

**SUPERINTENDENCIA
NACIONAL DE
BIENES ESTATALES**



RESOLUCIÓN N° 062-2018/SBN

San Isidro, 09 de agosto de 2018

VISTO:

El Memorándum N° 373-2018/SBN-OAF-TI y el Memorándum N° 097-2018/SBN-OAF emitidos por la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información; el Informe Especial N° 00958-2018/SBN-OPP-SPBZ-KLS emitido por la Oficina de Planeamiento y Presupuesto; y el Informe N° 106-2018/SBN-OAJ emitido por la Oficina de Asesoría Jurídica, de fecha 08 de agosto de 2018; y,

CONSIDERANDO:

Que, mediante el Decreto Supremo N° 081-2017-PCM vigente desde el 10 de agosto de 2017, 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, el artículo 3 del Decreto Supremo N° 081-2017-PCM indica que las entidades de la Administración Pública deben elaborar un Plan de Transición al Protocolo IPv6, el cual será aprobado por el Titular de cada entidad. Asimismo, el artículo 5 señala que las entidades de la Administración Pública cuentan con un plazo máximo de un (01) año, contado a partir de la vigencia del Decreto Supremo, para la elaboración y aprobación de sus respectivos Planes de Transición, el mismo que una vez aprobado deberá ser comunicado a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros; así como, precisa que el Plan de Transición al Protocolo IPv6 debe implementarse progresivamente en un plazo máximo de cuatro (04) años luego de su aprobación;

Que, mediante Resolución N° 010-2018/SBN de fecha 26 de enero de 2018, se designó a el(la) Supervisor(a) de Tecnologías de la Información de la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información, como responsable de coordinar con la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros, para la adecuada implementación del protocolo IPv6 de la Superintendencia Nacional de Bienes Estatales, dentro de los alcances del Decreto Supremo N° 081-2017-PCM;

Que, mediante Memorándum N° 697-2018/SBN-OAF de fecha 08 de agosto de 2018, la Oficina de Administración y Finanzas eleva el Memorándum N° 373-2018/SBN-OAF-TI que contiene el proyecto del Plan de Transición al Protocolo IPv6 de la SBN para su aprobación por parte del Titular de la SBN;

Que, a través del Informe Especial N° 00958-2018/SBN-OPP-SPBZ-KLS, la Oficina de Planeamiento y Presupuesto precisa que el Plan de Transición al Protocolo IPv6 de la SBN, presentado por la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información, se ajusta al contenido mínimo establecido en el artículo 4 del Decreto Supremo N° 081-2017-PCM, el cual refleja la necesidad e importancia de su implementación para la continuidad de los procesos y servicios informáticos en la SBN adaptados a los cambios



tecnológicos del entorno; las actividades programadas para dicha implementación y para la realización de pruebas contribuirán al logro de la Acción Estratégica 04.02 "Sistema de información implementado para la operatividad institucional" del Objetivo N° 04 "Mejorar la gestión Institucional" del Plan Estratégico Institucional 2018-2020, Modificado", aprobado por la Resolución N° 028-2018/SBN de fecha 27 de marzo de 2018. Asimismo, se indica que se cuenta con el presupuesto estimado de S/. 64,000.00 (Sesenta y Cuatro Mil con 00/100 Soles) para desarrollar dicho Plan;

Que, mediante Informe N° 106-2018/SBN-OAJ de fecha 08 de agosto de 2018, la Oficina de Asesoría Jurídica opina favorablemente respecto al Plan de Transición al Protocolo IPv6 de la SBN, el cual se enmarca en lo establecido en el artículo 4 del Decreto Supremo N° 081-2017-PCM y se encuentra alineado al Objetivo Estratégico Institucional OEI.04 "Mejorar la gestión institucional" y contiene la Acción Estratégica Institucional AEI.04.02 "Sistema de información implementado para la operatividad institucional" contenida en el Plan Operativo de la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información;

Con el visto de la Gerencia General, las Oficinas de Administración y Finanzas, de Planeamiento y Presupuesto y de Asesoría Jurídica; y,

De conformidad con el Decreto Supremo N° 081-2017-PCM; las facultades previstas en el literal r) del artículo 11 del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales, aprobado por el Decreto Supremo N° 016-2010-VIVIENDA;

SE RESUELVE:

Artículo 1.- Aprobar el Plan de Transición al Protocolo IPv6 de la Superintendencia Nacional de Bienes Estatales-SBN, dentro de los alcances del Decreto Supremo N° 081-2017-PCM, el cual forma parte integrante de la presente Resolución.

