Plan de Transición Local a IPv6 del Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California

Departamento de Redes
Dirección de Telemática
CICESE

Versión 1.9
17 de junio de 2022

Tabla de contenidos

Notas Legales

Alcance

Este documento define las actividades a realizar dentro de la Red del Centro de Investigación Científica y de Educación Superior de Ensenada, Baja California (“Red-CICESE”) para lograr una transición hacia el uso de IPv6 de acuerdo con lo señalado en la “Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal” emitido por la Coordinación de Estrategia Digital Nacional (CEDN).

Este Plan de Transición está dirigido al personal técnico, técnicos de apoyo, administradores de sitios web y responsables de servicios y consultas públicas del CICESE que, para su operación, hacen uso de los recursos de red del Centro. El personal del CICESE mencionado deberá observar y cumplir las políticas aquí contenidas.

Introducción

La “Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal”[1] emitida por la Coordinación de Estrategia Digital Nacional (CEDN), define los entregables que las dependencias federales deberán hacer llegar a la propia CEDN a fin de que sea posible evaluar el nivel de implementación de IPv6 en la Administración Pública Federal.

La Guía señala que todas las dependencias federales deberán integrar un Grupo de Trabajo para IPv6 (GTIPv6) que será el interlocutor con el Comité de Supervisión para IPv6 de la CEDN.

Uno de los primeros entregables señalados en la Guía es la elaboración de un Plan de Transición Local que deberán generar las dependencias federales como parte de la implementación del protocolo IPv6.

Este Plan de Transición considera los hitos señalados en la guía emitida por la CEDN:

1. Publicación del Plan de Transición Local a IPv6.
2. Solicitud de los recursos de direccionamiento IPv6 a IAR México.
3. Implementación de un piloto de pruebas de IPv6.
4. Reporte de los resultados del piloto de pruebas.
5. Implementación gradual del protocolo IPv6.

Este documento también señala los procedimientos a implementar para lograr la transición a IPv6 en el CICESE:

- El programa de capacitación para el personal técnico,
- La definición de los escenarios de coexistencia y técnicas de transición,
- Las diversas políticas por implementar,
- Aspectos de Seguridad de la Información asociados a la transición,
- Aspectos operativos asociados a la transición,
- Equipamiento físico,
- Plan de direccionamiento IPv6,
- Escalabilidad y,
- Costos asociados.

Este documento se dará a conocer a la comunidad en general del CICESE y a petición expresa de la CEDN, se publicará en la página web institucional.

[1] Coordinación de Estrategia Digital Nacional. Enero 2022. Guía para la Transición al Protocolo de Internet versión 6 (IPv6) en la Administración Pública Federal. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/686219/Gui_a_IPv6_-_v1.pdf.

Todos los aspectos de implementación señalados en este documento son de carácter obligatorio para todos los activos de información de la Red-CICESE.

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

La transición hacia el uso del protocolo IPv6 es un tema de carácter técnico y para la mayoría de los usuarios del CICESE el proceso será transparente y no será disruptivo de ninguna de sus actividades.

No obstante, el GTIPv6 del CICESE reconoce la necesidad de crear recursos de información general dirigidos a usuarios con diferentes niveles de conocimiento técnico.

Campaña de Información para la comunidad CICESE

Con el objetivo de consolidar la información disponible hacia los usuarios en general, el GTIPv6 del CICESE y la Dirección de Telemática, publicarán el sitio de intranet https://www.cicese.edu.mx/ipv6. En este sitio se hospedarán los contenidos, datos y métricas relacionados a la implementación del protocolo IPv6 en el CICESE.

El GTIPv6 del CICESE generará una sección de Preguntas Frecuentes que también será publicada en el sitio. La información relativa a este sitio y a la transición en general, será dada a conocer a la comunidad del CICESE a través de una campaña de información basada en correos electrónicos informativos, así como mediante la publicación de carteles en cada uno de los edificios de los campus del Centro.

Capacitación para técnicos de apoyo y desarrolladores

Debido al carácter técnico de sus funciones, los técnicos de apoyo de las diferentes áreas del CICESE recibirán una capacitación específica y básica acerca de la transición hacia IPv6, las implicaciones que ésta tiene en el ofrecimiento de los servicios internos y, en general, en tareas básicas de soporte a usuarios[2]. Los desarrolladores de sistemas internos o aplicaciones del CICESE también serán incluidos en esta capacitación.

La asistencia a estas capacitaciones será de carácter obligatorio para los técnicos de apoyo y desarrolladores o administradores de sistemas internos o aplicaciones del CICESE.

