**ANEXO 2A REQUERIMIENTO TÉCNICO**

**SERVICIOS DE RED privada VIRTUAL de la**

**suprema corte DE JUSTICIA DE LA NACIÓN**

Contenido

[INTRODUCCIÓN 3](#_Toc486247497)

[1. DEFINICIÓN DEL PROYECTO 3](#_Toc486247498)

[2. OBJETIVOS 4](#_Toc486247499)

[3. REQUERIMIENTOS GENERALES 4](#_Toc486247500)

[4. REQUISITOS PARA LA PROPUESTA TÉCNICA. 6](#_Toc486247501)

[5. REQUERIMIENTO TÉCNICOS DE LOS SERVICIOS 7](#_Toc486247502)

[6. REQUERIMIENTOS GENERALES DEL SERVICIO DE INTERNET 12](#_Toc486247508)

[7. SERVICIOS DE SEGURIDAD INFORMÁTICA 14](#_Toc486247513)

[8. SERVICIOS DE VIDEOCONFERENCIA 16](#_Toc486247515)

[9. SERVICIOS DE TELEFONÍA IP / TARIFICACIÓN 21](#_Toc486247526)

[10. SERVICIOS DE RED LAN EXTENDIDA 29](#_Toc486247542)

[11. SERVICIOS DE RED INALÁMBRICA PARA CASAS DE LA CULTURA 32](#_Toc486247544)

[12. PUNTOS DE CONSOLIDACIÓN DE INFRAESTRUCTURA Y SERVICIOS 35](#_Toc486247547)

[13. INFRAESTRUCTURA AUXILIAR PARA LOS SERVICIOS 36](#_Toc486247549)

[14. SERVICIOS ADMINISTRADOS DE RED Y SEGURIDAD 39](#_Toc486247550)

[15. NIVELES DE SERVICIO PARA LOS SERVICIOS SOLICITADOS 47](#_Toc486247559)

[16. INSTALACIÓN DEL SERVICIO 48](#_Toc486247560)

[17. MANTENIMIENTO CORRECTIVO Y PREVENTIVO 49](#_Toc486247561)

# INTRODUCCIÓN

La Suprema Corte de Justicia de la Nación cuenta a nivel nacional con edificios jurídicos y administrativos, centros de datos, centros de información (Casas de la Cultura Jurídica) y librerías, mediante los cuales se da acceso a servidores públicos y público en general a la información jurídica y administrativa generada por este Alto Tribunal.

Con la finalidad de proveer los servicios de comunicación, seguridad, telefonía, videoconferencia, red inalámbrica, servicios de internet y de intercambio de información para cada una de estas localidades, la SCJN requiere de contar con un servicio integral de una Red Privada Virtual mediante la tecnología MPLS-VPN (Multiprotocol Label Switching)

Para la presente solución se han definido 6 tipificaciones de los sitios que integran la red de la SCJN, los cuales son:

* Sitios Tipo 1: Son los inmuebles principales de la SCJN, donde se requiere una infraestructura de comunicaciones de alta disponibilidad y con un esquema redundante.
* Sitios Tipo 2: Son aquellos donde se requiere una infraestructura de comunicaciones de alta disponibilidad con un esquema redundante, porque cuentan con un centro de datos de la SCJN.
* Sitios Tipo 3: Son aquellos donde la conexión hacia este tipo de sitios será a través de un enlace único no redundante, para las Casas de la Cultura Jurídica.
* Sitios Tipo 4: Son aquellos donde la conexión hacia este tipo de sitios será a través de un enlace único no redundante, para librerías, almacén y SEDE Histórica de la SCJN.
* Sitios Tipo 5: Son aquellos donde la conexión hacia este tipo de sitios, será a través de un enlace único no redundante, con capacidad de ancho de banda media.
* Sitios Tipo 6: Son aquellos donde la conexión hacia este tipo de sitios, será a través de un enlace único no redundante, con capacidad de ancho de banda baja.

# DEFINICIÓN DEL PROYECTO

La Suprema Corte de Justicia de la Nación, a fin de satisfacer su necesidad de proveer los servicios informáticos requeridos en cada uno de sus inmuebles, así como permitir la interconexión entre los mismos, en un ambiente que garantice la correcta comunicación y seguridad del medio, requiere de la contratación de una Red Privada con tecnología MPLS-VPN, la cual será denominada como Red Privada Virtual de la Suprema Corte de Justicia de la Nación.

El proyecto tendrá un periodo de contratación de 36 meses y se requiere que sus servicios estén completamente instalados a más tardar el 31 de marzo de 2018 y comenzarán a operar a partir de las 0:00 horas del 1 de mayo de 2018, la migración de los servicios se debe realizar en coordinación con el actual prestador del servicio CFE Telecomm.

Todo equipo, licenciamiento, accesorios y servicios que sean requeridos para la puesta en operación de la Red Privada Virtual, serán totalmente responsabilidad del prestador de servicios, debiendo considerar la administración, gestión de configuraciones, mantenimiento y servicios profesionales que sean requeridos por la SCJN durante la prestación del servicio.

# OBJETIVOS

* Proveer un servicio integral de telecomunicaciones y de seguridad informática, que permita brindar disponibilidad, integridad y confidencialidad a la comunicación y servicios que integran al proyecto de la Red Privada Virtual de la Suprema Corte de Justicia de la Nación.
* Interconectar los edificios del área metropolitana, librerías y Casas de la Cultura Jurídica a nivel nacional de la Suprema Corte de Justicia de la Nación.
* Proveer a cada uno de los inmuebles de la SCJN, con los servicios de comunicación, seguridad, telefonía, videoconferencia, red inalámbrica, servicios de internet y de intercambio de información, de acuerdo sus necesidades.
* Mejorar el desempeño de los recursos de comunicaciones en disponibilidad, tiempos de respuesta, uso de ancho de banda y priorización de aplicaciones.
* Que el proyecto de la Red Privada Virtual de la Suprema Corte de Justicia de la Nación permita eficiencia en la operación y en el uso de servicios informáticos en la SCJN, mediante el uso de esquemas de comunicación con calidad de Servicio, aseguramiento de la continuidad del servicio, y manteniendo un servicio operativo las 24 horas del día, los 365 días del año por la vigencia del contrato.

# REQUERIMIENTOS GENERALES

La Suprema Corte de Justicia de la Nación, requiere explícitamente de los servicios de RED RPV - MPLS e INTERNET para interconectar todos los domicilios de la misma dependencia integrando servicios de red LAN, red inalámbrica (WLAN), telefonía IP, videoconferencia y seguridad.

La SCJN requiere los servicios administrados de interconexión entre sus diversos inmuebles localizados a lo largo de la República Mexicana, usando para ello enlaces con tecnología MPLS-VPN para el manejo y optimización de tráfico. Aunado a ello, se requieren servicios de acceso a Internet mediante enlaces dedicados, con los niveles de ocupación y disponibilidad que aseguren un eficiente servicio.

Para lo cual, los servicios solicitados dentro del proyecto de Red Privada Virtual de la Suprema Corte de Justicia de la Nación son:

* Canales de Comunicación.
* Datos.
* Telefonía.
* Red Inalámbrica.
* Videoconferencia.
* Canales de acceso a Internet para las Casas de la Cultura Jurídica.
* Centro de Operaciones de Red (NOC).
* Centro de Operaciones de Seguridad (SOC).

Cada uno de los servicios requeridos se dividen en tres rubros o conceptos básicos, lo anterior con el fin de especificar los requerimientos puntuales de cada servicio:

* Instalación.
* Operación y Monitoreo.
* Soporte.

Se requiere considerar los equipos necesarios para los servicios requeridos, en al menos dos puntos de consolidación de infraestructura y servicios, para contar con un esquema de alta disponibilidad, los cuales son propiedad y responsabilidad del prestador de servicios

El prestador de servicios debe considerar que los sitios donde se implementarán estos servicios, son descritos en el **Apartado 1**, debiendo garantizar los niveles de servicio solicitados por la institución.

