SALUD
SECRETARÍA DE SALUD

Instituto Nacional de Rehabilitación
Luis Guillermo Ibarra Ibarra

PLAN LOCAL DE TRANSICION A IPV6 EN EL INSTITUTO NACIONAL DE REHABILITACIÓN LUIS GUILLERMO IBARRA IBARRA 2023

Versión 1.0

Fecha: 15/03/2023	Elaboró: Ing. Donato Lucio López López	Revisó: Ing. Omar Mercado Pedraza	Autorizó: Mtra. María de Lourdes Zaldivar Martínez
Puesto	*Coordinador de la Red de Datos*	*Jefe del Departamento de Gestión de Arquitectura e Infraestructura Tecnológica*	*Subdirectora de Tecnologías de la Información y Comunicaciones*
Firma			

I. Contenido

1.- JUSTIFICACIÓN

El protocolo IPV4 se creó en 1983 para el uso de ARPANET, red que para aquella época era bastante pequeña, sus creadores no llegaron a vislumbrar el tamaño e importancia actual y es por este motivo que el protocolo IPV4 no fue suficiente para la cantidad de dispositivos que se conectan en la actualidad a internet. Durante todos estos años de su funcionamiento se han explorado diferentes maneras de resolver este inconveniente y estos métodos también se quedaron cortos ante el gran tamaño de internet es por esto que la Internet Assigned Numbers Authority (IANA) decidió adoptar como protocolo de direccionamiento IPV6 el cual permite solucionar este inconveniente. Pero esto plantea nuevos retos como lo son la transición de estos dos protocolos, por esta razón se decretó el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal publicado en 6 de septiembre de 2021, en el cual se menciona en el Artículo 51.- "*Las instituciones deberán adoptar las medidas para migrar sus servicios de telecomunicaciones hacia el protocolo de internet IPV6, de conformidad con la guía que para tal efecto emita la CEDN; mientras tanto, podrán utilizar el Protocolo de Internet IPv4 en aquellos servicios que sean expuestos tales como correo electrónico, transferencia de archivos, conexiones seguras y aplicaciones web*". Para ello es necesario tener en cuenta diferentes factores que se describirán en el desarrollo de este documento.

2.- OBJETIVO

Establecer el plan local de transición, planificada y de manera gradual al protocolo de internet versión 6 (IPV6) en el Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra en los equipos de comunicaciones de alta criticidad que brindan servicio a la ciudadanía y conforman la infraestructura tecnológica de TIC dentro del INRLGII, procurando en todo momento evitar la interrupción de los servicios.

3. ANTECEDENTES

Con fecha 06 de septiembre de 2021 fue publicado en el Diario Oficial de la Federación el ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal, el cual establece en su ARTÍCULO DÉCIMO transitorio que la CEDN emitirá la Guía para la migración al Protocolo de Internet versión 6; dentro de los tres meses posteriores a la publicación de este Acuerdo, a partir de esa fecha, las Instituciones contarán con un plazo de 2 años para concretar la Transición de sus servicios de telecomunicaciones.

Con fecha 7 de diciembre de 2021, la Coordinación de la Estrategia Nacional emite la "Guía para la Transición al Protocolo de internet versión 6 (IPv6) en la Administración Pública Federal", en la cual se establecen las disposiciones de carácter general para orientar a las Instituciones Federales, en las acciones técnicas a desarrollar, con la finalidad de que la transición al Protocolo de Internet versión 6 se lleve a cabo de forma expedita y coordinada, con un mínimo de interrupciones y trastornos de carácter técnico u operativo, y en observancia de los controles mínimos de Seguridad de la Información, y su cumplimiento es de carácter general y obligatorio para todas las instituciones de la Administración Pública Federal.