Artículo 2.- El/la Supervisor (a) de Tecnologías de la Información de la Oficina de Administración y Finanzas debe comunicar a la Secretaría de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros la aprobación del Plan citado en el artículo 1 de la presente Resolución, de acuerdo a lo previsto en el artículo 5 del Decreto Supremo N° 081-2017-PCM; asimismo, es responsable de la ejecución de las actividades programadas en los plazos que se indican en los cronogramas que integran el Plan.

Artículo 3.- Notificar la presente Resolución a la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información para los fines pertinentes.

Artículo 4.- Encargar a la Oficina de Administración y Finanzas en el ámbito de Tecnologías de la Información la difusión de la presente resolución, en el Intranet de la SBN y en el portal institucional (www.sbn.gov.pe).

Regístrese y comuníquese.


ARMANDO MIGUEL SUBAUSTE BRACESCO
SUPERINTENDENTE
SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES

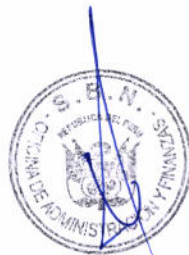


Plan de Transición al Protocolo IPv6

SBN

D.S. N° 081-2017-PCM

AGOSTO 2018



INDICE

I. INTRODUCCIÓN.....	3
II. BASE LEGAL.....	4
III. OBJETIVOS DE PLAN DE TRANSICIÓN.....	5
IV. ALCANCE DEL PLAN DE TRANSICIÓN.....	5
V. DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA.....	6
VI. IMPLEMENTACIÓN DEL PROTOCOLO IPV6.....	10
VII. REALIZACIÓN DE PRUEBAS.....	11
VIII. CAPACITACIÓN Y SENSIBILIZACIÓN.....	13
IX. PRESUPUESTO ESTIMADO.....	13
X. ANEXOS.....	14



I. INTRODUCCIÓN

LACNIC, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Su función es la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región.

El 15 de Febrero de 2017¹, LACNIC, informa que comenzó la Fase de Agotamiento de IPv4, cuando hablamos de agotamiento IPv4, nos referimos a que entramos en una etapa de reservas donde las asignaciones son restringidas en tamaño y periodicidad. Dichas restricciones fueron definidas por las políticas que se presentaron para discusión de la comunidad en el Foro Público de Políticas. Gracias a estas políticas se prevé una mejor administración de recursos para un agotamiento gradual de IPv4, así como también, permitir acceso a nuevos actores que quieran iniciar sus actividades de Internet en un futuro. Cuando decimos agotamiento, entonces nos referimos a que LACNIC no va a tener suficientes direcciones para cubrir las necesidades de direccionamiento IPv4 de nuestros miembros.

Ante el agotamiento de las direcciones IPv4, es necesario que las Empresas e Instituciones inicien el proceso de transición hacia el protocolo IPv6 de toda su infraestructura. Por este motivo se hace necesario que el Perú propicie un entorno que garantice la adopción del protocolo IPv6 por parte de la Administración Pública ante el inminente agotamiento de las direcciones IPv4, de tal manera que se asegure la comunicación y accesibilidad a dispositivos o servicios que utilizan el sistema de direccionamiento IPv6, 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.

IPv6 es el protocolo de Internet de última generación, diseñado para reemplazar al protocolo de Internet actual, IP versión 4. Para comunicarse a través de Internet, las computadoras y otros dispositivos deben tener direcciones de remitente y de destinatario.

¹ <http://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4>

El 9 de agosto de 2017, se publicó en el Diario el Peruano, el Decreto Supremo N° 081 – 2017 – PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las Entidades de la Administración Pública, donde su objetivo principal es disponer 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.

En ese sentido, el presente plan está desarrollado en el marco de lo establecido DS N° 081 – 2017 – PCM que ayudará a la Institución a iniciar el proceso de transición con al protocolo IPV6.

