REPUBLICA DEL PERU

Resolución Jefatural

N° 115 -2018-ACFFAA Lima, 08 AGO. 2018

VISTOS:

El Informe Técnico N° 000016-2018 de la Oficina de Informática y el Informe Legal N° 000133-2018/OAJ/ACFFAA de la Oficina de Asesoría Jurídica de la Agencia de Compras de las Fuerzas Armadas.

CONSIDERANDO:

Que, mediante Decreto Legislativo Nº 1128, se crea la Agencia de Compras de las Fuerzas Armadas, como organismo público ejecutor adscrito al Ministerio de Defensa, encargada de planificar, organizar y ejecutar los procesos de contrataciones de bienes, servicios, obras y consultorías a su cargo, en el mercado nacional y extranjero;

Que, el literal e) del artículo 9 del Decreto Supremo N° 004-2014-DE, que aprueba el Reglamento de Organización y Funciones de la Agencia de Compras de las Fuerzas Armadas, establece como función de la Secretaría General la de: *"Administrar los sistemas de telecomunicaciones, informáticos y estadística de la Agencia";*

Que, mediante Decreto Supremo N° 066-2011-PCM, se aprobó el Plan de Desarrollo de la Sociedad de la Información en el Perú, el cual establece como uno de sus objetivos el de: *"Asegurar el acceso inclusivo y participativo de la población de áreas urbanas y rurales a la Sociedad de la Información y de conocimiento"*, el cual contiene como una de sus estrategias la de: *"Proponer e implementar servicios públicos gubernamentales que utilicen soluciones de comunicación innovadoras soportadas por el Protocolo de Internet v6 (IPv6)";*

Que, mediante Decreto Supremo N° 081-2013-PCM, se aprobó la Política Nacional de Gobierno Electrónico 2013-2017, estableciendo como Lineamientos Estratégicos, entre otros, a la Tecnología e Innovación la cual indica que: *"Se debe promover el crecimiento de la Tecnología e Innovación a través de la provisión de*

una infraestructura adecuada a través del desarrollo de plataformas que permitan llevar a cabo innovaciones (...)"; así como también a la Infraestructura, la cual indica que: *"El requisito fundamental para la comunicación efectiva y la colaboración dentro del Estado es contar con una red informática y de telecomunicaciones que integre a todas las dependencias y a sus funcionarios públicos, incluyendo hardware, software, sistemas, redes, conectividad a la Internet, bases de datos, infraestructura para capacitación en línea (e-Learning) y recursos humanos especializados (...)*;

Que, mediante Decreto Supremo N° 081-2017-PCM, se dispuso 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;

Que, a partir de la vigencia del Decreto Supremo señalado en el párrafo anterior, se cuenta con un plazo máximo de un (01) año, para la elaboración y aprobación del Plan de Transición al Protocolo IPv6; asimismo establece que dicho Plan deberá ser aprobado por el Titular de la Entidad; por lo que una vez aprobado deberá ser comunicado a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros. Finalmente, dispone que el referido Plan deberá implementarse progresivamente en un plazo máximo de cuatro (04) años luego de su aprobación;

Que, mediante Informe Técnico N° 000016-2018/OI/ACFFAA, la Oficina de Informática, remitió el Plan de Transición al Protocolo IPv6 de la Agencia de Compras de las Fuerzas Armadas, para su aprobación correspondiente;

Que, mediante Informe Legal N° 000133-2018/OAJ/ACFFAA, la Oficina de Asesoría Jurídica, dentro del ámbito de su competencia, emite opinión favorable respecto a la aprobación del Plan de Transición al Protocolo IPv6, de acuerdo a lo recomendado por la Oficina de Informática;

Estando a lo solicitado por la Oficina de Informática, con el visado de la Secretaría General y de la Oficina de Asesoría Jurídica de la Agencia de Compras de las Fuerzas Armadas;

De conformidad con lo dispuesto en el Decreto Legislativo Nº 1128, el Decreto Supremo N° 066-2011-PCM, el Decreto Supremo N° 081-2013-PCM, el Decreto Supremo N° 004-2014-DE y el Decreto Supremo N° 081-2017-PCM.