4.- GLOSARIO

IPv6	Protocolo Internet versión 6
IPv4	Protocolo Internet versión 4
VPN	Virtual Private Network.
Firewall	Sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.
FW	Firewall
DMZ	Zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet.
TIC	Las Tecnologías de la Información y las Comunicaciones.
IPSec	Protocolo Internet Seguro.
CEDN	Coordinación de Estrategia Digital Nacional.
RFC-4890	Documento numérico en el que se describen y definen protocolos, conceptos, métodos.
NAT	Traductor de direcciones de Red.
HTTPS	Protocolo de transferencia de hipertexto seguro.
SENDMAIL	Aplicación de servidor que permite enviar correo electrónico usando el protocolo SMTP.
SMTP	Protocolo Simple de Transferencia de Correo.
LDAP	Protocolo de estándar abierto para usar con servicios de directorio en línea.
NTP	Network Time Protocol.
LAN	Red de Área Local.
ISP	Proveedor de servicios de Internet.
MGSI	Marco de Gestión de la Calidad.
DNS	Sistema de nombres de Dominio.
ASN	Números de sistema autónomo.
CTI	Congreso de calidad en áreas críticas.
CIIR	Congreso Internacional de Investigación en Rehabilitación
RedCap	Software de captura de datos electrónicos y una metodología de flujo de trabajo para diseñar bases de datos de investigación de ensayos clínicos e investigación.
ICMpv6	Protocolo de Mensajes de Control de Internet Versión 6.
OSPFv3	(Open Shortest Path First) es un protocolo de ruteo para IP.
VLANs	Red de área local virtual.

5.- PLAN DE TRANSISION LOCAL A IPV6 PARA EL INRLGII

A. Programa de capacitación para el personal técnico que participa en la administración de las redes y sistemas involucrados en la transición

La capacitación técnica es esencial para una adecuada transición local por lo que se consideran realizar cursos de capacitación relacionados al protocolo IPv6 para el personal involucrado en las diferentes áreas de TIC y que participarán directamente en el proceso de transición y/o en su caso despliegue del protocolo, como lo es el caso del desarrollo de nuevos sistemas.

Los temas de capacitación varían de acuerdo las instancias que las imparten, pero los cursos a considerar serían los siguientes:

• Enrutamiento de IPV6. • Servicios y aplicaciones sobre IPV6. • Seguridad en IPV6. • Curso IPV6 básico y avanzado	https://edutin.com/curso-de-ipv6-3548 https://campus.lacnic.net/mod/page/view.php?id=4706 https://ipv6.ift.org.mx/ https://campus.lacnic.net/mod/page/view.php?id=7248&lang=en https://www.mikrotikmexico.com.mx/mtcipv6e.html https://mikrotik-mexico.com.mx/producto/mikrotik-certified-ipv6-engineer/

B. Planteamiento de los escenarios de coexistencia entre IPv4 e IPv6

Actualmente los servicios que ofrece el instituto INRLGII, así como su conectividad hacia el internet se encuentran operando solo bajo el protocolo de internet versión 4 (IPV4) por lo tanto y con el propósito de realizar de manera gradual y ordenada la transición a IPv6 sin tener afectaciones en la operabilidad y rendimiento, se efectuarán las tareas necesarias para pasar de un esquema de configuraciones de solo IPV4 a un esquema de convivencia de ambos protocolos de internet versión 4 y versión 6, con una metodología de comunicación de paquetes configurada en DualStack, con la finalidad de realizar los cambios hacia IPV6 de manera controlada y sin afectar la operación del instituto.

C. Identificación de las técnicas de transición a implementar

Las tecnologías sugeridas para la coexistencia entre ambos protocolos son:

- **Dual-stack (doble pila)**: El Dual Stack propone que los hosts y enrutadores de la red del operador ISP tengan soporte dual de Protocolo IP. Esto es, todo dispositivo de red tiene soporte dual y simultáneo de los Protocolos IPv6 e IPv4. La idea de Dual Stack es que los hosts y las aplicaciones puedan hacer uso o bien del stack IPv4, del stack IPv6 e incluso de ambos Stacks de forma simultánea, para obtener mejor desempeño en el establecimiento de las conexiones. Los dispositivos duales stack pueden manejar conexiones IPv4 e IPv6 a través de una misma interfaz de red o bien hacerlo por interfaces de red separadas, según la arquitectura de red a la que estén conectados. Las aplicaciones que se conecten hacia servidores IPv4 lo harán desde una IPv4 y las conexiones hacia IPv6 se hacen desde IPv6. No suponen conexiones de IPv4 a IPv6 ni de IPv6 a IPv4 en el mecanismo Dual Stack.