II. BASE LEGAL

Se ha tomado como referencia los documentos de gestión y normativas vigentes relacionadas al tema de protocolo IPV6 para el Perú, y que a continuación se detallan:

- El Decreto Legislativo N° 604, Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29158, Ley Orgánica del Poder Ejecutivo.
- Ley N° 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica.
- Decreto Supremo N° 066-2011-PCM que aprueba el “Plan de Desarrollo de la Sociedad de la Información en el Perú-La Agenda Digital Peruana 2.0.”
- Decreto Supremo N° 081-2013-PCM que aprueba la Política Nacional de Gobierno Electrónico 2013-2017.
- Decreto Supremo N° 022-2017-PCM que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros.
- Decreto Supremo N° 081-2017-PCM, que aprueba la formulación de un Plan de Transición al Protocolo IPV6 en las entidades de la Administración Pública.
- Resolución N° 018-2018/SBN, que aprueba el “Plan Operativo Informático 2018” de la Superintendencia Nacional de Bienes Estatales-SBN.
- NTP ISO/IEC 27001:2014 Sistema de Gestión de Seguridad de la Información-SGSI.



III. OBJETIVOS DE PLAN DE TRANSICIÓN

El presente documento tiene como objetivo planificar las diversas actividades necesarias para lograr la transición del protocolo IPv4 a IPv6 en la infraestructura tecnológica de la SBN, estableciendo las líneas de acción más importantes a seguir, según las recomendaciones de la SEGDI que permitan su cumplimiento normativo.

Las principales actividades a realizar son:

- Elaborar y validar el inventario de activos de la infraestructura tecnológica
- Realizar el diagnóstico y la caracterización de la infraestructura tecnológica, software, hardware y servicios informáticos de la SBN.
- Identificar la brecha respecto del cumplimiento al protocolo IPv6, de su red de datos e infraestructura tecnológica, software, hardware y servicios informáticos de la SBN.
- Elaborar y ejecutar el cronograma de actividades de pruebas y resultados del protocolo IPv6.
- Elaborar y ejecutar el cronograma de actividades de la implementación del protocolo IPv6.
- Elaborar y ejecutar el cronograma de capacitación y sensibilización

IV. ALCANCE DEL PLAN DE TRANSICIÓN

El alcance del presente Plan de Transición se ha definido y establecido según los resultados de las actividades ejecutadas de relevamiento y caracterización de la infraestructura tecnológica de la SBN, cuyos resultados se han utilizado para identificar las diversas tareas requeridas que han involucrado los siguientes componentes:

- Equipos de comunicaciones: switches.
- Equipos de procesamiento y respaldo: servidor de datos, storage, enclousoure.
- Equipos End Point: Computadoras, laptops e impresoras de red.
- Software Base: Sistemas operativos y base de datos.
- Software de desarrollo de las aplicaciones.
- Equipamiento del ISP: Router.



V. DIAGNÓSTICO DE LA INFRAESTRUCTURA TECNOLÓGICA

Esta actividad se ha ejecutado entre los meses de junio y julio del 2018 con apoyo de una consultoría externa, cuyas actividades y análisis consolidado se describe a continuación:

5.1 Las actividades realizadas para la actividad de relevamiento, diagnóstico y caracterización de los componentes de la infraestructura tecnológica fueron las siguientes:

Cronograma de Actividades del Diagnóstico de la Infraestructura Tecnológica

N°	Actividades	Plazos	Responsables
1	Elaborar y validar el inventario de la infraestructura del ISP	Jun/Jul 2018	SBN (Área TI)
2	Elaborar y validar el inventario de los servidores de la SBN.	Jun/Jul 2018	SBN (Área TI)
3	Elaborar y validar el inventario de los equipos de seguridad y software de monitoreo.	Jun/Jul 2018	SBN (Área TI)
4	Elaborar y validar el inventario de los equipos de comunicaciones.	Jun/Jul 2018	SBN (Área TI)
5	Elaborar y validar el inventario de los equipos End Point (PCs, laptops, impresoras, teléfonos, cámaras, etc.).	Jun/Jul 2018	SBN (Área TI)
6	Elaborar y validar el inventario de software (Sistemas operativos, base de datos, lenguaje de programación).	Jun/Jul 2018	SBN (Área TI)
7	Caracterización y análisis de la infraestructura del ISP	Jun/Jul 2018	SBN (Área TI)
8	Caracterización y análisis de los servidores de la SBN.	Jun/Jul 2018	SBN (Área TI)
9	Caracterización y análisis de los equipos de seguridad y comunicaciones.	Jun/Jul 2018	SBN (Área TI)
10	Caracterización y análisis de los equipos End Point (PCs, laptops, impresoras y teléfonos.).	Jun/Jul 2018	SBN (Área TI)
11	Caracterización y análisis de Software (Sistemas operativos, base de datos y lenguaje de programación).	Jun/Jul 2018	SBN (Área TI)