El Centro de Operaciones de Red deberá de contar con los recursos, herramientas y metodologías de administración y gestión de forma centralizada. Los servicios requeridos en este concepto son:

* Una Mesa de Servicios Operativos, que será la encargada de proporcionar el punto único de contacto para la atención de solicitudes y problemas en la operación de los Servicios. Además, se encargará operativamente de coordinar y dar seguimiento a los cambios de domicilio, nuevos nodos solicitados y la cancelación de los mismos.
* Un servicio de Monitoreo Proactivo, que recolectará los indicadores de la operación y niveles de servicios de los diferentes componentes de la Red, con la finalidad de verificar el cumplimiento del grado de servicios solicitado en el presente proyecto, detectando y permitiendo corregir en forma anticipada problemas operativos.
* Un servicio de análisis de redes, que realizará la recolección y posterior análisis del comportamiento del tráfico que circula por cada uno de los sitios de la Red, con la finalidad de realizar mejoras operativas.

El Centro de Operaciones de Seguridad (SOC) deberá de contar con los recursos, herramientas y metodologías de administración y gestión de forma centralizada y basados en el estándar de seguridad de la información ISO 27000. Los servicios requeridos en este concepto son:

* El SOC del prestador de servicios se encargará del monitoreo, identificación, análisis, registro y resolución de cualquier incidente en materia de seguridad informática que pudieran suscitarse en el servicio de la Red Privada Virtual de la SCJN.
* El SOC del prestador de servicios deberá estar conformado por personal altamente capacitado en las distintas ramas de seguridad informática, análisis forense, telecomunicaciones, auditoria informática, así como atención y respuesta a incidentes.
* El SOC del prestador de servicios deberá contar con las herramientas especializadas de hardware y software necesarias para atender cualquier incidente de seguridad informática que pudiera suscitarse en el servicio de la Red Privada Virtual de la SCJN, entre las cuales se pueden mencionar las siguientes: correlacionador de eventos, escáner para análisis de flujos de red, herramientas de análisis forense, herramientas para análisis de logs, herramientas para análisis de malware, etc.

Todos los equipos proporcionados para la prestación deberán ser resguardados en un gabinete o rack provisto por el participante en cada locación de la SCJN, mediante el cual solo personal autorizado de la SCJN y del prestador de servicios tendrán acceso.

Se deberán considerar 3 cambios de domicilio, dentro de la misma ciudad, sin costo adicional para la SCJN, que se puedan aplicar en los sitios Tipo 3, 4, 5 y 6, durante la vigencia del contrato.

Se deberán considerar 5 reubicaciones de servicios, incluyendo los enlaces dentro de los domicilios sin costo adicional para la SCJN, para todos los sitios, durante la vigencia del contrato.

# REQUISITOS PARA LA PROPUESTA TÉCNICA.

* Se deberá entregar toda la documentación de la propuesta técnica en español o en el idioma original del documento, con traducción simple al español de las partes que respalden la propuesta, incluyendo: certificaciones técnicas, diplomas, documentación técnica, folletería, etc.
* Deberá presentar documentación de al menos 2 ingenieros o licenciados en las áreas de comunicaciones, electrónica, informática o carrera a fin, con certificación vigente para cada una de las soluciones de conectividad, red LAN, telefonía, videoconferencia, red inalámbrica y acceso a Internet que proponga, así como copia de la documentación que avale su último grado de estudios.
* Para el Servicio de Centro de Operaciones de Seguridad (SOC), se deberá presentar Certificados o documento de capacitación que avale que el personal (al menos una persona) que se encargará de prestar el servicio esté capacitado en alguno de los siguientes perfiles: ISO 27001/ CISSP (Certified Information Systems Security Professional) / ENSA (Network Security Administrator)/ ECSA (Certified Security Analyst) / CHFI (Hacking Forensic Investigator) / ECSS (Certified Security Specialist) o similares.
* El Servicio de Centro de Operaciones de Seguridad (SOC) del participante, deberá acreditar que cuenta con la certificación del ISO 27001 en alguno de sus procesos internos.
* Todo el equipamiento propuesto deberá ser nuevo y original, en todas y cada una de sus partes.
* Deberá contar con los permisos necesarios para la prestación de los servicios telecomunicaciones solicitados por la autoridad correspondiente, para lo cual se deberá acreditar este requisito a través de copia simple de la concesión o permiso correspondiente.
* El prestador de servicios deberá acreditar su experiencia en la implementación y operación, presentando 2 contratos similares en los últimos 3 años, con al menos 30 sitios a nivel nacional, basado en dispersión (número de sitios a nivel nacional donde se prestó el servicio), servicios prestados (mínimo conectividad, telefonía y videoconferencia), volumen (número de usuarios atendidos) y niveles de servicio, con clientes en la República Mexicana, pudiendo omitir aquella información que sea considerada como confidencial. La información requerida es:

1. Nombre del Cliente.
2. Nombre del proyecto.
3. Número de contrato.
4. Datos de un contacto.
   * + 1. Nombre
       2. Domicilio
       3. Teléfono
5. Descripción del proyecto llevado a cabo.
   * + 1. Periodo de contratación.
       2. Implantación:
6. Fecha de inicio
7. Fecha de conclusión
   * + 1. Lista de sitios por proyecto implantados incluyendo: nombre del contacto, domicilio, ancho de banda contratado.
       2. Cantidad de usuarios atendidos por proyecto, dando el total de usuarios por sitio y por el proyecto.
       3. Tecnología de red dorsal utilizada.
       4. Tecnología de red de acceso local utilizada en forma general para todos los sitios.
       5. Estándares y recomendaciones que se cumplen en el diseño.
       6. Servicios que se entregan (datos, voz, videoconferencia e internet).
       7. Niveles de servicios que se cumplen en la entrega.
       8. Criterios de diseño para el cumplimiento de los niveles de servicio en los tramos de la red dorsal y en la red de acceso local
       9. Descripción de los mecanismos de administración y gestión de los niveles de servicio e indicadores de la operación.

# REQUERIMIENTO TÉCNICOS DE LOS SERVICIOS

# SERVICIOS DE ENLACES DEDICADOS MPLS E INTERNET

La SCJN requiere de la implementación de un servicio de Red Privada Virtual (VPN, Virtual Private Network) compuesta por enlaces de telecomunicaciones dedicados de tipo simétrico, operando tanto en el sitio central de la SCJN como en sus sitios remotos y centros de datos, de acuerdo a lo establecido en el **Apartado 1**, donde se indica el ancho de banda requerido para cada servicio, considerando la utilización del medio para cursar el tráfico en forma simultánea tanto de entrada como de salida. Los sitios de la SCJN deberán ser conectados a través del mecanismo de transporte de datos MPLS (Multiprotocol Label Switching, por sus siglas en inglés), para tráfico de voz, datos y video con calidad de servicio (QoS) predefinida, vía el protocolo IP, obteniendo la misma funcionalidad de seguridad y desempeño que se tiene en una red privada.

La red deberá cumplir con los estándares RFC 4364 y RFC 3031 de operación y arquitectura de MPLS y su núcleo deberá operar mediante el protocolo IP, y deberá estar soportada a través de una infraestructura de telecomunicaciones con plataforma de capa 2 y 3 MPLS, con acceso a la nube de MPLS a través de comunicaciones punto a punto.

La solución deberá soportar la comunicación tipo malla completa (FULL-MESH) que permita la transmisión de voz, datos y video desde el sitio principal con la red del prestador de servicios.

Deberá ser escalable, es decir, tener la flexibilidad, eficiencia, y transparencia suficiente para que en el momento que sea necesario se puedan agregar nuevos servicios, nodos de red, o ampliar los anchos de banda, sin afectar la operación de la red misma o la operación de los demás nodos.

El prestador de servicios proporcionará, administrará, monitoreará y controlará los enlaces de comunicaciones y los equipos CPE propios del servicio, de igual manera, el prestador de servicios mantendrá un monitoreo proactivo para detectar cualquier evento que pudiera ocasionar una interrupción o degradación que impacte en el desempeño de las aplicaciones.