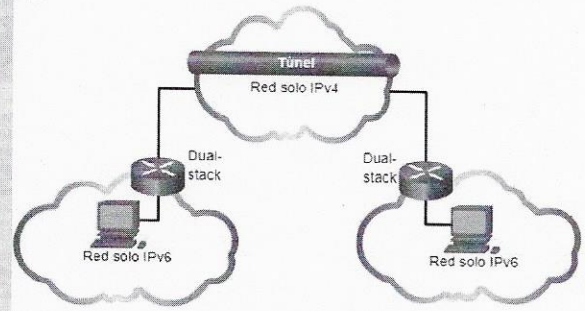
- **Tunneling**: Es un método para transportar paquetes IPv6 a través de redes IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.

- **Traducción:** La traducción de direcciones de red 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce en un paquete IPV4, y viceversa.

Para llevar a cabo el proceso de transición al protocolo IPv6, se propone emplear la técnica dual-stack por las siguientes razones:

- La primera razón y la más importante es que se permite una coexistencia indefinida de IPv4 e IPv6 y de esta manera se puede tener una migración más controlada hacía IPV6.
- Actualmente IPv6 está incluido en todos los sistemas operativos y dispositivos de última generación, por lo que al menos en los equipos de arrendamiento evitará tener costos adicionales.
- Las aplicaciones o librerías escogen la versión de IP a emplear.

En caso de ser necesario podría utilizarse la tecnología Tunelling mencionada arriba que permite el encapsulamiento de IPV6 dentro de IPV4 que nos permitan pasar por redes que aun estén bajo el protocolo IPV4 esto quedaría a cargo del proveedor de servicios de internet ISP.



D. Identificación de las aplicaciones y equipos que deberán ser actualizados o sustituidos.

Para el Instituto Nacional de Rehabilitación Luis Guillermo Ibarra Ibarra INRLGII se consideraron únicamente los activos críticos y aplicativos que brindan un servicio a la ciudadanía, y que actualmente cuentan con una dirección IPv4 publica.

El resto de los equipos que componen la red LAN no requieren el cambio a IPv6 ya que es un servicio interno y no interfiere con la falta de direccionamiento IPv4.

Las siguientes aplicaciones y equipos son los que se tienen contemplados para ser actualizados.

Aplicaciones:

Portal Web Institucional	inr.gob.mx
Correo Electrónico Institucional	correo.inr.gob.mx
Campus Virtual	campusvirtual.inr.gob.mx
CTI	cti.inr.gob.mx
CIIR.	ciir.inr.gob.mx
Biblioteca Tlacuilo	biblioteca.inr.gob.mx
Nube	nube.inr.gob.mx
RedCap	redcap.inr.gob.mx

Equipos:

Los equipos de direccionamiento que se consideran, de acuerdo a la maqueta que se realizó son actualmente compatibles con IPV6 por esto se considera solamente la configuración del siguiente equipamiento:

Firewall	Palo Alto 3050
Switch de Core	192.168.XXX.XXX

E. Identificación y planteamiento de atención a los potenciales riesgos a la seguridad de la información que se encuentren asociados a la transición.

De acuerdo a la Guía De Referencia Para la Implementación del Protocolo De Internet Versión 6 (Ipv6) donde se indica que "De igual manera se recomienda establecer un esquema de Seguridad especial para la comunicación por IPv6. Por ejemplo, el protocolo IPv6 depende mucho del tráfico

ICMPv6 lo cual implica un reajuste de políticas dentro del perímetro de Seguridad. Dicho reajuste debe estar apegado a las recomendaciones del RFC 4890."

IPv6 debido a su nueva implementación en el Instituto, se desconocen actualmente las vulnerabilidades que podrían presentarse en los activos para llevar a cabo dicha transición, los cuales pueden generar riesgos de seguridad de información, que impacten a los servicios de brinda el instituto a la ciudadanía; con el objeto de poder detectar estos riesgos se requiere hacer un análisis posterior que permita encontrar posibles vulnerabilidades bajo IPv6 para llevar a cabo este análisis de vulnerabilidades.

Este análisis se está programando para que se realice el segundo semestre del 2024, ya que es necesaria la adquisición de software y se requiere de recurso económico el cual se solicitara con anticipación para el ejercicio del 2024.