SE RESUELVE:

Artículo 1.- Aprobar el Plan de Transición al Protocolo IPv6 de la Agencia de Compras de las Fuerzas Armadas, la misma que como Anexo forma parte integrante de la presente Resolución.

Artículo 2.- Disponer que la Secretaria General notifique por escrito la presente Resolución a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia de Consejo de Ministros.

Artículo 3.- Disponer la publicación de la presente Resolución y su Anexo en el Portal Institucional de la Agencia de Compras de las Fuerzas Armadas (www.acffaa.gob.pe).

Regístrese, comuníquese y publíquese.

AGENCIA DE COMPRAS DE LAS FFAA - JEFATURA - REPUBLICA DEL PERU

Roy Marvin Carbajal Tarazona
Jefe de la Agencia de Compras de las Fuerzas Armadas

AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS

Comprando para la Seguridad y Defensa Nacional

Plan de Transición al Protocolo IPv6

OFICINA DE INFORMÁTICA

2018

AGENCIA DE COMPRAS FFAA V°B° Secretario General

ÍNDICE

AGENCIA DE COMPRAS FFAA V°B° Secretario General

V°B°

V°B°

I. Introducción

El Decreto Supremo que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública, DS Nº 081-2017-PCM, indica que "LACNIC señala que el agotamiento de las direcciones IPv4 en América Latina y el Caribe se encuentra en su tercera y última fase, debiendo los gobiernos priorizar el despliegue del protocolo IPv6, quienes deben asegurar que las acciones que se lleven a cabo garanticen que los nuevos recursos TIC cuenten con capacidad IPv6, tomando en consideración un periodo de transición necesario para pasar del IPv4 al IPv6, ello conforme con lo dispuesto en la Resolución Nº 180 correspondiente a la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones", por ese y otros motivos, el misionado D. S. dispone la elaboración de un "Plan de Transición al Protocolo IPv6" el que debe implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública.

Para la elaboración del Plan de Transición al Protocolo IPv6, la Agencia de Compras de las Fuerzas Armadas (ACFFAA) ha evaluado el Diagnóstico Preliminar de la Infraestructura Tecnológica, la complejidad de la infraestructura física, la complejidad las aplicaciones utilizadas, los plazos de implementación que determina el DS Nº 081-2017-PCM y las posibles estrategias o mecanismos a adoptar para la implementación del Protocolo IPv6. Como resultado dicha evaluación se ha elaborado el presente "Plan de Transición al Protocolo IPv6", el mismo que servirá como instrumento de gestión para la implementación del protocolo IPv6 en la ACFFAA.

La ejecución del Plan de Transición al Protocolo IPv6 en la ACFFAA estará a cargo de la Oficina de Informática, quienes deberán coordinar con las demás áreas orgánicas de la Entidad y con los proveedores a fin de llevar a cabo el plan de manera satisfactoria.

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 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 Nº 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.

AGENCIA DE COMPRAS FFAA V°B° Secretario General

III. Objetivos del Plan de Transición

- Definir las actividades que permitan, de manera progresiva, adaptar nuestra infraestructura, plataforma y servicios públicos digitales[1] al Protocolo IPv6
- Identificar la situación actual de nuestra infraestructura, plataformas y servicios públicos digitales en relación a su compatibilidad con el protocolo IPv6.

IV. Alcance del Plan de Transición

El presente plan de transición contempla como alcance toda la infraestructura, plataforma y servicios públicos digitales que estén bajo dominio de la Agencia de Compras de las Fuerzas Armadas al protocolo IPv6.

V. Riesgos de no adopción del Protocolo IPv6

5.1. Riesgos Identificados

Riegos identificados previo a la implementación del Plan, los riesgos son valorados en función del impacto que podrían generar al logro de los objetivos de la entidad y su probabilidad de ocurrencia.