# REQUERIMIENTOS ESPECÍFICOS PARA LOS SERVICIOS DE LOS ENLACES RPV-MPLS

El tráfico de voz, datos y video deberá ser etiquetado dentro de la MPLS con las siguientes calidades de servicio:

* Servicios de video: comunicación en tiempo real, utilizando protocolo RTP y los puertos TCP y UDP.
* Servicio de voz: comunicación en tiempo real, utilizando protocolo RTP y los puertos TCP y UDP.
* Datos normales: comunicación en tiempo no real con baja tasa de errores.
* Datos críticos: comunicación en tiempo real con baja tasas de errores.
* Datos de mejor esfuerzo: Comunicación en tiempo no real, con baja tasa de errores y sin especificar limitaciones temporales.

La calidad de servicio de orden superior deberá tener una prioridad mayor sobre las de orden inferior y la QoS asignada al tráfico se mantendrá de extremo a extremo en toda la trayectoria del paquete CPE-VPN/MPLS-CPE. El ancho de banda del enlace podrá ser empleado dinámicamente por cualquier tipo de aplicación dentro de su prioridad definida.

El prestador del servicio deberá proporcionar en el sitio el medio físico de acceso simétrico (enlace) y el equipo de ruteo (CPE) necesario para conectar cada localidad a la Red Privada Virtual (VPN-MPLS).

Se requiere que la solución garantice la privacidad de datos la red MPLS proporcionando encripción, misma que deberá realizar tanto en el nodo Central como en los nodos remotos. La tecnología requerida para esta funcionalidad deberá ser “tunnel-less (sin túnel)”.

Para el servicio de Internet, el punto de demarcación será el puerto Ethernet de red de área local (LAN) en el equipo CPE que será proporcionado por el prestador de servicios.

# CARACTERÍSTICAS TÉCNICAS DE LOS SERVICIOS DE LOS ENLACES MPLS

En la siguiente tabla se especifican los anchos de banda requeridos para cada sitio.

|  |  |  |
| --- | --- | --- |
| **Tabla de enlaces MPLS** | | |
| **Sitio** | **BW (Mbps)** | **Descripción** |
| Tipo 1 | 1000 | Enlace de 1 Gbps en Fibra Óptica y Enlace de 500 Mbps configurados en alta disponibilidad (Activo – Pasivo). |
| Tipo 2 | 1000 | Enlace de 1 Gbps en Fibra Óptica y Enlace de 500 Mbps configurados en alta disponibilidad (Activo – Pasivo). |
| Tipo 3 | 20 | Enlace de 20 Mbps en Fibra Óptica. |
| Tipo 4 | 10 | Enlace de 10 Mbps en Fibra Óptica. |
| Tipo 5 | 400 | Enlace de 400 Mbps en Fibra Óptica. |
| Tipo 6 | 100 | Enlace de 100 Mbps en Fibra Óptica. |
| Consolidación | 1000 | Enlace de 1 Gbps en Fibra Óptica. |
| Consolidación | 1000 | Enlace de 1 Gbps en Fibra Óptica. |

# DESCRIPCIÓN DEL SERVICIO DE RPV MPLS DE ACUERDO AL SITIO

El servicio de MPLS está asociado al tipo de sitio indicado anteriormente.

**Para los sitios Tipo 1 y Tipo 2.**

* Sitios: SEDE SCJN,16 de Septiembre y Casa de la Cultura Jurídica Guadalajara.
* Sitios con un ancho de banda de 1Gbps.
* El prestador de servicios deberá considerar en su diseño proporcionar el servicio mediante dos enlaces, un principal con capacidad de 1 Gbps y uno de respaldo con capacidad de 500 Mbps, en modalidad activo-pasivo.
* El enlace principal y el enlace de respaldo deberán ser proporcionados por rutas, centrales diferentes y equipo router (CPE) diferente.
* El medio de acceso deberá ser en FO para el enlace principal.
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.99%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 12.50% | 25.00% | 25.00% | 25.00% |

* El prestador de servicios deberá proporcionar un diagrama de conectividad donde se presente lo solicitado por cada sitio.

**Para los sitios tipo 3**

* Sitios : 44 Casa de la Cultura Jurídica
* Sitios con un ancho de banda de 20 Mbps.
* El medio de acceso deberá ser en FO.
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.92%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 12.50% | 25.00% | 25.00% | 25.00% |

**Para los sitios tipo 4**

* Sitios: 3 Librerías, 1 Almacén y SEDE Histórica.
* Sitios con un ancho de banda de 10 Mbps.
* El medio de acceso deberá ser en FO.
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.92%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 25.00% | 12.50% | 25.00% | 25.00% |

**Para los sitios tipo 5**

* Sitios: SEDE CJF y Revolución.
* Sitios con un ancho de banda de 400 Mbps.
* El medio de acceso deberá ser en FO
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.92%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 25.00% | 12.50% | 25.00% | 25.00% |

**Para los sitios tipo 6**

* Sitios: CENDI, Canal Judicial, CAJ Toluca y Tribunal Electoral.
* Sitios con un ancho de banda de 100 Mbps.
* El medio de acceso deberá ser en FO
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.92%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 25.00% | 12.50% | 25.00% | 25.00% |

**Para los puntos de consolidación de infraestructura y servicios, del prestador de los mismos**

* Sitios : Principal y Secundario
* Sitios con un ancho de banda de 1Gbps.
* El prestador de servicios deberá garantizar la disponibilidad de los servicios por redundancia en sitios.
* El medio de acceso deberá ser en FO.
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.99%
* El perfil requerido de calidad de servicio para este tipo de sitios es el siguiente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PORCENTAJES POR QoS** | | | | |
| Libre | Institucionales | Datos Críticos | Video | Voz |
| 12.50% | 25.00% | 12.50% | 25.00% | 25.00% |

La interconexión de los edificios Sede SCJN, 16 de Septiembre, Revolución, Guadalajara, Canal Judicial y Sede CJF el prestador de servicios deberá entregar los servicios solicitados para interconectarlos con los equipos de seguridad perimetral existentes los cuales son administrados por el personal de la Suprema Corte de Justicia de la Nación o del Consejo de la Judicatura Federal, por lo que deberán proporcionar todo el cableado certificado, en su caso FO con sus correspondientes GIBICS para su interconexión, conectorización, etiquetado y todo lo necesario para su funcionamiento, así como sujetarse a las políticas de seguridad informática de la SCJN.

# DESCRIPCIÓN DEL CPE DEL SERVICIO DE RPV MPLS

El equipo CPE deberá de ser nuevo de última generación y sin anuncio de fin de venta por el fabricante.

Los equipos CPE deberán de contar con soporte en sistema operativo, refacciones y componentes durante la vigencia del contrato.

El prestador de servicios deberá incluir en su propuesta un listado de los equipos que integran su solución, indicando la marca, el modelo, características de cada uno de ellos así como los documentos técnicos (folletos ó manuales solo de las hojas donde se menciona la característica solicitada en idioma español ó en inglés) de los equipos considerados. Además, deberá incluir diagramas con el diseño propuesto en donde se identifique en forma clara y detallada el diseño de la solución.

Las características de los CPE a proporcionar por el prestador de servicios, deberán de al menos contar con lo siguiente:

Para los sitios tipo 1, 2 y Puntos de Consolidación.

* Memoria DRAM de 4GB
* 6 puertos Gigabit Ethernet Small Form-Factor (SFP) de los cuales 2 SFP sean en FO.
* 2 SFP RJ-45
* Fuente de poder redundante.

Para los sitios Tipo 3, 4, 5 y 6.

* Puertos WAN o LAN 10/100/1000: 2, de los cuales 2 sean basados en RJ-45 y 1 tenga capacidad de SPF.
* Memoria DRAM de 4GB
* Flash Memory 4GB

Todos los equipos CPE que forman parte del proyecto deberán ser de la misma marca.