12	Equipos y servicios que no soportan IPv6	Jun/Jul 2018	SBN (Área TI)
13	Evaluación de Riesgo	Jun/Jul 2018	SBN (Área TI)

5.2 El resumen de los resultados de la actividad de relevamiento y caracterización que nos permite identificar la brecha respecto del cumplimiento de los componentes sobre el protocolo IPV6, son los siguientes:

Componentes	Cantidad Total Hw /Sw	Con Soporte IPv4	Con Soporte IPv6	Brecha IPv6	% Brecha IPv6
HARDWARE					
ROUTER ISP	1	1	0	0.5	50
SERVIDORES	12	12	12	0	0
EQUIPOS DE SEGURIDAD	1	1	1	0	0
COMUNICACIONES	23	23	23	0	0
PCS	492	492	489	3	1
IMPRESORAS	33	33	33	0	0
TELEFONOS					0
SOFTWARE					
MONITOREO	1	1	1	0	0
APLICACIONES	15	15	8	7	47

- Se puede observar que brecha identificada, en general es baja, excepto en las aplicaciones, lo cual indica que la plataforma tecnológica actual de la SBN es estable con respecto al cumplimiento del protocolo IPV6.
- Respecto a Router ISP según el modelo soporta el IPv6, sólo faltaría actualizar a la última versión del firmware.
- Respecto de las aplicaciones que son las que tienen mayor porcentaje de incumplimiento, habría que revisar las estrategias de mitigación a aplicar (Cambio, actualización, upgrade, nuevo desarrollo, entre otros) y complementar con el análisis de los documentos de gestión, como el Plan Estratégico de Gobierno Electrónico - PEGE y el Plan Operativo Institucional - el POI.
- Con respecto a las PCs, la estrategia de mitigación sería la renovación, por el costo y el mínimo porcentaje no debería representar mayor problema su cumplimiento.



De los resultados obtenidos del análisis de la brecha respecto del cumplimiento del protocolo IPv6, se ha elaborado la siguiente Matriz de Análisis de Impacto, que nos permitirá identificar los riesgos asociados a cada componente identificado en los puntos anteriores respecto del protocolo IPv6, y se propone la siguiente clasificación para la valoración del impacto de los componentes afectados e identificados:

- **ALTO:** Afecta seriamente a los procesos y servicios informáticos más importantes de la SBN, con tiempos de recuperación elevados o hasta irrecuperables.
- **MEDIO:** Afecta los procesos y servicios informáticos en áreas específicas de la SBN, pero pueden ser mitigados con acciones complementarias.
- **BAJO:** No afecta a ningún proceso o servicio informático de la SBN, y los tiempos de recuperación no son relevantes.

Para la evaluación del riesgo en general, se deberá considerar además del riesgo, el porcentaje de no cumplimiento, porque esta combinación permite una mejor valoración de las actividades mitigadoras y su respectiva ejecución en las posteriores etapas:



MATRIZ DE ANÁLISIS DE IMPACTO

Componentes	Cantidad Total Hw /Sw	Objetivo	Riesgo	Amenaza	Impacto	Estrategia de Mitigación
HARDWARE						
PCS	3	Que todos los usuarios internos puedan acceder a los servicios que funcionan con protocolo IPv6	No podrán acceder a los servicios que funcionan con protocolo IPv6.	Equipos obsoletos cuando la SBN solo trabaje con el protocolo IPv6.	Bajo	Adquisición o Renovación de los equipos
SOFTWARE						
APLICACIONES	7	Que todos los usuarios internos y externos puedan acceder a las aplicaciones que funcionan con protocolo IPv6	Ningún usuario interno o externo podrá acceder a las aplicaciones que funcionan con protocolo IPv6.	Aplicaciones sin uso cuando la SBN solo trabaje con el protocolo IPv6.	Alto	Mantenimiento y/o actualización y/o desarrollo nuevo y/o cambio de aplicación



VI. IMPLEMENTACIÓN DEL PROTOCOLO IPV6

A continuación, se describe un cronograma con actividades genérico (configuración de servicios, configuración del protocolo IPv6, formulación de política de seguridad, entre otros), donde se señala actividad, plazos y responsables para la actividad implementación del IPv6 en la SBN.

Las actividades de seguridad de la información e informática deben ser coordinadas con el Oficial de Seguridad de la Información de la SBN.