N°	Riesgo	Impacto	Probabilidad	Valoración		
				Alto	Medio	Bajo
1	Incompatibilidad de hardware	Alto	Medio	X		
2	Inestabilidad de las aplicaciones	Alto	Baja		X	
3	Problemas de funcionamiento del S.O	Medio	Medio		X	
4	Falta de compatibilidad ipv6 en los proveedores que brindan el servicio de Internet	Alto	Bajo		X	
5	Cortes de energía eléctrica inesperados no superados	Medio	Bajo		X	
6	Incompatibilidad de aplicaciones con el S.O.	Medio	Bajo		X	
7	Inestabilidad de la Base de Datos	Alto	Medio	X		
8	Falta de experiencia en el personal que realizará la implementación	Alto	Medio	X		
9	Perdida de información	Alto	Bajo	X		
10	Ocurra daño físico en los equipos durante la implementación	Medio	Bajo		X	
11	No disponibilidad de repuestos	Medio	Bajo			X

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

[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: http://www.peru.gob.pe/normas/docs/DS_033_2018_PCM_GobPE_y_disposiciones_adicionales_SEGDI.pdf

VI. Diagnóstico de la Infraestructura Tecnológica

6.1. Hardware

6.1.1 Equipamiento de Comunicaciones:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Firewall UTM Fortigate 200E	X	X	Alto
2	Switches Core - Administrable - Cisco Nexus 3048	X	X	Alto
3	Switches Distribución - Administrable - Cisco C3650	X	X	Bajo
4	Switches Acceso - Administrable - Cisco C2960X	X	X	Bajo
5	Wireless LAN Controller Cisco 2500 Series	X	X	Bajo

Leyenda:
Descripción: Indique el Equipo de Comunicaciones comprendida en el alcance definido: Access Point | Switch administrable | Switch no administrable
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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° 01: Equipamiento de comunicaciones

6.1.2 Equipamiento de Telefonía:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Router Cisco 2901	X	X	Alto
2	Central Telefónica Cisco Unified Call Manager	X	X	Alto
3	Cisco Unity Connection	X	X	Medio
4	Cisco Call Manager IM and Presence	X	X	Medio
5	Teléfonos Cisco 8940 8945	X		Alto
6	Yealink T21P E2	X	X	Alto

Leyenda:
Descripción: Indique el Equipo de Telefonía comprendida en el alcance definido: Anexos YeaLink T19 | Anexos YeaLink T21 | Anexos YeaLink T46
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
Riesgo: Se refiere al riesgo que emerge al no tener el Equipo de Telefonía soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 02: Equipamiento de Telefonía

AGENCIA DE COMPRAS FFAA V°B° Secretario General

6.1.3 Equipamiento de Video Conferencia

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	NO DISPONE			
2	NO DISPONE			
...				

Leyenda:
Descripción: Indique el Equipo de Video Conferencia comprendida en el alcance definido: Sistema de Video YEALINK VC120 | Sistema de Audio YEALINK VC40
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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

6.1.4 Equipamiento de Servidores – Físicos:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	02 SERVIDORES CISCO UCS C220 M3S	X	X	ALTO
2	01 SERVIDOR CISCO UCS C220 M3SBE	X	X	ALTO
3	01 SERVIDOR HP DL 360P	X	X	ALTO
4	01 SERVIDOR IBM X3250 M4	X	X	ALTO
...				

Leyenda:
Descripción: Indique el Equipamiento de Servidores – Físicos comprendida en el alcance definido: Servidor dedicado Dell Poweredge R730 | PC Propia Dell Optiplex 7040 | PC Alquilada Compatible
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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

6.1.5 Equipamiento de Servidores – Hypervisores:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	04 SERVIDORES VMWARE VSPHERE 6.5	X	X	ALTO
2	01 SERVIDOR VMWARE VSPHERE 5.1	X	X	BAJO
...				