# REQUERIMIENTOS GENERALES DEL SERVICIO DE INTERNET

La SCJN requiere de un servicio de acceso a Internet mediante enlaces dedicados para brindar acceso a Internet a sus usuarios. El prestador de servicios deberá considerar un servicio en alta disponibilidad en su Backbone para garantizar el funcionamiento de conexión a internet.

Con el fin de asegurar la redundancia de rutas hacia la red mundial de Internet, el prestador de servicios deberá contar con al menos 2 diferentes accesos al Tier-1 de los Estados Unidos de América en 2 ciudades distintas del territorio nacional que sumen al menos 50 Gbps y con capacidad de poder cambiar de forma automática las rutas de acceso al backbone internacional en caso de falla. El prestador de servicios debe de contar con enlaces hacia Internet a nivel (Tier-1) con los que bridará el servicio a la SCJN.

El prestador de servicios deberá contar con acuerdos de Peering con los proveedores con mayor tráfico de Internet en México (al menos 2), con la finalidad de optimizar el intercambio de tráfico entre los distintos proveedores de internet, mismos que se deberán encontrar en diferentes zonas geográficas.

La red del servicio de acceso a Internet del prestador de servicio deberá estar diseñada de tal manera que el transporte de los paquetes sea de una manera eficiente, además debe contar con la redundancia necesaria que le permita ofrecer un alta disponibilidad en su Backbone.

# REQUERIMIENTOS ESPECÍFICOS PARA EL SERVICIO DE ACCESO A INTERNET

* Las direcciones IP configuradas en las interfaces de los equipos CPE de internet serán responsabilidad del prestador del servicio.
* La red del prestador de servicios deberá estar lista para operar en IPv6 en caso que la SCJN lo requiera.
* El prestador de servicios deberá entregar los servicios en condiciones 100% operativas, de acuerdo con las especificaciones técnicas solicitadas.
* Para el servicio de Internet, el punto de demarcación será el puerto de red de área local (LAN) en el equipo CPE que será proporcionado por el prestador de servicios.
* El prestador de servicios deberá considerar en sus servicios una solución de protección que garantice que el tráfico de internet es filtrado y limpiado de ataques de DDos. El servicio deberá ser proporcionado mediante un applience de uso dedicado para la SCJN o a través de una solución en nube que garantice el servicio solicitado.

# CARACTERÍSTICAS TÉCNICAS DE LOS SERVICIOS DE ENLACES DE INTERNET

En la siguiente tabla se especifican los anchos de banda requeridos en total de enlaces, lo cuales se detallan en el **Apartado 1**.

|  |  |  |
| --- | --- | --- |
| **Tabla Enlaces Internet** | | |
| **Cantidad Enlaces** | **BW (Mbps)** | **Descripción** |
| 45 | 10 | Enlaces de 10 Mbps (45 Casas de la Cultura) |
| 2 | 500 | Enlaces de 500 Mbps simétrico para los Sitios puntos de consolidación de infraestructura y servicios proporcionar por el prestador de los mismos. |

# DESCRIPCIÓN DEL SERVICIO DE INTERNET DE ACUERDO AL TIPO DE SITIO

**Para los sitios Tipo 1, 4, 5 y 6.**

* No se considera salida local a Internet, de acuerdo con lo establecido en el

**Apartado 1**.

* La salida a internet para estos sitios será a través de los puntos de consolidación de infraestructura y servicios.

**Para los sitios tipo 2 y 3.**

* Sitios con un ancho de banda de 10 Mbps de acuerdo con lo establecido en el

**Apartado 1**.

* El medio de acceso deberá ser en FO
* Para este tipo de sitio se requiere una disponibilidad mínima del 99.92% mensual.

**Puntos de consolidación de infraestructura y servicios.**

* Sitios: Principal y Secundario
* Sitios con un ancho de banda de 512 Mbps simétrico.
* El medio de acceso deberá ser en FO.
* Para este tipo de sitio se requiere una disponibilidad mínima de 99.92% mensual.
* Un segmento de direcciones IP homologado /25 para publicar servicios en internet, ruteado en ambos sitios, el cual deberá tener la facilidad de ser entregado hasta los equipos de seguridad en los edificios SEDE y 16 de Septiembre, sin necesidad de hacer NAT.

# DESCRIPCIÓN DEL CPE DEL SERVICIO DE INTERNET

El prestador de servicios deberá considerar como parte del mismo servicio, los equipos CPE´s necesarios de acuerdo a lo solicitado en el presente Anexo Técnico.

El prestador de servicios deberá encargarse de la instalación, activación, puesta a punto y soporte técnico, durante toda la vigencia del contrato que se derive del presente procedimiento.

El equipo CPE deberá de ser nuevo de última generación y sin anuncio de fin de venta del fabricante.

Los equipos CPE deberán de contar con soporte en sistema operativo, refacciones y componentes durante la vigencia del contrato.

El prestador de servicios deberá incluir en su propuesta un listado de los equipos que integran su solución, indicando la marca, el modelo, características de cada uno de ellos así como los documentos técnicos (folletos ó manuales solo de las hojas donde se menciona la característica solicitada en idioma español ó en inglés) de los equipos considerados. Además, deberá incluir diagramas con el diseño propuesto en donde se identifique en forma clara y detallada el diseño de la solución.

Las características de los CPE a proporcionar por el prestador de servicios, deberán de al menos contar con lo siguiente:

Para los sitios Tipo 2 y 3.

* Total WAN o LAN 10/100/1000: 2, de los cuales 2 sean basados en RJ-45 y 1 tenga capacidad de SPF.
* Memoria DRAM de 4GB
* Flash Memory 4GB

Para los sitios de consolidación de infraestructura y servicios.

* Servicios de software simultáneos a velocidades de hasta 2 Gbps
* Total de puertos WAN o LAN 10/100/1000 de los cuales 4
* Memoria DRAM de 4GB
* Flash Memory 8GB

Todos los equipos CPE que forman parte del proyecto deberán ser de la misma marca.

# SERVICIOS DE SEGURIDAD INFORMÁTICA

La SCJN requiere un Servicio denominado “Seguridad Informática (CiberSeguridad)”, que habilite un Modelo de Gobierno de Seguridad de la Información para el proyecto de Red Privada Virtual de la SCJN. El Servicio de Seguridad Informática es requerido para responder ante amenazas y riesgos derivados de incidentes de seguridad que puedan afectar la disponibilidad, integridad y confidencialidad de la información de la SCJN, mediante la habilitación de componentes de detección, contención y visibilidad de amenazas o comunicaciones anómalas inclusive sobre tráfico cifrado SSL. Se requiere habilite al menos las siguientes características:

Se deberá incluir la administración y operación de la infraestructura de seguridad, incluyendo los procesos y controles requeridos para la contención de incidentes de seguridad registrados por la misma.

Deberá habilitar una Metodología para la Gestión de la Seguridad Informática que permitan mantener un ciclo de mejora continua sobre los componentes de seguridad informática requeridos para el proyecto de la Red Privada Virtual de la SCJN, basándose en el estándar de seguridad de la información ISO 27000.