Estas actividades se llevarán a cabo durante el primer trimestre del año 2023 en una fecha determinada por el GTIPv6 del CICESE y la cual se dará a conocer de manera posterior a la implementación del piloto de pruebas.

[2] Los técnicos de apoyo ofrecen el primer nivel de soporte hacia los usuarios en general.

Capacitación del personal técnico de la Dirección de Telemática

El GTIPv6 del CICESE también reconoce la necesidad de generar un conocimiento básico y homogéneo, en la plantilla de técnicos adscritos a la Dirección de Telemática, acerca de los cambios que representa en la operación de los servicios ofrecidos, el uso del protocolo IPv6.

El personal del Departamento de Redes será el encargado de preparar los contenidos correspondientes e impartir los cursos de capacitación a los técnicos de la Dirección de Telemática.

Los contenidos a desarrollarse tendrán por objetivo atender las necesidades de operación de IPv6 de la Red-CICESE y de los servicios y aplicaciones que hacen uso de ella. Por lo anterior, el carácter de dichos contenidos tendrá un nivel básico de entendimiento de temas como agotamiento del direccionamiento IPv4, IPv6 como solución a largo plazo, estructura de una dirección IPv6, subnetting básico para IPv6 y, además, aspectos específicos de la implementación del protocolo en la Red-CICESE.

Estos aspectos específicos de la implementación del protocolo IPv6 en el CICESE estarán orientados principalmente a la utilización del servicio de DNS y DHCPv6, a la actualización de los procesos internos que se requieren para la operación del Centro y a la Seguridad de la Información.

Se conformará un grupo de trabajo técnico con la participación de personal de los departamentos de Redes, Cómputo e Informática. Este grupo de trabajo deberá participar en actividades de formación en temas de IPv6, previo a fungir como capacitadores del resto del personal técnico de la Dirección de Telemática.

Lo anterior, con el objetivo de identificar áreas de oportunidad que deban ser cubiertas en las capacitaciones posteriores y, sobre todo, que requieran capacitación adicional a la que actualmente puede proveer el Departamento de Redes, o que sea requerida por los técnicos del propio Departamento de Redes.

El GTIPv6 del CICESE solicitará la asignación de recursos para capacitaciones específicas en IPv6 para algunos técnicos de la Dirección de Telemática, Lo anterior, con el objetivo de que estos puedan volverse formadores de formadores en función de las necesidades operativas del CICESE.

Escenarios de coexistencia de IPv4 e IPv6, Técnicas de transición y Políticas de Implementación

Para realizar una transición o lograr la coexistencia de los protocolos IPv4 e IPv6, se pueden utilizar diferentes técnicas basadas en:

- Utilización simultánea de ambos protocolos (Dual-Stack),
- Túneles para interconectar zonas que operan con protocolos diferentes y,
- Traducción de direcciones.

En todos sus campi, la Red-CICESE hace uso de manera exclusiva de direcciones IPv4 públicas, propias, pertenecientes a prefijos de Enrutamiento de Dominios Sin Clases (CIDR, por sus siglas en inglés). Dentro de la Red-CICESE no se enrutan paquetes que pertenezcan a segmentos privados de acuerdo con lo definido en el RFC 1918[3].

Lo anterior ha permitido que el CICESE no haya percibido en su operación los problemas resultantes del agotamiento de direcciones públicas IPv4 y por ello, la implementación del nuevo protocolo IPv6 parte de la premisa de que todos los equipos que actualmente pertenecen a la Red-CICESE conservarán su direccionamiento IPv4 en el futuro previsible.

Esta situación, aunada a que de forma nativa la mayoría de los Activos de Información Esenciales cuentan con soporte completo para IPv6 y, a que no se cuenta con equipos o aplicaciones que sean IPv6 only[4], permite definir que la técnica de transición más adecuada para implementarse en la Red-CICESE sea el uso de Dual-Stack.

Con el objetivo de evitar que durante la transición hacia el uso exclusivo de IPv6 en la Red-CICESE existan nodos IPv4 only[5] que queden aislados de los servicios de intranet e Internet, la Red-CICESE operará con la técnica Dual-Stack en el futuro previsible[6]; el Departamento de Redes del CICESE implementará mecanismos para evaluar el tráfico

[3] Los documentos RFC (Request for Comments) son publicados por el Grupo de Trabajo de Ingenieros de Internet (IETF, por sus siglas en inglés) y son los estándares de facto en la implementación de la pila de protocolos TCP/IP.