Leyenda:
Descripción: Indique el Equipamiento de Servidores – Hypervisores comprendida en el alcance definido: Servidor VMWARE - EXSI 6.0 | ...
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6

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

6.1.6 Equipamiento de Servidores – Sistema Operativo:

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	10 SERVIDORES	LINUX	X	X	ALTO
2	2 SERVIDORES	Windows Server 2016	X	X	ALTO
3	6 SERVIDORES	Windows Server 2012 R2	X	X	ALTO
...					

Leyenda:
Descripción: Indique el Equipamiento de Servidores – Sistema Operativo comprendida en el alcance definido: Virtual SIAF | Virtual SIGA | Virtual Intranet | Virtual Antivirus
Sistema Operativo: Windows Server 2012 |
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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

6.1.7 Equipamiento de Usuarios – Sistema Operativo:

N°	Descripción	Sistema Operativo	Soporte IPv4	Soporte IPv6	Riesgo
1	110 PCS	WINDOWS 7	X	X	ALTO
2	10 LAPTOPS	WINDOWS 7	X	X	ALTO
...					

Leyenda:
Descripción: Indique el Equipamiento de Usuarios – Sistema Operativo comprendida en el alcance definido: PC Propia ("Cantidad") | PC Alquiladas ("Cantidad") | Laptop propias ("Cantidad") | Laptop alquiladas ("Cantidad")
Sistema Operativo: Windows 10 | Windows 8.1
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Usuarios – Sistema Operativo soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 07: Equipamiento de usuarios PC

AGENCIA DE COMPRAS FFAA VºBº Secretario General

6.1.8 Equipamiento de Cámaras CCTV:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	NO CONTEMPALDO EN EL ALCANCE			
2				
...				

Leyenda:
Descripción: Indique el Equipamiento de Cámaras CCTV comprendida en el alcance definido: Cámara Tipo 1 | Cámara Tipo 2 ....
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Cámaras CCTV soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 08: equipamiento de CCTV

6.1.9 Equipamiento de Control de Asistencia:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	NO CONTEMPLADO EN EL ALCANCE			
2				
...				

Leyenda:
Descripción: Indique el Equipamiento de Control de Asistencia comprendida en el alcance definido: Biostation ...
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
Riesgo: Se refiere al riesgo que emerge al no tener el Equipamiento de Control de Asistencia soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 09: equipamiento de CCTV

6.2. Servicios

6.2.1. Servicio de Internet

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	OPTICALS NETWORK ENLACE 1:1 40 Mbps	X	X	ALTO
2	ROUTER WAN CISCO 2960	X	X	ALTO
...				

Leyenda:
Descripción: Indique breve descripción sobre el Servicio de Internet comprendida en el alcance definido: Detalle Ancho de banda contratado y proveedor. Por Ejemplo: Servicio de Internet 40 Mbps – **[Proveedor]**
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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° 10: Servicio de internet

6.2.2. Servicio de Central de Telefonía Virtual:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	Central Telefónica Cisco Unified Call Manager	X	X	Alto
2	Cisco Unity Connection	X	X	Medio
3	Cisco Call Manager IM and Presence	X	X	Medio

Leyenda:
Descripción: Indique breve descripción sobre el Servicio de Central de Telefonía Virtual comprendida en el alcance definido. Por Ejemplo: Servicio de Central Telefónica Virtual
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
Riesgo: Se refiere al riesgo que emerge al no tener el Servicio de Central de Telefonía Virtual soportado con el protocolo IPv6. El riesgo puede clasificarse en: Alto | Medio | Bajo

Tabla N° 11: Servicio de telefonía fija

6.2.3. Servicio de alojamiento de dominio:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	DOMINIO ACFFAA.GOB.PE RED CIENTIFICA	X	X	ALTO
2				
...				

Leyenda:
Descripción: Indique breve descripción sobre el Servicio de alojamiento de dominio comprendido en el alcance definido. Por Ejemplo: Servicio de dominio [Nombre de la entidad].gob.pe – punto.pe
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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° 12: Servicio de dominio

6.2.4. Servicio de correo electrónico:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	NO CONTEMPLADO EN EL ALCANCE			
2				
...				