Finalmente señalar, que el presente cronograma es referencial y que estará sujeto a actualizaciones según recomendaciones de la SEGDI, y de las buenas prácticas de la industria que en los próximos años se comiencen a implementar respecto de los mecanismos y metodologías de implementación del protocolo IPV6.

Cronograma de actividades de la Implementación

N°	Actividades	Plazos	Responsables	Entregables
1	Gestionar y adquirir los equipos que NO CUMPLEN protocolo IPV6	I - II Semestre 2019	SBN (Área TI)	Informe detallado de las actividades ejecutadas y anexos sustentatorios
2	Verificar y validar que las aplicaciones identificadas que NO CUMPLEN respecto del protocolo IPV6, no contengan código IP o URL IPV4 embebido.	I Semestre 2019	SBN (Área TI)	
3	Desarrollar y/o modificar y/o adquirir aplicaciones que NO CUMPLEN protocolo IPV6	II Semestre 2019 - I Semestre 2020	SBN (Área TI)	
4	Gestionar la habilitación de bloque o paquete de direccionamiento IPV6 para actividades de pruebas y despliegue en coordinación con la SEGDI, ente rector en esta materia.	I Semestre 2019	SBN (Área TI) / SEGDI	
5	Habilitación direccionamiento IPV6 para cada uno de los componentes de hardware y	II Semestre 2020	SBN (Área TI)	



	software de acuerdo al plan de diagnóstico de la Primera Fase.			
6	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	II Semestre 2020	SBN (Área TI)	
7	Configuración del protocolo IPv6 en aplicativos, sistemas de comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.	II Semestre 2020	SBN (Área TI)	
8	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea la SBN de acuerdo con los RFC de seguridad en IPv6.	II Semestre 2020	SBN (Área TI)	
9	Coordinación con el (los) proveedor (es) de servicios de Internet ISP, para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	I Semestre 2019	SBN (Área TI)	
10	Aplicación de alternativas de transición de servicios que no soportan IPv6. Recomendado Dual Stack	II Semestre 2019	SBN (Área TI)	

VII. REALIZACIÓN DE PRUEBAS



A continuación, se describe un cronograma con actividades genérico (pruebas de funcionalidad, calidad del servicio, compatibilidad de los equipos y monitoreo del IPv6, pruebas frente a las políticas de seguridad, afinamiento de las configuraciones realizadas, entre otros), donde se señalan actividades, plazos, responsables y entregables para la implementación del IPv6 en la SBN.



Las actividades de seguridad de la información e informática deben ser coordinadas con el Oficial de Seguridad de la Información de la SBN.



Finalmente señalar, que el presente cronograma es referencial y que estará sujeto a actualizaciones según recomendaciones de la SEGDI, y de las buenas prácticas de la industria que en los próximos años se comiencen a implementar respecto de los mecanismos y metodologías de implementación del protocolo IPV6.



Cronograma de actividades de pruebas

N°	Actividades	Plazos	Responsables	Entregables
1	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la SBN	I semestre 2021	SBN (Área TI)	Informe detallado de las actividades ejecutadas y anexos sustentatorios
2	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI	I semestre 2021	SBN (Área TI)	
3	Afinamiento de las configuraciones realizadas de hardware, software y servicios de la SBN	I semestre 2021	SBN (Área TI)	
4	Verificación de conectividad entre servidores de la zona LAN, DMZ e internet	I semestre 2021	SBN (Área TI)	
5	Verificación de conectividad de telefonía	I semestre 2021	SBN (Área TI)	
6	Verificación de conectividad de impresoras y equipos finales	I semestre 2021	SBN (Área TI)	
7	Verificación de conectividad VLAN	I semestre 2021	SBN (Área TI)	
8	Verificación de conectividad de equipos de cómputo para usuarios finales	I semestre 2021	SBN (Área TI)	
9	Pruebas de funcionalidad de aplicaciones	II semestre 2021	SBN (Área TI)	
10	Pruebas de calidad de servicio	II semestre 2021	SBN (Área TI)	
11	Compatibilidad de la infraestructura de red	II semestre 2021	SBN (Área TI)	
12	Verificación del cumplimiento de las políticas de seguridad	II semestre 2021	SBN (Área TI)	
13	Monitoreo de tráfico IPv6	II semestre 2021	SBN (Área TI)	



VIII. CAPACITACIÓN Y SENSIBILIZACIÓN

A continuación, se describe un cronograma con actividades genéricas (tipos de cursos, talleres, workshop entre otros), donde se señalan la descripción, tipo, duración, plazo y responsables para las actividades de migración del IPv6 en la SBN.