[4] Un equipo IPv6 only es aquel que por sus características, solo soporta el uso del protocolo IPv6 y le es imposible comunicarse con otros equipos haciendo uso del protocolo IPv4. Se asume la existencia en el Internet de equipos de reciente creación o aplicaciones de reciente desarrollo que estén orientadas a redes IPv6 y que no tienen compatibilidad hacia atrás con IPv4.

[5] Un equipo IPv4 only es aquel que por sus características, solo soporta el uso del protocolo IPv4 y le es imposible comunicarse con otros equipos haciendo uso del protocolo IPv6. Un equipo o aplicación que no soporte IPv6 es generalmente, un activo que se encuentra en el fin de su vida útil, en virtud de que el protocolo IPv6 es soportado desde hace más de diez años por los sistemas operativos más comunes, como Windows, MacOS y aquellos basados en Linux.

[6] No es posible definir a priori una fecha en la que IPv4 deje de ser utilizado, se asume que la coexistencia de ambos protocolos, IPv4 e IPv6, tendrá una duración de muchos años, quizás inclusive, décadas. Aunque se reconoce también, que conforme el uso de IPv6 se vaya extendiendo a nivel mundial, cada vez habrá menos conexiones entre nodos remotos a través de Internet haciendo uso de IPv4.

de ambos protocolos como una métrica de su utilización. Esto con la finalidad de poder determinar, en conjunto con el GTIPv6 del CICESE, el momento en el que se dejará de soportar el protocolo IPv4 en la Red-CICESE.

El GTIPv6 del CICESE reconoce que el uso de IPv6 en Internet permitirá solucionar los problemas de agotamiento de direcciones IPv4 actuales y por ello, a partir de la publicación de este documento en la web institucional, todos los equipos nuevos que se integren a la red y las aplicaciones que se desarrollen internamente en el CICESE en cualquiera de sus divisiones académicas o de apoyo, deberán soportar el protocolo IPv6 y operarán en modo Dual-Stack hasta que el GTIPv6 del CICESE, en conjunto con el Departamento de Redes, determinen algún cambio en la estrategia de implementación.

Los equipos y servicios de la Red-CICESE que sean IPv4 only deberán migrarse hacia nuevas infraestructuras que soporten IPv6.

La Red-CICESE soportará los equipos IPv4 only que no puedan ser migrados a nuevas infraestructuras hasta que el GTIPv6 del CICESE, en coordinación con la Dirección de Telemática, determinen la fecha del fin de soporte para este protocolo.

No es posible determinar a priori esta fecha y el GTIPv6 del CICESE no prevé que esto pueda suceder en el mediano o corto plazo.

Aparte de la técnica de Dual-Stack, la Red-CICESE no implementará algún otro mecanismo para soportar equipos IPv4 only.

Las aplicaciones, servidores y equipos que no se encuentren bajo la administración de la Dirección de Telemática del CICESE, y que formen parte de las consultas públicas que el Centro ofrece, deberán soportar IPv6 de manera nativa, por lo menos en sus Front Ends, antes de que finalice el año 2023.

Una vez publicado el Plan de Transición en la web institucional, los administradores de los activos mencionados en el párrafo anterior, serán notificados de dicho requerimiento con el fin de que puedan evaluar la capacidad de sus equipos y aplicaciones para soportar el protocolo IPv6. La implementación de la técnica Dual-Stack para estos activos se realizará después de la ejecución del piloto de pruebas y las capacitaciones al personal técnico del CICESE.

Todas las solicitudes de servicio o reportes de problemas asociados con la implementación de IPv6, deberán ser canalizadas a través de la Mesa de Servicio de la Dirección de Telemática.

Política de Seguridad de la Información para la transición al Protocolo IPv6 en el CICESE

La implementación del protocolo IPv6 en el CICESE, requiere tomar como base los esquemas de seguridad de información aplicados actualmente sobre el protocolo IPv4; contemplando políticas de confidencialidad, integridad y disponibilidad en los activos y procesos esenciales.

La implementación de IPv6 y sus consecuencias operativas se agregarán a los planes de contingencia de los diferentes servicios o activos. En ellos se definirá un plan de recuperación en caso de presentarse fallos en la disponibilidad de los servicios, o de eventos que atenten contra la seguridad de la información y de las comunicaciones del CICESE, al momento de implementar el protocolo IPv6.