Leyenda:
Descripción: Indique breve descripción sobre el Servicio de correo electrónico comprendida en el alcance definido: Por Ejemplo: Servicio de correo electrónico office365
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4

AGENCIA DE COMPRAS FFAA V°B° Secretario General

Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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° 13: Servicio de correo electrónico

6.2.5. Servicio de hosting [Nube]:

N°	Descripción	Soporte IPv4	Soporte IPv6	Riesgo
1	NO DISPONE			
2				
...				

Leyenda:
Descripción: Indique breve descripción sobre el Servicio de hosting [Nube] comprendido en el alcance definido. Por Ejemplo: Servicio de hosting –www.[servicio].peru.gob.pe | www.[entidad].peru.gob.pe
Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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 N° 14: Servicio de hosting [Nube]

6.2.6. Otros comprendidos en el alcance

6.3. Aplicaciones

	Descripción	Componentes Servidores	Soporte IPv4	Soporte IPv6	Riesgo
1	SERVICIO DNS MS WINDOWS SERVER 2016		X	X	ALTO
2	SERVICIO DHCP MS WINDOWS SERVER 2016		X	X	ALTO
...					

Leyenda:
Descripción: Indique breve descripción sobre las Aplicaciones comprendidas en el alcance definido. Por Ejemplo: Aplicación X – Desarrollo | Directorio Activo | SIAF | SIGA | Tramite Documentario | Intranet | File Server | Antivirus |

Soporte IPv4: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV4
Soporte IPv6: Marcar con un "X" si el hardware tiene soporte al Protocolo IPV6
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 15: Aplicaciones

VII. Implementación del Protocolo IPv6

La implementación se realizará por fases, las mismas que se describen a continuación:

Fase 1: Diagnóstico de la Infraestructura relacionada con la Transición al Protocolo IPV6

El objetivo de esta fase es contar con toda la información necesaria para evaluar los requisitos técnicos de la infraestructura determinando aquellos que tengan soporte necesario para adoptar el IPv6 y aquéllos a los que no tengan dicho soporte. Para los equipos críticos se podría considerar una estimación de presupuesto necesario para su renovación.

Entregables:

1. Inventario y diagnóstico de la infraestructura informatica involucrada en el la implementación del Ipv6. Se debe contar con el inventario actualizado de todos los equipos presentes en la red (routers, switches, firewalls, servidores, teléfonos, impresoras, etc.), identificando información importante para la incorporación del IPv6, como: fabricante del equipo, modelo, versiones de software, cantidad de memoria, licencias asociadas, módulos de hardware de expansión, sistemas operativos utilizados tanto en servidores como en las computadoras personales, hardware y/o software asociado a servicios básicos: HTTP(S), DNS, FTP, SSH, DHCP, hardware y/o software asociado a servicios específicos de la red, incluyendo bases de datos y aplicaciones internas de la institución.

2. Identificar la topología actual de la red y su funcionamiento dentro de la Entidad.

3. Evaluación de Riesgo
   Evaluar el grado de compatibilidad del protocolo IPv6 a nivel de hardware y software para preparar la nueva infraestructura de red de la entidad

Fase 2: Definición y Diseño

El objetivo de esta fase es determinar el diseño de la nueva arquitectura de red que soporte el IPv6 y la estrategia para su adopción, es decir, los mecanismos de transición para su adopción.

Entregables:

1. Revisión de la red
2. Definición del diseño de la red
3. Definición de los mecanismo de adopción del IPv6

Fase 3: Migración de Servicios y Aplicaciones

Fase 3.1: Migración de Servicios orientados a Internet

Esta fase debe considerar las acciones necesarias para mantener la funcionalidad completa de IPv4, mientras se establece una presencia de Internet IPv6.