N°	Descripción	Tipo	Duración	Plazo	Responsables
1	Introducción al protocolo IPV6 – Funcionarios en general	Taller/Workshop Gerencial	02 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)
2	Introducción al protocolo IPV6 – Personal del área de TI en general	Curso técnico	08 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)
3	Protocolo IPV6 para gestión de infraestructura	Curso técnico	15 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)
4	Protocolo IPV6 para gestión de redes	Curso técnico	15 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)
5	Protocolo IPV6 para gestión de seguridad	Curso técnico	15 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)
6	Protocolo IPV6 para gestión de desarrollo	Curso técnico	15 horas	II Semestre 2018 - I Semestre 2019	SBN (Área TI)

IX. PRESUPUESTO ESTIMADO

Teniendo en consideración la brecha de componentes identificados sin soporte IPv6, a continuación se detalla la relación de proyectos que la SBN debe planificar a fin de asegurar que la plataforma tecnológica cumpla con el soporte protocolo IPv6:



Componentes	Cantidad Total Hw /Sw	Objetivo	Valor Referencial
PCS	03	Que todos los usuarios internos puedan acceder a los servicios que funcionan con IPv6	S/. 9000
APLICACIONES	07	Que todos los usuarios internos y externos puedan acceder a las aplicaciones que funcionan con IPv6	S/. 20000
SERVICIOS DE APOYO	01	Apoyo en la implementación y plan de pruebas IPv6	S/. 20000
SENSIBILIZACIÓN A FUNCIONARIOS Y PERSONAL DE TI		Que todos los funcionarios tengan conocimiento de la importancia del uso de IPv6 y su impacto dentro de las actividades que realiza la SBN	S/. 10000
CAPACITACIÓN		Capacitar al personal de TI, en los conceptos básicos de IPv6 y posteriormente una capacitación especializada haciendo énfasis en los distintos roles de redes, seguridad, administración de sistemas y desarrollo. Esta actividad debería realizarse antes del inicio de las pruebas e implementaciones.	S/. 10000

X. ANEXOS

Se adjunta los documentos y formatos de trabajo en digital que se utilizaron para realizar el diagnóstico y caracterización correspondiente, los cuales se encuentran en formato digital:

- Anexo 01 - Inventario de equipos de infraestructura
- Anexo 02 - Inventario de equipo de comunicaciones
- Anexo 03 - Inventario de End Point
- Anexo 04 - Inventario de equipo de seguridad
- Anexo 05 - Proveedor ISP
- Anexo 06 - Inventario de aplicaciones.



Anexo 01 - Inventario de Equipo de Infraestructura

N°	Marca	Modelo	Cantidad	Sistema Operativo	Soporte IPV6	Referencia
1	DELL	PowerEdge R310	2	W2008R2	Si	http://www.dell.com/downloads/global/products/pedge/en/PowerEdgeR310TechGuide.pdf
2	DELL	PowerEdger 2950	1	W2008R2	Si	http://www.dell.com/downloads/global/solutions/11Gtransition.pdf
3	HP	HP DL380 G7	1	W2008R2	Si	https://www.voxility.com/dedicated-server/custom/DL380+Gen7+%281xE5645%29+SFF
4	HP	PC	1	W2000	Si	https://www.mouser.com/pdfdocs/82567brief-2.pdf
5	Oracle	SUN BL X6270 M3	5	W2008R2	No	https://docs.oracle.com/cd/E20881_01/pdf/E20891.pdf
6	Oracle	SUN BL X4-2B	2	W2008R2	No	https://docs.oracle.com/cd/E37035_01/pdf/E37039.pdf
7	Oracle	SUN BLADE 6000 CHASSIS	1		Si	https://docs.oracle.com/cd/E19938-01/820-0050-11/Configuring_terminal_network.html