1. Estrategias de Seguridad de la Información para IPv6.

Las estrategias de seguridad mencionadas a continuación deberán ser implementadas en todos los servicios que se van a migrar a IPv6. El Área de Seguridad de la Información del Instituto será la encargada de coordinar la implementación de estas estrategias en conjunto con las áreas correspondientes.

Se promoverá la implementación de políticas de seguridad de la información en IPv6 que permitan la disponibilidad, accesibilidad, integridad y autenticidad de los recursos de TIC´s, de los servicios críticos de la institución y de la información como activo principal.

Todo el tráfico IPv6 que se intercambie entre redes externas y la Red Institucional, será validado y autorizado por los mecanismos de seguridad implementados en el Instituto por medio del Firewall PaloAlto, priorizando una política de seguridad de la información restrictiva para el tráfico IPv6 que requiera ingresar a la Red Institucional

Por medio del Firewall se gestionará la seguridad en zonas de seguridad perimetral DMZ para alojar servicios de TIC públicos sobre IPv6.

Es indispensable contar con un software para la detección de vulnerabilidades que ayude al análisis para prevenir y detectar vulnerabilidades y ataques de seguridad de la información, el cual se llevara a cabo al final de la transición, toda vez que se autorice el presupuesto para la adquisición del Software.

En este sentido, el proceso de transición a IPv6 deberá privilegiar la protección de la información en sus cuatro principales propiedades: confidencialidad, integridad, disponibilidad y autenticidad.

2. VPN (Redes Privadas Virtuales).

Se definirán o en su defecto se modificarán las reglas del Firewall que minimicen los incidentes de seguridad del tráfico de IPv4 e IPv6 por Dual Stack de las comunicaciones a través de redes privadas virtuales.

La Red Institucional solo implementará VPN's basadas en IPSec, utilizando la herramienta Global Protect esta herramienta es propia del Firewall, una vez que este implementado Dual Stack con la ayuda de software se identificaran posibles riesgos de seguridad en el uso de VPN's sobre IPv4 e IPv6 por Dual Stack.

3. Monitoreo de IPv6.

Las actividades de monitoreo del tráfico IPv6 de la DMZ hacia la red Institucional permitirá la detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad.

Al realizar el monitoreo de los servicios de red en IPv6 se considerará:

a) El tráfico generado por los dispositivos de red,
b) El estado de los servicios y aplicaciones que operan en el INRLGII
c) Las rutas que sigue el tráfico dirigido a Internet.

Estas tres consideraciones se realizarán con el Firewall PaloAlto para ambos protocolos, toda vez que cuenta con posibilidad de hacerlo.

4. Análisis y gestión de riesgos en IPv6

Como parte del proceso de gestión en la transición a IPv6, se realizará una evaluación para identificar los riesgos potenciales derivados del proceso de transición que permita determinar cuál es el nivel de riesgo de los activos de la información que brindan el servicio a la ciudadanía.

Dicho análisis se propone realizarlo con la herramienta de seguridad (**Vulnerability Manager Plus**) la cual detecta y evalúa las vulnerabilidades. Para gestionar los riegos hasta su eliminación o mitigación.

El personal de seguridad de la Información del INRLGII analizará activamente las vulnerabilidades de los activos de información que surjan como consecuencia de la implementación de IPv6 en la Red, este análisis se pretende realizar a inicios del segundo semestre del 2024.

Una vez identificados los riesgos o vulnerabilidades será realizada una estimación y evaluación de riesgos que permitan medir las consecuencias o impactos tanto cuantitativa como cualitativamente, así como su probabilidad de ocurrencia y determinar el tratamiento que se aplicará a cada riesgo.

Todo lo anterior alineado a los controles establecidos en el Marco de Gestión de Seguridad de la Información (MGSI)

F. Identificación y Planteamiento de atención a los efectos operativos en las aplicaciones y redes que eventualmente pudieran afectarse durante y después de la transición

Los servidores, máquinas virtuales, equipos de Comunicaciones y de Seguridad, son capaces de aceptar la configuración del nuevo protocolo y soportan la operatividad establecida.

Asimismo, los servicios de red que contengan los servidores virtuales se encuentran actualizados para adaptarse a la nueva tecnología. Por mencionar algunos servicios HTTP, HTTPS, SENDMAIL, LDAP, etc. En cuanto al equipo de red con soporte IPV6, son aptos para establecer la comunicación deseada y así solo realizar un cambio en la configuración.