En el proceso de transición hacia el nuevo protocolo IPv6, se revisará la seguridad de la información de las infraestructuras de Tecnologías de la Información (TI) y el nivel de impacto en servicios como: el Directorio Activo, el Sistema de Nombres de Dominio (DNS), el Correo Electrónico, el Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), el Servicio de enrutamiento, los Servicios de virtualización y centro de datos, los Servicios de aplicaciones y bases de datos, los Servicios Web y los Sistemas de Gestión y Monitoreo.

Los técnicos encargados de implementar el nuevo protocolo en los diferentes servicios que administran, generarán la documentación necesaria que contemple los aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surjan del proceso de implementación de IPv6.

Como parte del proceso de levantamiento de nuevos servicios o modificación de estos con soporte para IPv6, el área de Seguridad de la Información del CICESE realizará análisis de posibles riesgos de seguridad de la información (vulnerabilidades) en los servicios de la institución, los cuales puedan presentarse como consecuencia de la implementación del protocolo IPv6. Lo anterior en consideración a que múltiples protocolos como IPSec, HTTP, TCP, UDP o SIP, harán uso de IPv6 una vez que esté implementado.

La planeación del direccionamiento en IPv6 se realizará con base en los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones, permitiendo que el funcionamiento del direccionamiento sea transparente para los usuarios finales del CICESE.

La implementación de IPv6 se realizará de acuerdo con las mejores prácticas para separar el tráfico de red. Se crearán subredes específicas que se asignarán a las VLANs (Redes de Área Local Virtuales) existentes con propósitos de pruebas de direccionamiento, tráfico, monitoreo, seguridad y sistemas de producción.

Al igual que con IPv4, el protocolo IPv6 se implementará siguiendo las buenas prácticas de seguridad, aplicando segmentación lógica en zonas de la LAN y en los firewalls para

la infraestructura de Tecnologías de la Información y las Comunicaciones (TIC), con el objeto de garantizar una mayor protección en la red de comunicaciones que genere o transmita tráfico IPv6.

Se deberán disponer y fortalecer las capacidades del equipo de Seguridad de la Información del CICESE para verificar y monitorear los problemas de seguridad de información que surjan al momento de ejecutar las fases de implementación y pruebas de funcionalidad. El trabajo entre el área de Seguridad de la Información y las distintas áreas de TIC del CICESE para la implementación de IPv6, se realizará de manera conjunta.

EL GTIPv6 del CICESE en la medida de sus capacidades, gestionará presupuesto de inversión que permita fortalecer los niveles de seguridad en la red y servicios TIC sobre el protocolo IPv6, así como, el monitoreo preventivo, auditorías de seguridad y análisis de riesgos.

Política de sumarización de rutas externas

La sumarización de rutas es una técnica que se utiliza en enrutamiento cuyo objetivo principal es disminuir el consumo de memoria de acceso aleatorio (RAM, por sus siglas en inglés) en los enrutadores de Internet. La técnica consiste en representar a la mayor cantidad de redes o subredes posibles, con el prefijo más corto posible[7], reduciendo así, la cantidad de prefijos anunciados a los enrutadores vecinos.

De esta forma, un Proveedor de Servicios de Internet con 256 clientes, puede publicar un anuncio de una red con longitud de prefijo /16 en lugar de hacer 256 anuncios con una longitud de prefijo /24. Existen algunas condiciones especiales para poder realizar lo anterior, pero el concepto fundamental es como se ha descrito.

Dado que la sumarización de rutas es considerada una mejor práctica en el uso de la pila de protocolos TCP/IP, la Red-CICESE hará uso de esta técnica al momento de implementar IPv6.

La política de sumarización de rutas externas para IPv6 establecida en este documento es realizar la menor cantidad de anuncios de prefijos IPv6 hacia Internet en la sede y Unidades Foráneas del CICESE; el diseño del esquema de direccionamiento IPv6 ya considera este requerimiento.

[7] En enrutamiento, un prefijo es la cantidad de bits, leídos de izquierda a derecha, que no cambia en una dirección IP, para una red determinada. Un Proveedor de Servicios de Internet, podría proporcionar una dirección de red 200.200.240.0/20 a uno de sus clientes; el prefijo sería /20 e indica que los primeros 20 bits de todas las posibles direcciones IP de ese cliente, siempre van a ser los mismos.

Política de sumarización de rutas internas

El concepto de sumarización de rutas también puede (y debe) aplicarse a las redes que se propagan dentro de un Sistema Autónomo (AS, por sus siglas en inglés). Implementar esta sumarización reduce la carga de los enrutadores internos y simplifica la gestión de rutas.