# COMPONENTES DEL SERVICIO DE SEGURIDAD INFORMÁTICA

## 

El servicio deberá incluir todos aquellos componentes (equipos, licenciamiento y accesorios) de seguridad informática que permitan en su conjunto cumplir los siguientes requerimientos:

* Alta disponibilidad en toda la infraestructura de seguridad informática.
* El participante deberá proponer e implementar una infraestructura de seguridad informática que ofrezca múltiples capas de detección y protección en los enlaces de comunicación de la Red Privada Virtual de la SCJN, incluyendo como mínimo los siguientes elementos: Seguridad perimetral, Sistema de detección y detección de intrusos, filtrado de Contenido y aplicaciones, Inteligencia de Seguridad informática, Antimalware y Antifraude.
* La infraestructura de seguridad informática permitirá la protección de los canales de comunicación de datos y de internet de los diversos inmuebles que sean integrados al proyecto de la Red Privada Virtual de la SCJN, contra ataques de malware, amenazas avanzadas, comportamientos anómalos y cualquier amenaza que pueda comprometer la integridad, disponibilidad y confidencialidad de la información de la SCJN que sea transitada a través de los métodos de comunicación proporcionados por el prestador de servicios.
* Permitirá la inspección de todo el tráfico de la red proveniente de todos los inmuebles que sean integrados al proyecto de la Red Privada Virtual de la SCJN, desde los diversos inmuebles y hacia internet, con la finalidad de vigilar, detectar, aislar y detener comportamientos anómalos, trafico anómalo, trafico proveniente de amenazas malware, amenazas avanzadas o ataques dirigidos hacia o desde los activos de información de la SCJN.
* Permitirá vigilar, analizar y detectar cualquier anomalía de los eventos registrados en los equipos de seguridad que conforman la solución, como pueden ser; exceso de conexiones TCP/UDP, incrementos súbitos de ancho de banda, conexiones anormales y cualquier otro evento que ponga en riesgo la integridad de los servicios de la SCJN.
* Permitirá definir y configurar políticas de acceso, de flujo de tráfico y de protección por grupos de usuarios/puerto/protocolo o direcciones IP.
* Permitirá contar con un sistema de detección de método múltiple incluyendo firmas compuestas, firmas de estado, anomalía de protocolo y detección de puerta trasera (back door), así como la obtención de tendencias y vectores de ataque con las firmas que el sistema detecte.
* Permitirá detectar y bloquear de manera activa accesos no autorizados.
* Permitirá la detección y contención de ataques informáticos desde sus etapas tempranas.
* Deberá proveer un sistema de monitoreo de seguridad informática donde se puedan observar y detectar el estado de salud de la Red Privada Virtual de la SCJN.
* Todos los equipos de la solución de seguridad propuesta por el prestador de servicios, para asegurar que tenga la madurez y experiencia en el ramo, se solicita que se encuentren dentro del cuadrante mágico de Gartner en el sector de líderes.

# SERVICIOS DE VIDEOCONFERENCIA

El prestador de servicios deberá proporcionar el servicio de videoconferencia en HD (alta definición) en el video, audio y contenido transmitido, con el cual la SCJN podrá mantener sesiones de videoconferencia punto a punto y punto multipunto entre las salas de videoconferencia a instalarse en los diferentes sitios remotos, a través de SIP y H.323, conectados a la VPN-MPLS y externos simultáneos conectados vía internet.

La arquitectura de videoconferencia deberá ser centralizada en un punto de consolidación de infraestructura y servicios, y deberá contar con redundancia geográfica en otro punto de consolidación de infraestructura y servicios secundario.

La definición mínima solicitada para establecer una sesión será de 720p a 30 FPS.

La cantidad de puertos concurrentes en el MCU será de 50 endpoints.

El servicio propuesto deberá contemplar el suministro, instalación, configuración y soporte de los endpoint, dispositivos de control, cámaras, pantallas, componentes de audio, visualización y almacenamiento de video y de transmisión de contenido, durante la vigencia del Contrato.

La solución deberá proveer mecanismos de Packet loss recovery

La solución deberá contar con alguna tecnología que evite sonidos no deseados en las conferencias.

# CARACTERÍSTICAS DE LOS EQUIPOS

Las especificaciones requeridas para los componentes de la solución de videoconferencia se indican a continuación:

# UNIDAD DE CONTROL MULTIPUNTO (MCU)

El equipo MCU propuesto por el prestador de servicios tendrá lo necesario para mantener hasta 10 conferencias de 6 participantes en total, de manera concurrente, bajo los estándares H.323 y SIP, para transmitir una imagen de alta definición de 720p a 30fps como mínimo. Contará con capacidad para soportar clientes a diferentes velocidades (transrating) o resolución (transcoding) bajo el estándar de video H.264 como mínimo.

El prestador de servicios deberá considerar que en las reuniones multipunto se realiza la funcionalidad de activación de voz (video swiching), en donde siempre se observará en pantalla a la localidad que hace uso de la palabra, así como por recuadros, en donde los participantes observarán al participante activo y a los participantes más recientes de la sesión. La solución deberá considerar componentes que permitan el reconocimiento facial y el seguimiento de los participantes de una videoconferencia ubicados en una misma sala de videoconferencia.

El equipo MCU propuesto por el prestador de servicios deberá contar con la capacidad de programar videoconferencias futuras mediante reservaciones, y tendrá la capacidad de configurar al menos 10 cuartos de videoconferencia (meetings rooms).

El equipo MCU para las sesiones de videoconferencias multipunto formará parte de la infraestructura instalada en los puntos de consolidación de infraestructura y servicios propuestos por el prestador de servicios, y desde donde se interconectará con los distintos endpoints de videoconferencia mediante enlaces con conexión a la VPN-MPLS y por medio de Internet.

La solución propuesta por el prestador de servicios deberá tener la capacidad de transmitir el contenido generado desde una computadora conectada al endpoint vía el protocolo H.239 o BFCP.

El equipo de MCU videoconferencia multipunto de alta definición propuesto por el prestador de servicios deberá contar con las siguientes características:

* El prestador de servicios deberá considerar que la solución cuente con mecanismos que permitan configurar tanto el protocolo SIP como el protocolo H.323.
* Podrá soportar el incremento en el número de puertos disponibles mediante cascadeo, apilamiento o clustering diseñadas para este propósito.
* Resolución mínima: 720p a 30 FPS
* Codecs de audio: G.711, G.722, G.729.
* Encripción por medio de AES.

# SERVIDOR DE ADMINISTRACIÓN

El prestador de servicios deberá proporcionar un servidor para la administración del MCU vía web. A fin de monitorear el total de sesiones de videoconferencia en un horario de 7x24 horas, los 365 días del año y deberá contar con las siguientes funcionalidades:

* Soportar la creación de diferentes perfiles de administrador con su respectiva clave, que permita crear y administrar las videoconferencias, así como la administración completa de las funcionalidades del equipo.
* Permitir crear reservaciones para sesiones de videoconferencia, monitorear en línea el estado de los participantes activos en una conferencia y poder mover a los participantes entre videoconferencias.
* Diagnóstico de funcionamiento del MCU y del rendimiento en línea.
* Consulta de alarmas y archivos de reporte de fallas.
* Visualización de reportes de utilización y duración de las videoconferencias.
* Podrá ser administrado por navegadores web de última generación como Chrome, así como Safari y Firefox
* La programación de las videoconferencias estará a cargo del personal en sitio
* Obtener estadísticas de uso y errores en los sistemas

# SERVIDOR DE GRABACIÓN

La solución de videoconferencia propuesta por el prestador de servicios deberá contar con la funcionalidad de grabar las sesiones de videoconferencia multipunto en alta definición (720p a 30 FPS), y las mantendrá para su acceso posterior utilizando un visualizadores estándar como Windows Media, Real Player o VLC y vía los sistemas de videoconferencia operando en los puntos finales (endpoint). Deberá contar con capacidad de llevar a cabo consultas bajo demanda en directo, y deberá contar con la capacidad de al menos 1000 horas de grabación a 512 Kbps y de grabación de al menos 4 sesiones simultáneas, soportando sistemas externos de almacenamiento para aumentar la capacidad de grabación.

El grabador de videoconferencias se deberá conectar localmente al MCU. Adicionalmente, el grabador podrá ser accedido vía IP y deberá ofrecer un portal en que estén almacenadas las conferencias. La grabación de videoconferencias integrará el contenido transmitido en la sesión vía el protocolo H.239 o BFCP.

Se deberán realizar respaldos mensuales manuales a fin de administrar mejor el espacio en el servidor. Se definirá en conjunto con la convocante, las políticas para la administración y permanencia de videos en el servidor.

La arquitectura de videoconferencia deberá ser centralizada en un punto de consolidación de infraestructura y servicios, y deberá contar con redundancia geográfica en otro punto de consolidación de infraestructura y servicios secundario.