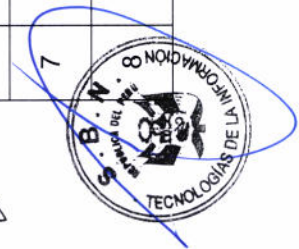

Anexo 02 - Inventario de Equipo de comunicaciones

N°	Equipo	Marca	Modelo	Puertos Ethernet		Cantidad	Año de Adquisición	Propio / Alquiler	Soporte IPv6	Referencia
				Cantidad	Tipo					
1	Switch Core	HP	HP5 800	48	Gigas Ethernet	2	2015	Propio	Si	https://support.hp.com/hpsc/doc/public/display?docId=emr_na-c02648783 - https://www.originmicro.com/product/538/9 - https://www.elgigantenforetag.se/pdf/EE5DE1E3-8DBC-4074-A519-CE7A6B19C990.pdf
2	Switch Borde	HP	HP5 120	48	Gigas Ethernet	8	2015	Propio	Si	https://support.hp.com/hpsc/doc/public/display?docId=emr_na-c03996973 - https://h50146.www5.hp.com/products/networking/datasheet/HP_5120EI_Switch_Series.pdf
2	Switch Borde	HP	HP5 130	24	Gigas Ethernet	13	2015	Propio	Si	https://h50146.www5.hp.com/products/networking/datasheet/HP_5130EI_Switch_Series_J.pdf



Anexo 03 - Inventario de Equipo de EndPoint

N°	Equipo	Marca	Modelo	Cantidad	Soporte IPv6	Sustento
1	PC	-	-	1	Si	http://www.educa.madrid.org/web/colegio1/equipamientos/Patrimonio_primaria_2007_2008_equipos_HP_Serlinge/img/Documentacion/Intel82566GigabitNC.pdf
2	PC	HP	Compaq 8200 Elite Series	2	Si	http://content.ettilize.com/user-manual/1021692738.pdf
3	PC	Server Guru	Compatible	5	Si	https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-connection-i219-datasheet.pdf
4	PC	HP	HP ProDesk 400	1	Si	http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA6-9030EEAP - http://www.realtek.com.tw/products/productsView.aspx?Langid=1&PNid=13&PFid=5&Level=5&Conn=4&ProdID=319
5	PC	Lenovo	ThinkCentre M58e	3	No	No existe información
6	PC	Lenovo	P310	1	Si	https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/i218-ethernet-connection-datasheet.pdf
7	PC	Lenovo	ThinkCentre M72e	127	Si	https://www.unixblogger.com/2016/08/11/how-to-get-your-realtek-rtl8111rtl8168-working-updated-guide/
8	PC	Lenovo	ThinkCentre M73	61	Si	https://www.unixblogger.com/2016/08/11/how-to-get-your-realtek-rtl8111rtl8168-working-updated-guide/



PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

9	PC	Lenovo	ThinkCentre M82	53	Si	https://www.mouser.com/pdfdocs/82579brief.pdf
10	PC	Lenovo	ThinkCentre M900	74	Si	https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-connection-i219-datasheet.pdf
11	PC	Lenovo	ThinkCentre M93p	59	Si	https://www.mouser.com/pdfdocs/82579brief.pdf
12	PC	Advance	VISSION	7	Si	http://www.educa.madrid.org/web/colegio1/equipamientos/Patrimonio_primaria_2007_2008_equipos_HP_Seringe/img/Documentacion/Intel82566GigabitNC.pdf
13	PC	Advance	VISSION 6685 DPM	6	Si	https://www.mouser.com/pdfdocs/82567brief-2.pdf
14	PC	Advance	VISSION 7650-G DBM	1	Si	https://www.intervalzero.com/assets/IZSupportedNIC.pdf
15	PC	Advance	VISSION VC2293	43	Si	https://www.mouser.com/pdfdocs/82567brief-2.pdf
16	PC	Lenovo	Z270-HD3	2	Si	https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/ethernet-connection-i219-datasheet.pdf
17	Laptop	Lenovo	ThinkPad E550	5	Si	https://usermanual.wiki/Lenovo/E550E555E550CUGEs.244041561.pdf
18	Laptop	Lenovo	ThinkPad L570	35	Si	https://cdn.cnetcontent.com/syndication/mediaserver/inlinecontent/all/086/3e6/0863e6d458a4ce707af28ea08ddcab03a/original.pdf - https://usermanual.wiki/Lenovo/L570UGEs.1687788648.pdf
19	Laptop	Toshiba	PT234P-00KLM1	1	Si	https://www.mouser.com/pdfdocs/82579brief.pdf
20	Laptop	Lenovo	T430	5	Si	https://www.mouser.com/pdfdocs/82579brief.pdf