Aunque es de esperarse que en las comunicaciones Intra-AS existan una mayor cantidad de rutas, más específicas que en las comunicaciones Inter-AS, se deberá planificar la implementación de IPv6 de tal forma que las subredes sean asignadas por zonas y que dichas asignaciones sean contiguas (en el sistema de numeración binario) para que puedan ser agregadas en la menor cantidad de prefijos posibles.

Cada enrutador de la red interna deberá entonces, realizar anuncios sumarizados de los prefijos que tiene directamente conectados en sus diferentes interfaces, promoviendo que los enrutadores más cercanos a la capa de acceso utilicen los prefijos más largos y que estos se vayan reduciendo en longitud conforme se aproximen al núcleo de la red.

Se deberá considerar también la usabilidad operativa del protocolo IPv6 en la Red-CICESE, de forma que sea lo más sencillo posible la identificación de las subredes IPv6 respecto a sus contrapartes IPv4 en el entorno de Dual-Stack. El Departamento de Redes evaluará el compromiso que exista entre ambos requerimientos y definirá la asignación correspondiente de subredes.

En el caso específico de los Centros de Datos, la sumarización de rutas internas al centro de datos per se, la realizarán los enrutadores de núcleo de centro de datos y estos realizarán los anuncios correspondientes al núcleo de LAN (acrónimo en inglés de Red de Área Local). De esta forma, los enrutadores de LAN propagarán la información de enrutamiento del Centro de Datos de forma sumarizada.

Política de enrutamiento BGP-4

La política de enrutamiento externo haciendo uso del protocolo BGP-4 se realizará considerando las políticas de sumarización descritas y el esquema de direccionamiento IPv6 definido.

Los enrutadores de frontera de la Red-CICESE se identificarán con una dirección IPv6 propia que será asignada en una interfaz loopback o una interfaz de gestión del equipo y con esa dirección realizarán el proceso de peering con sus vecinos.

Las políticas de enrutamiento de entrada y salida vigentes para IPv4 serán replicadas en IPv6 y se considerarán las mejores prácticas para tal fin.

La Red-CICESE se apegará a los principios y acciones de MANRS (Mutually Agreed Norms for Routing Security)[8].

Con el objetivo de evitar el envío o la recepción de tráfico basura, se establecerán filtros de prefijos de entrada y salida para filtrar los anuncios propios, y los prefijos de los clientes y de los peers de la Red-CICESE. También se implementarán filtros de prefijos bogon.

Se verificará que la información de enrutamiento IPv6 de los clientes de la Red-CICESE corresponda con sus prefijos registrados ante los repositorios públicos pertinentes.

El CICESE publicará en dichos repositorios públicos los prefijos asignados por IAR México a su AS. Esto con el objetivo de que los peers y clientes puedan validar la información de enrutamiento IPv6 que la Red-CICESE anunciará.

Política de enrutamiento interna

La política de enrutamiento interna se realizará considerando las políticas de sumarización descritas y el esquema de direccionamiento IPv6 definido.

La definición de zonas de la Red-CICESE utilizadas actualmente en IPv4, serán implementadas también en IPv6. Existirá un cambio significativo en el Centro de Datos del CICESE, el cual será consistente con el diseño de crecimiento de la red a mediano y largo plazo, y que considerará al Centro de Datos como una entidad de enrutamiento separada. Este cambio se verá reflejado en el esquema de direccionamiento IPv6 y permitirá al Centro de Datos contar con mayor flexibilidad en la asignación de subredes considerando el crecimiento a futuro.

Se implementará una versión compatible con IPv6 del protocolo de enrutamiento de gateway interior que actualmente se utiliza en la Red-CICESE. Se mantendrán las dos instancias de enrutamiento en todos los enrutadores de la red, hasta que el GTIPv6 del CICESE y Departamento de Redes indiquen un cambio en dicha política.

Se implementarán técnicas de autenticación entre los vecinos para la aceptación de actualizaciones de rutas de acuerdo con las mejores prácticas de enrutamiento de gateway interior.

[8] Las Normas Mutuamente Acordadas para la Seguridad de Enrutamiento es una iniciativa global que ayuda a reducir las amenazas más comunes en enrutamiento. Pueden ser consultadas en https://www.manrs.org.

Aplicaciones y equipos que deberán ser actualizados o sustituidos

Debido a que se implementará la técnica Dual-Stack en la Red-CICESE, los equipos y aplicaciones que no soporten IPv6 podrán seguir siendo alcanzados a través de IPv4.