Todo lo anterior alineado a los controles establecidos en el Marco de Gestión de Seguridad de la Información (MGSI)

Servicio de Internet.

El ISP que proporciona el servicio de internet en el Instituto deberá cumplir con las siguientes características:

- Soportar los protocolos IPv4 e IPv6 en modo dual stack.
- Brindar el servicio de direccionamiento DNS de IPv6 e IPv4 (Dual Stack)
- Atención y monitoreo del enlace 7 x 24 x 365 días.
- Disponibilidad del servicio de acuerdo con el SLA que maneja el instituto, aproximadamente del 99,8%
- El Instituto cuenta con un ancho de banda de 150 Mbps para cubrir las necesidades del presente y futuro del Instituto.
- En caso de una contingencia se cuenta con un enlace redundante que permite la continuidad de la operación del Instituto.

G. Plan de direccionamiento IPv6 independiente del prefijo

Se llevo a cabo la solicitud de bloques de direcciones IPV6 y ASN ante IAR México, quien asigno dichos recursos tecnológicos al INRLGII, los cuales ya se reportaron en la Herramienta de Gestión de Política TIC, ante la Coordinación de Estrategia Digital, como se muestra a continuación:

Bloque de direcciones (tabla segmentación)

IPv6	2801:C4:3B:0:0:0:0:0/48
ASN	270191

Con el bloque de direcciones IPV6 y ASN, el cual se reportó en la Herramienta de Gestión de Política TIC ante la Coordinación de Estrategia Digital, se expone el siguiente plan de direccionamiento:

Subneteo IPv6

Dirección IP/Mask	2801:C4:3B:0:0:0:0:0/56
Dirección IP Full	2801:00c4:003b: 0000:0000:0000: 0000:0000
Total, de Direcciones IP	4,722,366,482,869,640,000,000
Total /64 Redes	256
Red	2801:00c4:003b:0000::0000
Rango de IPs	2801:00c4:003b:0000::0000 - 2801:00c4:003b:00ff: ffff:ffff:ffff:ffff

Asignación de Direccionamiento IPv6

2801:C4:3B:00:0:0:0:0	Rango para los activos, interfaces FW, Switches de Core, Etc.
2801:C4:3B:01:0:0:0:0	Rango reservado
2801:C4:3B:02:0:0:0:0	Rango para las aplicaciones (servidores)
2801:C4:3B:03:0:0:0:0	Rango reservado

H. Proyecciones de escalabilidad del Plan de Transición Local a IPV6

La escalabilidad del plan se definirá de acuerdo con los resultados de la transición.

El resultado y la proyección de escalabilidad se integrará de manera gradual como parte del presente plan.

- En cada uno de los activos antes mencionados se habilitarán los Protocolos IPv4 e IPv6.
- Establecer la Comunicación y probar conexiones con ambos protocolos de manera local y de manera externa desde internet.

I. Programa de costos y acciones administrativas asociados a la transición

Para la contratación de los recursos del bloque de direcciones IPV6 y ASN, que requiere contratar el INRLGII, será de acuerdo a las nuevas tarifas autorizadas por la Asamblea de Miembros de LACNIC de mayo de 2017 (Foz de Iguazú, Brasil), mismas que entraron en vigor a partir del día 1° de enero de 2018. Para referencia, se muestran las tarifas vigentes hasta el día 31 de diciembre de 2017 y las tarifas que entrarán en vigor a partir del 1° de enero de 2018.

Todas las cantidades están expresadas en dólares americanos, y se pagan en Moneda Nacional utilizando la cotización establecida por el Banco de México para solventar obligaciones denominadas en dólares de los EE.UU.A., pagaderas en la República Mexicana.

Tarifas pagadas:

Tarifa de Registro y/o Renovación de Asignaciones de Direcciones IPv6 para Usuarios Finales. Cantidades en dólares americanos. Las cantidades no incluyen IVA.

La factura con folio: IAR-4311, se expide el 17 de enero del 2023, donde se desglosa las siguientes cantidades pagadas en pesos mexicanos.