Anexo 04 - Inventario de Equipo de Seguridad

N°	Tipo de Equipo	Software	Rol	Virtual o Físico	Cantidad	Sistema Operativo	Versión del Sistema Operativo	Año de Adquisición	Propio / Alquilado	Soporte IPv6	Referencia
1	HW	WATCHGUARD M400	Firewall	Físico	1	Fireware OS	V12.1.b548280	2016	Propio	Si	http://www.arp.com/medias/54c8ecc59ce969b82eec20af.pdf



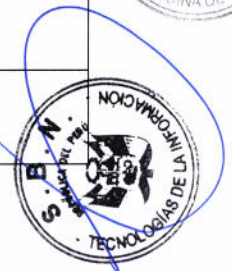
Anexo 05 - Proveedor ISP

Sede	ISP	Dirección IP WAN	Mascara	Velocidad (BW)	Servicio	Equipo	Marc	Modelo	Soporte IPv6	Sustento	Referencia
CHINCHON	OPTICAL NETWORK KS	168.121.236.16	28	60 Mbps	Internet	Router	Cisco	Cisco2811	Cumple Parcialmente	Depende de la versión del IOS	https://learningnetwork.cisco.com/thread/90960



Anexo 06 - Inventario de Aplicaciones

No.	Nombre Aplicación, SI o servicio	Plataforma de la Herramienta desarrollo y version	Rol de la Aplicación	Relación con otros sistemas	Entorno
1	SINABIP Cliente – Servidor	LP: Power Builder Vs: 8.0	Administra los actos que se pueden dar sobre un predio. Como parte de los procedimientos del acto, se pueden generar documentos internos en el SID. CUS (Código Unico Sinabip) Código Interno	SID SICA JMAP	Ciente Servidor
2	SINABIM Cliente – Servidor	LP: Power Builder Vs: 8.0	Sistema de Información Nacional de Bienes Muebles		Ciente Servidor
3	Sistema Integrado Documentario SID	LP: Power Builder Vs: 8.0	Sistema que permite gestionar la documentación que ingresa a la SBN, reflejada en solicitudes de ingreso y documentos internos.	SINABIP SICA	Ciente Servidor
4	Control de accesos por aplicativos – SICA	LP: Power Builder Vs: 8.0	Sistema para gestionar los accesos de usuarios a las diferentes aplicaciones desarrolladas en Power Builder.	Permite brindar acceso a aplicativos cliente servidor: - SID - SINABIP - PPJJ - COMISIÓN DE SERVICIOS	Ciente Servidor



PLAN DE TRANSICIÓN AL PROTOCOLO IPV6

5	Control vehicular	LP: Power Builder Vs: 8.0	Sistema que permite gestionar información de los vehículos de la SBN tales como consumo de combustible, kilometraje.	SICA	Cliente Servidor
6	Procesos Judiciales	LP: Power Builder Vs: 8.0	Aplicativo utilizado por Procuraduría SBN.	SICA	Cliente Servidor
7	Comisión de Servicios		Aplicativo que registra boletas de comisión de servicios de los colaboradores de la SBN.	SICA	Cliente Servidor
8	Aporte Gráfico	Visual C# .Net - Net Framework 4.0	Registro gráfico de Actos Administrativos	Web Services Aportes	Cliente Servidor
9	Web Service PIDE	Visual C# .Net - Net Framework 4.0	Remisión de información para PLATAFORMA DE INTEROPERABILIDAD DEL ESTADO - PIDE	SINABIP WEB SINABIP CLIENTE SERVIDOR	Web Service
10	Web Service Remisión MVCS	Visual C# .Net - Net Framework 4.0	Remisión de información para el Ministerio de Vivienda	Relación a nivel de base de datos del SID y SINABIP	Web Service
11	Web Service Aportes	Visual C# .Net - Net Framework 4.0	Conexión entre aplicativo de aportes y base de datos gráfica	SID JMAP	Web Service
12	INTRANET	PHP 5.6	Sistema interno de la SBN	SINABIP C/S, SINABIP WEB SID PORTAL WEB JMAP	web
13	SINABIP WEB	PHP 5.6	Administra bienes muebles e inmuebles de las entidades asociadas a la SBN	SINABIP C/S SID JMAP	web
14	JMAP	JAVA (JDK 1.8 64 bits)	Plataforma de integración cartográfica	Relación a nivel de base de datos del SID, SINABIP WEB y Aporte Gráfico	web
15	PORTAL WEB	PHP 5.6 (WORDPRESS)	Pagina Web institucional	Relación a nivel de base de datos del SID (consultas)	web