# SERVIDOR DE CONTROL Y REGISTRO DE ENDPOINTS

El prestador de servicios deberá considerar en su solución el dispositivo de comunicaciones para controlar y administrar las sesiones de videoconferencia, con capacidad de asignar anchos de banda por llamada, definir zonas, autorizar el acceso de los sistemas de videoconferencia a una sesión, mantener el estado de las sesiones activas y generar del registro de las llamadas efectuadas. Adicionalmente, la solución deberá incluir la funcionalidad de Firewall trasversal para permitir el paso de forma segura de sesiones provenientes de otras redes.

El equipo propuesto por el prestador de servicios tendrá la capacidad de integrarse nativamente con el servicio de telefonía IP descrito en este anexo vía SIP o H.323. El prestador de servicios contempla un servidor de registro y proxy para SIP, con esto permitirá que los dispositivos SIP puedan registrarse a la red para la admisión y control de llamadas.

La solución propuesta por el prestador de servicios deberá soportar la función de traslación SIP y H.323 con la finalidad de que los usuarios puedan marcarse entre una sala de videoconferencia H.323 y una terminal SIP.

La solución deberá incluir la función trasversal con soporte de protocolos H.460.18 / H.460.19, permitiendo una conexión H.323 y SIP segura pasando por un firewall sin modificar el perímetro de seguridad de la red. El servicio de firewall trasversal propuesto por el prestador de servicios deberá contar con mecanismos de seguridad que permitirán evitar llamadas de video no deseadas desde internet, para ello deberá contar con mecanismos de programación de políticas de control de llamadas.

El equipo considerado por el prestador de servicios deberá contar con la característica STUN. Administración segura por HTTPS y/o SSH.

# SISTEMAS DE VIDEOCONFERENCIA

# ENDPOINT DE SALA

El endpoint de sala deberá contener las siguientes características:

* El códec de sala requerido deberá constar de: un códec, una cámara HD, un control remoto, micrófono con un rango de 360 grados, capacidad para transmitir el contenido de computadora y dos monitores integrados a una base donde estarán integrados todos los componentes.
* Soportar los estándares H.323, SIP, H.264, G.722, H.239 y BFCP.
* Resolución 720p a 30 FPS.
* Contar con soporte para la transmisión del contenido enviado desde una computadora.
* Conexión a redes Ethernet a través de un puerto UTP de 10/100/1000 Mbps.
* El Códec propuesto deberá contar con las entradas necesarias para recibir las señales de audio, video HDMI, micrófonos y red
* Deberá operar con dos monitores.
* El sistema tendrá la capacidad de soportar conexiones de 720p a 30 FPS consumiendo un ancho de banda de 768 Kbps como máximo.
* El sistema tendrá la capacidad de cifrar llamadas punto a punto, tanto del canal principal de video como del canal de contenido o el canal secundario de video.
* El codec de sala deberá integrar dos monitores a color de tecnología LED de alta definición (1080p) de al menos 55“, compatible con los formatos de video y entradas de audio y video del códec ofertado. Los monitores pueden ser de marca distinta del fabricante de la solución de videoconferencia, sin embargo deberá ser compatible con la base del sistema de videoconferencia.
* El códec, cámara HD y los dos monitores ofertados deberán estar integrados en una base de la misma marca que el fabricante.
* El prestador de servicios contemplará en la presente propuesta una cámara PTZ (Pan-Tilt-Zoom), con un zoom óptico de al menos 10x; con operación automática del foco, luminosidad y contraste. Adicionalmente deberá soportar un formato de hasta 1080p60.
* El prestador de servicios contempla en la presente propuesta micrófonos con cobertura de 360° para mesa de tipo alámbrico o inalámbrico. La solución propuesta por el prestador de servicios deberá contar con cancelación de eco automática, supresión de ruido, control de ganancia, y capacidad de enmudecimiento (mute).
* Adicionalmente la solución contará con altavoces en estéreo y subwoofer conectados al códec.

# ENDPOINT DESMONTABLE

El endpoint portátil deberá contener las siguientes características:

* Soportar los estándares H.323, SIP, H.264, G.722, H.239 y BFCP.
* Resolución 720p a 30 FPS.
* Contar con soporte para la transmisión del contenido enviado desde una computadora.
* Conexión a redes Ethernet a través de un puerto UTP de 10/100/1000 Mbps.
* El Códec propuesto deberá contar con las entradas necesarias para recibir las señales de audio, video HDMI para dos pantallas, micrófono y puerto de red.
* Deberá operar con 1 monitor no considerado en este sistema de videoconferencia y cuya conexión con el códec será en HDMI.
* El sistema tendrá la capacidad de soportar conexiones de 720p a 30 FPS consumiendo un ancho de banda de 768 Kbps como máximo, sin encabezados.
* El sistema tendrá con la capacidad de cifrar llamadas punto a punto, tanto del canal principal de video como del canal de contenido o el canal secundario de video.
* El endpoint requerido deberá constar de: un códec, una cámara HD, un control remoto, un micrófono, capacidad para transmitir el contenido de computadora y la capacidad para conectar un monitor mediante HDMI.
* Para este caso, se requiere que los componentes sean almacenados en un estuche que lo proteja de impactos y permita su transporte.
* Adicionalmente la solución contará con altavoces en estéreo y subwoofer conectados al códec.
* El prestador de servicios contemplará en la presente propuesta una cámara PTZ (Pan-Tilt-Zoom), con un zoom óptico de al menos 10x; con operación automática del foco, luminosidad y contraste. Adicionalmente deberá soportar un formato de hasta 1080p60.
* El prestador de servicios contempla en la presente propuesta un micrófono con cobertura de 360° para mesa de tipo alámbrico o inalámbrico. La solución propuesta por el prestador de servicios deberá contar con cancelación de eco automática, supresión de ruido, control de ganancia, y capacidad de enmudecimiento (mute).
* El sistema tendrá la capacidad de soportar conexiones de 720p a 30 FPS consumiendo un ancho de banda de 768 Kbps como máximo.

# CLIENTE DE VIDEOCONFERENCIA POR SOFTWARE

El prestador de servicios contempla en la presente propuesta una aplicación para ser instalada en equipos de cómputo o Dispositivos móviles con sistema operativo Windows 8 y 10, MAC OS X, iOS y Android. Deberá permitir realizar una videoconferencia, transmitiendo imagen de alta resolución de 720p a 30FPS. El prestador de servicios considerará 100 licencias de los clientes ligeros de video, que no aumentarán la cantidad de puertos (sesiones concurrentes en el MCU anteriormente descritas).

# DESCRIPCIÓN DE ENDPOINT DE VIDEOCONFERENCIA POR TIPO DE SITIO

Los sitios que requieren equipo de videoconferencia se señalan en el **Apartado 1**.

**Para los sitios Tipo 1.**

* Se requieren 5 endpoints desmontables.

**Para los sitios Tipo 2 y 3.**

* Sitios: 45 sitios (Casas de la Cultura Jurídica) se requiere un endpoint de sala por sitio.

Todos los equipos de la solución de videoconferencia utilizados para la Red Privada Virtual de la Suprema Corte de Justicia de la Nación, deberán ser de la misma marca.

# SERVICIOS DE TELEFONÍA IP / TARIFICACIÓN

La SCJN requiere contar con un modelo de comunicaciones basado en tecnología IP, seguro, redundante y flexible incluyendo servicios como los de telefonía IP, buzón de voz y mensajería unificada, por lo cual el prestador de servicios deberá proveer un servicio con tecnología de última generación que cumpla con los requerimientos que se especifican en el presente documento.

# SERVICIO DE TELEFONÍA IP

La SCJN requiere el servicio de Telefonía IP el cual deberá ser implementado por el prestador de serviciosen una arquitectura de alta disponibilidad, la cual será a nivel de hardware y software, es decir, el conmutador será instalado en servidores físicos separados para garantizar mayor nivel de confiabilidad. Deberá considerarse también que este conmutador será implementado en un esquema de redundancia geográfica con servidores distribuidos en dos diferentes puntos de consolidación de infraestructura y servicios proporcionados por el prestador de servicioslos cuales estarán comunicadas entre sí a través de la MPLS para poder realizar la sincronización de configuración y de usuarios.

