orientados a Internet	19/08/2019	180	14/02/2020
		Contratación del servicio de internet vía IPV6 para servicios publicados	19/08/2019	180	14/02/2020
		Adquisición de equipamiento requerido para soporte IPV6	19/08/2019	180	14/02/2020
4	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas - OTI	Migración de las aplicaciones	08/04/2019	54	31/05/2019
		Adquisición de equipamiento o servicio requerido para soporte IPV6 de aplicaciones	3/06/2019	180	29/11/2019
5	Jefatura OTI	Formulación de nuevo de alcance para el Plan	01/05/2020	87	26/07/2020
		Nuevo Plan aprobado	27/07/2020	13	08/08/2020

3. ANEXO: Cronograma para la realización de pruebas

Item	Responsable	Actividad	Fecha Inicio	Duración	Fecha Fin
1	Unidad de Redes e Infraestructura – OTI	Pruebas: Migración de servicios orientados a Internet Optimización	19/08/2019	180	14/02/2020
2	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas - OTI	Pruebas: Migración de las aplicaciones Optimización	03/06/2019	26	28/06/2019

0450

4. ANEXO: Cronograma de capacitación y sensibilización

	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
1	Unidad de Redes e Infraestructura – OTI / Unidad de Desarrollo de Sistemas / Oficial de Seguridad - OTI	Capacitación: Personal Técnico	3/09/2018	360	28/08/2019
2	Unidad de Redes e Infraestructura – OTI / Oficial de Seguridad – OTI / Jefatura de la OTI	Capacitación: Usuario Final	19/08/2019	60	17/10/2019

0450