Con base en la información de obsolescencia respecto al soporte de IPv6 en configuración, sistemas operativos y hardware, del inventario de Activos de Información Esenciales de la Red-CICESE, se determinó que se cuenta con muy pocos activos IPv4 only.

Se determinó también que todos los Activos de Información Esenciales que soportan IPv6, requieren actualización de sus configuraciones. Algunos de estos activos, requieren además de actualizaciones del sistema operativo, las cuales serán ejecutadas durante ventanas de mantenimiento programadas.

Todos los equipos de la Red-CICESE que son IPv4 only se encuentran en fin de vida, es decir, que son obsoletos y requieren ser sustituidos independientemente del soporte a IPv6. Se prevé que estos equipos serán sustituidos antes de que la Red-CICESE se convierta en una red IPv6 only. En cuanto a los equipos IPv4 only que actualmente brindan algún servicio contemplado para el despliegue del protocolo, se estima que estos equipos pueden ser sustituidos antes de que comience el piloto.

Por lo anterior, no se prevé que la transición hacia IPv6 haciendo uso de Dual-Stack tenga un impacto que afecte la operación de la Red-CICESE y los servicios que ésta soporta.

En la Red-CICESE se establecerá y difundirá la política de que los equipos y aplicaciones IPv4 only deberán ser migrados tan pronto como sea posible a infraestructura que sí soporte el nuevo protocolo. Cuando estos activos sean migrados, mantendrán su direccionamiento IPv4 anterior y contarán con direccionamiento IPv6, es decir, se integrarán al modelo Dual-Stack.

Estos equipos y aplicaciones se mantendrán en dicho modo de operación hasta que el Grupo de Trabajo para IPv6 del CICESE indique que se termina el soporte de IPv4 en la Red-CICESE.

Si existiesen equipos o aplicaciones IPv4 only que no puedan ser migrados a infraestructura que soporte IPv6, solo se podrán conectar a la Red-CICESE mientras continúe el uso de IPv4.

Identificación y planteamiento de atención a los potenciales riesgos de seguridad de la información asociados a la transición

Estrategias de Seguridad de la Información para IPv6

Las estrategias de seguridad mencionadas a continuación deberán ser implementadas en todos los campi del CICESE, es decir, en la sede principal y en las Unidades Foráneas.

El Área de Seguridad de la Información será la encargada de coordinar la implementación de estas estrategias en conjunto con las áreas correspondientes.

1. Seguridad perimetral y Zonas Desmilitarizadas

La Dirección de Telemática (DT) promoverá la implementación de políticas de seguridad de la información en IPv6 que permitan garantizar la disponibilidad, accesibilidad e integridad de los recursos de TIC, 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-CICESE, requiere ser validado y autorizado por los mecanismos de seguridad implantados por la DT, priorizando una política de seguridad de la información restrictiva para el tráfico IPv6 que requiera ingresar a la Red-CICESE.

La DT gestionará la seguridad en zonas desmilitarizadas para alojar servicios TIC públicos sobre IPv6 que estarán expuestos a riesgos de seguridad.

La DT proveerá sistemas de detección de intrusos para prevenir y detectar vulnerabilidades y ataques de seguridad de la información. Estos sistemas podrán detectar fugas de información cuya pérdida o difusión pudiese tener un impacto negativo para la institución.

El tráfico IPv6 generado en todos los nodos de la Red-CICESE será revisado por un sistema especializado para prevenir fuga de datos por conexión a sitios web y aplicaciones que contienen virus, malware, troyanos.

Será restringido el acceso a sitios web ajenos a las actividades sustantivas de la institución.

El correo electrónico entrante a cuentas del servicio @cicese.mx será revisado por un sistema automático especializado en la protección contra spam y virus informático.

2. Sistemas operativos.

La implementación de IPv6 en algunos sistemas operativos aún no se encuentra habilitada en todos sus módulos de funcionalidad, un ejemplo de ello son los sistemas operativos basados en Linux. Algunos ataques en la capa de enlace de datos son permitidos por la configuración por defecto de la pila TCP/IP en los sistemas Linux, como puede ser el uso de ICMPv6 para ataques de intermedio, etc. Es conveniente revisar los parámetros del kernel, para evitar este tipo de ataques.

3. VPN (Redes Privadas Virtuales).

Se deberán definir actividades que garanticen la seguridad del tráfico IPv6 de las comunicaciones a través de redes privadas virtuales. La Red-CICESE solo implementará VPNs basadas en IPSec.