Los sitios remotos deberán contar con un esquema de sobrevivencia telefónica básica, la cual será provista por el Gateway telefónico de cada inmueble, el cual tendrá la capacidad de registrar la totalidad de teléfonos IP del sitio y de realizar el procesamiento de llamadas entre los teléfonos IP de dicho sitio además de permitir realizar llamadas hacía la red pública de telefonía conmutada. Esto deberá ser realizado de manera automática cuando el Gateway del sitio pierda conectividad de red con el conmutador telefónico IP.

# CARACTERÍSTICAS GENERALES DEL SERVICIO DE TELEFONÍA IP

Las características que deberá cumplir el sistema de telefonía propuesto por el prestador de serviciosse enlistan a continuación:

* Sistema de procesamiento de llamadas de nueva generación.
* Soporte del protocolo IPv4.
* Alta disponibilidad y Redundancia Geográfica de los servicios de telefonía IP.
* En caso de falla en el servidor principal, los teléfonos se registrarán de manera automática al servidor de respaldo, cuando el sistema se restablezca los teléfonos podrán regresar al servidor al que estaban originalmente registrados para el procesamiento de llamadas.
* Lo sitios remotos deberán contar con funcionalidades de supervivencia telefónica básica a través del equipo Gateway ubicado en cada sitio.
* El conmutador telefónico deberá soportar los protocolos de señalización SIP y H323.
* El conmutador telefónico deberá soportar teléfonos IP que utilicen los protocolos SIP y H323.
* Se deberá soportar el registro de teléfonos IP en software y hardware.
* El conmutador deberá soportar el registro de teléfonos de software instalados en teléfonos inteligentes y tabletas electrónicas con sistemas operativos Android y iOS.
* Deberá soportar la integración con un directorio externo Active Directory LDAP, para ofrecer la funcionalidad de Directorio Institucional.
* El prestador de serviciosdeberá considerar en su propuesta la última versión de software disponible que sea estable y con al menos tres meses de haber sido liberada por el fabricante.

# FUNCIONALIDADES DE SEGURIDAD DEL SERVICIO DE TELEFONÍA IP

* El conmutador y los teléfonos IP deberán soportar el cifrado de las llamadas entre extensiones IP mediante el protocolo SRTP (Secure Real-time Transport Protocol), para asegurarse que los flujos de voz entre los diferentes dispositivos son seguros y que solo los dispositivos autorizados puedan recibir y descifrar el contenido de las conversaciones.
* El conmutador y los teléfonos IP deberán soportar el cifrado de la señalización de las llamadas entre teléfonos IP utilizando el protocolo TLS (Transport Layer Security)
* El cifrado de las llamadas entre teléfonos IP se deberá llevar a cabo utilizando el algoritmo de cifrado AES-128 como mínimo, el cual deberá ser soportado tanto en los teléfonos IP como en el conmutador.
* Las conferencias telefónicas entre extensiones IP deberán realizarse de manera cifrada utilizando el protocolo SRTP para la media y TLS para la señalización así como con el algoritmo de cifrado AES-128 como mínimo.
* Los mecanismos de cifrado deberán poder ser habilitados o deshabilitados individualmente por extensión IP desde el conmutador.
* Por seguridad y estabilidad, el sistema operativo de la plataforma de procesamiento de llamadas no estará basado en Microsoft Windows.

# FUNCIONALIDADES DEL SERVICIO DE TELEFONÍA IP

Las funcionalidades que soportará el sistema telefónico propuesto se enlistan a continuación:

* El sistema telefónico debe soportar la funcionalidad de Marcación Entrante Directa (DID, por sus siglas en inglés).
* El conmutador IP permitirá que un teléfono que recibe una llamada, obtenga la información del número telefónico de la línea que lo llama.
* El conmutador permitirá transferir una llamada establecida previamente hacia otro teléfono consultando previamente con el destinatario si se desea recibir la llamada
* El conmutador deberá soportar la transferencia de una llamada previamente establecida hacia otro teléfono de manera directa sin realizar una consulta previa.
* El sistema debe tener la capacidad de establecer conferencias de voz de 6 participantes por sesión sin realizar cascadeo.
* Se deberá soportar la funcionalidad que permite a un usuario crear sesiones de conferencia de voz las cuales estén asociadas a un número de extensión, el cual será marcado por los usuarios invitados para integrarse a la conferencia.
* El sistema contará con la funcionalidad de marcación a números restringidos a través de un código de seguridad numérico, que podrá utilizar el usuario en cualquier teléfono IP perteneciente al conmutador.
* El conmutador debe soportar la funcionalidad que permite escuchar música o mensajes de audio, cuando se pone una llamada en espera.
* El sistema permitirá realizar desvío de todas las llamadas entrantes de un teléfono IP hacia un número predefinido por el usuario.
* Se podrán realizar desvíos de las llamadas entrantes de una extensión en el caso de que estas no sean contestadas después de un determinado número de timbrados.
* La solución debe soportar la funcionalidad de “Numero único de marcado”, la cual brinda la posibilidad de tener un timbrado simultáneo en varios dispositivos telefónicos, ya sea en teléfonos físicos o de software.
* El conmutador debe soportar la funcionalidad que permite a un usuario firmarse en cualquier otro teléfono IP perteneciente al mismo conmutador, con su usuario o número de identificación además de su contraseña, para que este se reconfigure con su número de extensión y con las programaciones, facilidades y privilegios de llamadas que tenga asignadas en su teléfono original.
* El sistema deberá permitir a través del Teléfono IP, la programación de marcaciones rápidas mediante teclas, dependiendo de la capacidad de teclas programables.
* Se deberá soportar la funcionalidad de marcación abreviada la cual permite a los usuarios, marcar números de teléfono predefinidos por medio de solo algunos dígitos.
* El sistema soportará arreglos Jefe / Secretaria en los cuales las llamadas sean enviadas a la secretaria, quien decidirá en base a la disponibilidad del Jefe si le transfiere la llamada o no.
* El sistema deberá ser capaz de generar un histórico de llamadas el cual será usado por un sistema de tarificación de llamadas para su procesamiento.

# SERVICIO DE BUZÓN DE VOZ Y MENSAJERÍA UNIFICADA

La SCJN requiere un servicio de buzón de voz y mensajería unificada que permita a sus usuarios telefónicos recibir mensajes de voz cuando estos no se encuentren disponibles y que estos puedan consultarlos posteriormente ya sea a través de su dispositivo telefónico o a través de un mensaje de audio en su correo electrónico.

El servicio de Buzón de Voz y Mensajería Unificada deberá ser implementado por el prestador de serviciosen una arquitectura centralizada con servidores físicos redundantes, ubicados en un centro de datos que prestador de servicios deberá proporcionar, los cuales permitan mayor disponibilidad del servicio. El sistema de buzón de voz deberá estar integrado al sistema de correo electrónico de La SCJN para habilitar los servicios de mensajería unificada.

# FUNCIONALIDADES DEL SISTEMA DE BUZÓN DE VOZ Y MENSAJERÍA UNIFICADA

* El servicio de buzón de voz, podrá ser consultado mediante una tecla de acceso rápido en el teléfono, con el uso de una contraseña como medida de seguridad.
* Se deberá poder acceder a los mensajes de voz, desde cualquier teléfono dentro o fuera de la red de La SCJN, marcando a un número directo en donde una grabación solicitará el número de extensión y contraseña del usuario de buzón de voz para permitirle el acceso a este.
* El usuario tendrá la capacidad de personalizar el mensaje de bienvenida a su buzón de voz.
* El servicio de buzón de voz deberá soportar al menos los idiomas español e inglés para los audios con los que el sistema interactúa con los usuarios.
* El sistema podrá clasificar los mensajes de voz como normal y/o urgente.
* El sistema tendrá la capacidad de almacenar mensajes de voz de hasta 5 minutos por extensión.
* Se debe soportar la integración del sistema de buzón de voz con el sistema Microsoft Exchange propiedad de ***La SCJN*** para proveer los servicios de mensajería unificada
* Se soportará la funcionalidad de mensajería unificada la cual debe permitir que los usuarios reciban una copia del buzón de voz en su correo electrónico en formato .WAV y/o mp3.