Es importante considerar:

1. Aspectos de seguridad en los equipos firewalls, servidores Web, enrutador del proveedor de servicio de Internet y zona desmilitarizada,
2. Coordinaciones con el proveedor del servicio Internet

3. Considerar los tiempos de contratación y/o adquisición de equipamiento necesario.

Fase 3.2: Migración del acceso a internet desde usuarios internos mediante IPv6

El objetivo de esta fase es identificar y ejecutar todas las actividades necesarias para permitir que usuarios internos accedan a Internet IPv6. Se considerar:

1. Los mecanismos de TUNELAJE o SERVIDORES PROXY dado que pueden proveer la manera de que usuarios IPv4 en la red privada accedan el Internet con IPv6,
2. Los tiempos de contratación y/o adquisición de equipamiento necesario.

Fase 3.3: Migración de aplicación

El objetivo de fase es identificar y ejecutar las acciones necesarias para que todas las herramientas de aplicación interna y administración de red sean migradas a un ambiente de solo IPv6, se debe considerar los tiempos de contratación y/o adquisición de equipamiento necesario.

Fase 3.4: Migración completa a IPv6

El objetivo de fase es identificar y ejecutar las acciones necesarias para asegurar que IPv6 exista de extremo-a-extremo. Se debe considerar:

1. La necesidad de accesibilidad a puntos extremos de Internet de IPv4 que aún puedan existir,
2. Los tiempos de contratación y/o adquisición de equipamiento necesario.

VIII. Realización de Pruebas

El objetivo de esta fase es realizar las actividades que nos permitirán realizar las pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento, Sistemas de Comunicaciones y servicios de la entidad para validar su correcto funcionamiento.

Se debe considerar las siguientes pruebas:

8.1. Pruebas de migración de servicios orientados a Internet
8.2. Pruebas de migración al acceso a internet desde usuarios internos mediante IPv6
8.3. Pruebas de Migración de las aplicaciones
8.4. Pruebas de Migración completa a IPv6

IX. Capacitación y Sensibilización

Capacitación se realizará al personal técnico de la ACFFAA para generar las habilidades técnicas necesarias para la nueva red de datos que soporte el IPV6.

La capacitación debe ser coordinada con la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, parta que sea la SEGDI la que brinde la asistencia técnica y la capacitación, la misma que consideraría los siguientes módulos:

- Módulo 1: Introducción to IPv6
- Módulo 2: IPv6 Operaciones
- Módulo 3: IPv6 Servicios
- Módulo 4: IPv6-Enabled Routing Protocols

- Módulo 5: IPv6 Multicast Services
- Módulo 6: IPv6 Mecanismos de Transición
- Módulo 7: IPv6 Seguridad
- Módulo 8: Implementación de IPv6
- Módulo 9: IPv6 and Proveedores de Servicio

X. Presupuesto Estimado

Para el presente año, no se realizará ningún gasto en la ejecución del Plan de Transición al Protocolo IPV6 en la ACFFAA, pues se realizará con recursos propios. Asimismo, de acuerdo al análisis del Diagnóstico Preliminar de la Infraestructura Tecnológica, se estima que no se requiere actualizar o reemplazar los equipos considerados críticos para la implementación del IPv6 en la ACFFAA. Sin embargo, en la ejecución de la Fase 2 del Plan se determinará con precisión el presupuesto en el caso de requerir algún cambio de equipo o aplicación.