Se deberán identificar riesgos de seguridad en el uso de VPNs sobre IPv6.

4. Monitoreo de IPv6.

Las actividades de monitoreo del tráfico IPv6 de la Red-CICESE permitirán la detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad. Se deberá contar con un plan de contingencias.

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 CICESE,
c) Las rutas que sigue el tráfico dirigido a Internet.

5. Análisis y gestión de riesgos en IPv6

En el proceso de transición a IPv6 se deberá realizar un análisis de riesgos que permita identificar a qué tipo de amenazas se encuentran expuestos los activos del CICESE y cuál es su nivel de riesgo e impacto. La transición a IPv6 se deberá integrar al proceso de gestión de riesgos existente para la Red-CICESE.

6. Análisis y explotación de vulnerabilidades en IPv6

El equipo de seguridad de la Información de CICESE analizará activamente las vulnerabilidades de los activos de información que surjan como consecuencia de la implementación de IPv6 en la Red-CICESE.

Una vez implementado el protocolo en el enrutamiento de gateway exterior, se deberán programar pruebas de penetración de IPv6 hacia la Red-CICESE desde el exterior en busca de vulnerabilidades que deban ser corregidas.

Identificación y solución a los efectos operativos en las aplicaciones y redes por la transición

Aunque el diseño de la transición se ha realizado en apego a los estándares y buenas prácticas, se espera que se presenten desafíos técnicos durante la implementación del protocolo IPv6. Por lo anterior, se ejecutará un plan de seguimiento a problemas operativos encontrados en aplicaciones y redes durante la transición a IPv6.

Los administradores de red y de servicios de cómputo e informática, así como los usuarios de la Red-CICESE en general, podrán utilizar la Mesa de Servicios de la Dirección de Telemática para reportar problemas generados con la implementación del protocolo.

El proceso seguido en la Mesa de Servicios asigna un identificador a cada reporte o solicitud y es posible involucrar a otras áreas o técnicos de la Dirección de Telemática que estén relacionadas con el reporte en cuestión.

Este sistema permitirá identificar, registrar y gestionar los problemas encontrados durante la implementación del protocolo IPv6 y permitirá generar guías internas de buenas prácticas para la mejora continua del servicio.

La implementación de la técnica Dual-Stack trae de manera inherente una duplicidad en la carga de trabajo para la gestión de la red. Por tal motivo será importante el apagar el soporte para IPv4 en cuanto sea posible. Esto es, una vez que todos los servicios, aplicaciones y clientes de la Red-CICESE operen en IPv6 y sin dejar de tomar en cuenta la oferta de servicios de Internet basados en IPv4.

Plan de direccionamiento IPv6

El plan de direccionamiento IPv6 empatará las subredes que existen actualmente en IPv4 con sus nuevas asignaciones IPv6. Lo anterior con el propósito de que visualizar las nuevas subredes sea lo más transparente posible para los administradores y usuarios finales que ya estén familiarizados con el esquema utilizado en IPv4.

En términos generales, el esquema de direccionamiento de IPv6 es similar al utilizado en IPv4 (Red-Subred-Host). En IPv6 el diseño incluye el Global Routing Prefix, asignado por el ISP, el prefijo de subred (subnet prefix) y el identificador de interfaz (interface ID).

Para la Red-CICESE se propone utilizar un esquema de direccionamiento de 4 jerarquías, subdividiendo el subnet prefix en dos partes. La primera parte identificará a los sitios o centros de datos, y la segunda a las subredes contenidas en cada sitio. El interface ID tendrá una longitud de 64 bits, excepto en lo señalado por el RFC 6164.

A cada subred se le asignará una dirección para la puerta de enlace predeterminada y se ofrecerán tanto el servicio de DHCPv6 como el de asignación estática de direcciones IPv6.

El diseño del plan de direccionamiento, e inclusive su implementación, se pueden realizar aún sin tener un prefijo asignado por IAR México a través del uso de direcciones Unique Local. Cuando se cuente con el Global Routing Prefix asignado por IAR México, solo se requerirá modificar los primeros bits de la dirección IPv6, correspondientes al Global Routing Prefix e identificador de sitio.

Proyecciones de escalabilidad del Plan de Transición Local a IPv6

El Plan de Transición Local a IPv6 descrito en este documento contempla múltiples acciones que deberán ser ejecutadas en una línea de tiempo acorde a los hitos señalados en la Guía publicada por la CEDN.