Concepto	Monto Inicial.
Asignación inicial IPv6 /48	$49,100.00
Asignación de ASN	$19,640.00
MONTO TOTAL PAGADO	$68,740.00

Tarifas por pagar:

Tarifa de Renovación de Asignaciones de Direcciones IPv6 para Usuarios Finales. Cantidades en dólares americanos. Las cantidades no incluyen IVA.

Concepto	Renovación de Asignación Anual
Prefijo de Direcciones IPv6 /48	$600

Propuestas de costos por pagar en moneda nacional, sujetas a previa autorización.

Concepto	Costos Pago único.
Software para la mitigación de Vulnerabilidades	$250,500
Capacitación a 8 Ingenieros	$95,000
Análisis de Vulnerabilidades	$850,000

1. Programa de Transición a IPv6

Las Instituciones, deberán poner en operación su Plan de Transición Local a IPv6, éste deberá considerar el cumplimiento de los siguientes hitos:

a) Cuando menos el 20% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2023.
b) Cuando menos el 50% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2024.
c) Cuando menos el 80% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2025.

Plan de Transicion IPv6																								
Activos / Aplicativos	2023								2024								2025							AVANCES
	1er Semestre				2do Semestre				1er Semestre				2do Semestre				1er Semestre				2do Semestre			
Firewall																								
Core																								Cuando menos el 20% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2023.
CIIR																								
Biblioteca Tlacuilo																								
Portal_Web																								Cuando menos el 50% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2024.
Correo institucional																								
CampusVirtual																								
CTI																								Cuando menos el 80% de los activos que brindan servicio a la ciudadanía deberán operar en un ambiente IPv6 para finales de 2025.
Nube																								
RedCap																								
Analisis de Vulnerabilidades																								

Por medio de una solicitud de cambio se ejecutarán las siguientes actividades:

- **Se realizará la configuración y puesta en marcha de los equipos de seguridad perimetral FW y CORE.**

  El FW recibe el enlace IPv6 proveniente del ISP, la configuración seria de la siguiente manera:

  - Configuración del puerto del FW con una dirección IPv6/126
  - El ISP realizara la misma configuración con otra dirección IPv6/126 del mismo segmento.
  - Configuración del enrutamiento entre ambos puntos con el protocolo OSPFv3.

  En la LAN el FW deberá dar direccionamiento IPv6/64 y enrutar al menos estáticamente hacia el CORE.
  Y el CORE deberá dar direccionamiento en IPv6/64 y enrutar estáticamente hacia el FW de la siguiente manera:

  - Creación y configuración de VLANS en IPv6.
  - Configuración de direccionamiento hacia el FW por las VLANs del CORE
  - Configurando una ruta estática IPv6 hacia el FW
  - Configuración de Acceso (en este caso se deberán extender las VLANs desde el CORE hacia los Switch de acceso a las Maquinas Virtuales con los aplicativos).

- **Se realizará la configuración y puesta en marcha de cada uno de los aplicativos que brindan servicio a la ciudadanía.**

  En cada una de las máquinas virtuales de los aplicativos les será configurado la interfase de red con:

  - La dirección IPv6
  - Longitud de prefijo de subred (/64)
  - Puerta de enlace
  - Y DNS primario y secundario.

- **Análisis de vulnerabilidades.**
    - Como se mencionó anteriormente el personal de seguridad de la Información del INRLGII analizará activamente las vulnerabilidades de los activos de información en base al MGSI, se realizará dicho análisis con una periodicidad semestral y para el caso de la transición una vez realizada se llevará a cabo un análisis extraordinario para verificar las vulnerabilidades que surjan como consecuencia de la implementación de IPv6 en la Red.

En relación con el objetivo de cumplir con lo antes mencionado, se enlista el 100% de activos que brindan servicio a la ciudadanía.

Firewall	panos.inr.gob.mx
Switch de Core	192.168.XXX.XXX
Portal Web Institucional	inr.gob.mx
Correo Electrónico Institucional	correo.inr.gob.mx
Campus Virtual	campusvirtual.inr.gob.mx
CTI	cti.inr.gob.mx
CIIR	ciir.inr.gob.mx
Biblioteca Tlacuilo	biblioteca.inr.gob.mx
Nube	nube.inr.gob.mx
RedCap	redcap.inr.gob.mx