XI. Anexo

AGENCIA DE COMPRAS FFAA V°B° Secretario General

ANEXO: Cronograma de actividades del Plan de Transición al Protocolo IPV6

Item	Actividad	Responsable	Días	Inicio	fin
1.1	**Diagnóstico de la Infraestructura relacionada con la Transición al Protocolo IPV6**	**Oficina de Informática**	**130 días**	**mar 2/10/2018**	**lun 1/04/2019**
1.1.1	Inventario	Oficina de Informática	65 días	mar 2/10/2018	lun 31/12/2018
1.1.2	Diagnostico	Oficina de Informática	44 días	lun 3/12/2018	jue 31/01/2019
1.1.3	Diagramas de topología actual de la Red	Oficina de Informática	65 días	mar 2/10/2018	lun 31/12/2018
1.1.4	Evaluación de Riesgo	Oficina de Informática	42 días	vie 1/02/2019	lun 1/04/2019
1.1.4.1	Medición de Riesgo - Infraestructura Tecnológica	Oficina de Informática	42 días	vie 1/02/2019	lun 1/04/2019
1.1.4.2	Medición de Riesgo - Servicios	Oficina de Informática	42 días	vie 1/02/2019	lun 1/04/2019
1.1.4.3	Medición de Riesgo - Aplicaciones	Oficina de Informática	42 días	vie 1/02/2019	lun 1/04/2019
1.1.4.4	Entregable de Medición de Riesgo	Oficina de Informática	42 días	vie 1/02/2019	lun 1/04/2019
1.2	**Definición y Diseño**	**Oficina de Informática**	**64 días**	**mar 2/04/2019**	**vie 28/06/2019**
1.2.1	Revisión de la red	Oficina de Informática	64 días	mar 2/04/2019	vie 28/06/2019
1.2.2	Definición del diseño de la red	Oficina de Informática	64 días	mar 2/04/2019	vie 28/06/2019
1.2.3	Definición de los mecanismo de adopción del IPv6	Oficina de Informática	64 días	mar 2/04/2019	vie 28/06/2019
1.3	**Migración a IPv6**	**Oficina de Informática**	**175 días**	**mié 1/05/2019**	**mar 31/12/2019**
1.3.1	Migración de Servicios orientados a Internet	Oficina de Informática	27 días	jue 25/07/2019	vie 30/08/2019
1.3.2	Contratación del servicio de internet vía IPV6 para servicios publicados	Oficina de Informática	58 días	mié 1/05/2019	vie 19/07/2019
1.3.3	Migración del acceso a internet desde usuarios internos mediante IPv6	Oficina de Informática	21 días	lun 2/09/2019	lun 30/09/2019
1.3.4	Migración de las aplicaciones	Oficina de Informática	65 días	lun 2/09/2019	vie 29/11/2019
1.3.5	Migración completa a IPv6	Oficina de Informática	22 días	lun 2/12/2019	mar 31/12/2019
1.4	**Ejecución de Pruebas**	**Oficina de Informática**	**114 días**	**jue 25/07/2019**	**mar 31/12/2019**

AGENCIA DE COMPRAS FFAA V°B° Secretario General

Item	Actividad	Responsable	Días	Inicio	fin
1.4.1	Pruebas: Migración de servicios orientados a Internet	Oficina de Informática	42 días	jue 25/07/2019	vie 20/09/2019
1.4.2	Optimización	Oficina de Informática	72 días	lun 23/09/2019	mar 31/12/2019
1.4.3	Pruebas. Migración del acceso a internet desde usuarios internos mediante IPv6	Oficina de Informática	35 días	lun 2/09/2019	vie 18/10/2019
1.4.4	Optimización	Oficina de Informática	52 días	lun 21/10/2019	mar 31/12/2019
1.4.5	Pruebas: Migración de las aplicaciones	Oficina de Informática	60 días	lun 2/09/2019	vie 22/11/2019
1.4.6	Optimización	Oficina de Informática	27 días	lun 25/11/2019	mar 31/12/2019
1.4.7	Pruebas: Migración completa a IPv6	Oficina de Informática	22 días	lun 2/12/2019	mar 31/12/2019
1.4.8	Optimización	Oficina de Informática	22 días	lun 2/12/2019	mar 31/12/2019
1.5	**Capacitación**	**Oficina de Informática**	**305 días**	**lun 1/10/2018**	**vie 29/11/2019**
1.5.1	Capacitación: Personal Técnico	Oficina de Informática	45 días	lun 1/10/2018	vie 31/11/2018
1.5.2	Capacitación: Usuario Final	Oficina de Informática	20 días	lun 4/11/2019	vie 29/11/2019

AGENCIA DE COMPRAS FFAA V°B° Secretario General