No obstante, existen metas que no están previstas en dicho documento guía y que, como se ha mencionado anteriormente, no es posible asignarles una fecha determinada. Lo anterior debido al carácter variable de la implementación de IPv6 a nivel global y la obsolescencia de IPv4.

Tomando esto en consideración, se prevé que el GTIPv6 continuará realizando sus funciones de enlace con la CEDN en atención a las nuevas normativas y disposiciones que devengan, modificando las acciones descritas en este plan de acuerdo con las necesidades correspondientes.

Se considera que cuando se alcance el hito de contar con 80% de los activos de red operando de manera nativa en IPv6 en la Red-CICESE (segundo semestre de 2025), las actividades del GTIPv6 del CICESE en coordinación con el Departamento de Redes, estarán enfocadas mayormente a la evaluación del uso de IPv4. Lo anterior con propósitos de determinar la fecha de la suspensión del soporte de dicho protocolo o, en su defecto, la implementación de acciones para mantener comunicación con equipos IPv4 obsoletos fuera de la Red-CICESE.

El GTIPv6 y la Dirección de Telemática también evaluarán la pertinencia de mantener activos los recursos destinados a las métricas de uso de IPv6 que se hayan dispuesto y en general, a los recursos destinados a la transición de IPv4 a IPv6.

A menos de que exista un señalamiento o indicación diferente por parte de la CEDN, el GTIPv6 del CICESE determinará el momento en el que dejará de estar activo, y sus actividades y responsabilidades sean trasladadas a la Dirección de Telemática del CICESE.

Programa de costos y acciones administrativas asociados con la transición

La transición hacia el uso de IPv6 en las redes puede ser considerada como un proceso de actualización de los activos de información de las organizaciones. Principalmente, si se tiene en cuenta que puede conllevar cambios en software y hardware y actualizaciones de políticas y procesos.

En todas las organizaciones estos cambios y actualizaciones tienen costos asociados que incluyen, pero no están limitados a:

- Capacitación,
- Adquisición de material de apoyo,
- Tiempo que el personal dedica a diseñar y prepararse técnicamente para los cambios,
- Tiempo dedicado en la implantación de los cambios,
- Actualización de la documentación de los procesos involucrados,
- Identificación de limitantes de hardware y software,
- Adquisición o actualización de activos de información,
- Servicios externos asociados,
- Elaboración de materiales de difusión y capacitación interna.

Las organizaciones que, como el CICESE, ya cuentan con procesos establecidos de mejora continua, pueden absorber dentro de su operación la mayoría de los costos descritos previamente.

Para ejecutar la transición a IPv6 en la Red-CICESE, el GTIPv6 ha identificado y estimado los costos correspondientes.

Se debe observar que se ha reconocido la posibilidad de que existan gastos de implementación adicionales que no pueden ser cuantificados en esta etapa. Esto último es principalmente, en lo relativo a actualización de hardware que algunos activos de información esenciales puedan requerir una vez que haya iniciado la transición a IPv6.

Se debe señalar que el costo de renovación de la asignación de direcciones IPv6 señalado se tendría que ejercer hasta el año 2023.

Los recursos de Internet (direcciones IPv4, direcciones IPv6, números de Sistema Autónomo) son administrados por organizaciones sin fines de lucro, dependientes de organismos internacionales, que cobran cuotas por la asignación y mantenimiento de dichos recursos. Existen cuotas de asignación inicial y renovación.

Los costos asociados a cursos de capacitación y material bibliográfico están orientados a la preparación del personal técnico de la Dirección de Telemática del CICESE asignado directamente a la implementación de IPv6 que, como ya se mencionó en secciones anteriores de este documento, fungirán como formadores de formadores para el resto del personal técnico del Centro.

Para la elaboración y diseño de materiales de difusión se hará uso de los recursos internos del CICESE y no se prevé que existan gastos que no puedan ser cubiertos por la propia operación de la institución. El GTIPv6 del CICESE en el marco de sus atribuciones, realizará las gestiones necesarias con las áreas correspondientes para asegurar la asignación de los recursos internos que apliquen.

El GTIPv6 reconoce la necesidad de monitorear el desempeño de todos los activos de información esenciales principalmente, en términos de consumo de Memoria de Acceso Aleatorio y Unidades de Procesamiento Centrales, de manera posterior a la implementación de IPv6 en la Red-CICESE y con el objetivo de identificar oportunamente aquellos activos que requieran ser actualizados como consecuencia del uso de la técnica Dual-Stack.