# SERVICIO DE CONTESTADORA AUTOMÁTICA

El prestador de serviciosdeberá proveer un sistema de contestadora automática el cual será compatible con el conmutador telefónico IP propuesto. El sistema de contestadora automática deberá implementarse en una arquitectura distribuida, de forma tal que estos servicios sean provistos de manera local en cada uno de los sitios lo cual permitirá que al perderse la conectividad con el conmutador IP, los servicios de contestadora automática sigan operando de manera normal. Estos servicios deberán ser provistos mediante hardware instalado en los equipos Gateway de voz de cada localidad.

# FUNCIONALIDADES DEL SERVICIO DE CONTESTADORA AUTOMÁTICA

El servicio de contestadora automática tendrá las siguientes características:

* El servicio de contestadora automática permitirá recibir llamadas originadas por usuarios de la red pública de telefonía las cuales procesará y enviará al destinatario correcto de acuerdo a la interacción por medio de tonos DTMF con el usuario que marca.
* El servicio deberá ser provisto mediante hardware instalado en los equipos Gateway de voz de cada localidad.
* El servicio permitirá recibir un máximo de 4 llamadas simultáneas desde la red pública de telefonía para su posterior procesamiento.
* La cantidad máxima de niveles del árbol de decisión de la contestadora automática será de cuatro.
* El servicio deberá ser soportado en idiomas español e inglés.

# SERVICIOS DE GATEWAY DE VOZ

Las localidades remotas pertenecientes a la SCJN requieren tener acceso a la red de telefonía pública conmutada, por lo cual es necesario que el prestador de serviciosprovea los servicios de Gateway de Voz en cada una de las localidades que cuentan con telefonía IP. Este servicio deberá ser provisto en una arquitectura con equipos Gateway distribuidos en las diversas localidades remotas los cuales se integrarán al conmutador para el procesamiento de las llamadas.

# CARACTERÍSTICAS DEL GATEWAY DE VOZ

El equipo Gateway de Voz considerado para todas las localidades deberá contar con las siguientes características:

* Deberá soportar los protocolos de señalización H.323 y SIP
* El Gateway deberá ser un elemento físico independiente a la arquitectura de networking (routers, etc) con la finalidad de garantizar un mayor nivel de disponibilidad y continuidad de la operación en caso de contingencia.
* El equipo deberá incluir recursos de conferencia locales para realizar al menos tres conferencias simultáneas de seis participantes cada una.
* Deberá soportar los códec de voz G.711, G.722, G.729a, G.729b y G.729ab.
* El equipo soportará los protocolos SNMP, SSHv2 y Telnet
* El Gateway de voz será capaz de proveer música en espera de manera local.
* El equipo deberá incluir la funcionalidad de contestadora automática mediante un módulo de hardware incluido en el equipo.
* Se deberán incluir puertos FXO para la conexión de troncales analógicas de acuerdo a la cantidad de troncales existentes especificadas en el **Apartado 1.**
* Deberá incluir un mecanismo de sobrevivencia telefónica básica para realizar el procesamiento de llamadas de los usuarios cuando la conectividad de red hacia el conmutador sea interrumpida.
* La solución de sobrevivencia se activa de manera automática, sin intervención del administrador de la red, en el momento en que se pierda la conectividad hacia el conmutador.
* La funcionalidad de sobrevivencia deberá ser soportada para un máximo de 50 teléfonos IP por sitio.
* Las funcionalidades que deberá soportar en modo de sobrevivencia son: Llamada entre extensiones del mismo sitio, llamada hacia la red PSTN, música en espera, conferencias de tres participantes y transferencias de llamadas.

# TELÉFONOS IP

El prestador de serviciosdebe incluir como parte de su servicio el suministro de aparatos telefónicos IP que sean de la misma marca que la del conmutador para asegurar la completa compatibilidad y soporte de funcionalidades.

# TELÉFONO IP BÁSICO

Características del teléfono:

* Pantalla monocromática de 3 pulgadas o superior.
* Deberá soportar como mínimo 5 líneas telefónicas
* Deberá incluir teclas softkey para el acceso a funciones y servicios
* El teléfono contará con botón físico para activar el altavoz
* Botón físico para consultar el buzón de voz
* Botón físico para consultar el directorio telefónico o la lista de contactos
* Botón físico para consultar historial de llamadas
* Botones de navegación dedicados
* Indicador físico de recepción de buzón de voz
* 1 puerto de red Gigabit Ethernet base-T para conexión a la red
* 1 puerto de red Gigabit Ethernet base-T para conexión a PC
* Soporte del protocolo SIP y H.323
* Deberá soportar PoE (IEEE 802.3af).
* Cifrado utilizando el estándar AES-128 como mínimo
* Cifrado de la señalización con TLS
* Cifrado del flujo de audio de las llamadas con SRTP
* Soporte de 802.1Q, 802.1P, 802.1x
* Soportará asignación de dirección IP de manera estática o de manera dinámica con DHCP
* Deberá soportar los códecs G.711, G722, G.729a

*Funcionalidades de las terminales.*

* Caller ID
* Fecha y hora
* Tonos de timbre seleccionables por el usuario.
* Soporte para al menos los idiomas español e inglés
* Desvío de llamadas
* Conferencias
* Transferencias
* Estacionar llamadas
* Captura de llamada
* Movilidad de extensión
* Llamada en espera
* Códigos de autorización de llamadas
* Silencio
* Directorio
* Remarcado
* Marcaciones rápidas
* Buzón de voz
* Línea compartida

# TELÉFONO IP EJECUTIVO

Características del teléfono:

* Pantalla a color de 3.5 pulgadas o superior.
* Deberá soportar como mínimo 5 líneas telefónicas
* Deberá soportar la adición de un módulo de expansión de botones
* Deberá incluir teclas para el acceso a funciones y servicios
* El teléfono contará con botón físico para activar el altavoz
* Botón físico para consultar el buzón de voz
* Botón físico para consultar el directorio telefónico o la lista de contactos
* Botón físico para consultar historial de llamadas
* Botones de navegación dedicados
* Indicador físico de recepción de buzón de voz
* 1 puerto de red Gigabit Ethernet base-T para conexión a la red
* 1 puerto de red Gigabit Ethernet base-T para conexión a PC
* Soporte del protocolo SIP y H.323
* Deberá soportar PoE (IEEE 802.3af).
* Cifrado utilizando el estándar AES-128 como mínimo
* Cifrado de la señalización con TLS
* Cifrado del flujo de audio de las llamadas con SRTP
* Soporte de 802.1Q, 802.1P, 802.1x
* Soportará asignación de dirección IP de manera estática o de manera dinámica con DHCP
* Deberá soportar los códecs G.711, G722, G.729ª

*Funcionalidades de las terminales.*

* Caller ID
* Fecha y hora
* Tonos de timbre seleccionables por el usuario.
* Soporte para al menos los idiomas español e inglés
* Desvío de llamadas
* Conferencias
* Transferencias
* Estacionar llamadas
* Captura de llamada
* Movilidad de extensión
* Llamada en espera
* Códigos de autorización de llamadas
* Silencio
* Directorio
* Remarcado
* Marcaciones rápidas
* Buzón de voz
* Línea compartida

La cantidad de teléfonos IP requerida se especifica en el **Apartado 1.**

Todos los equipos de la solución de telefonía utilizados para la Red Privada Virtual de la Suprema Corte de Justicia de la Nación, deberán ser de la misma marca.

# SERVICIO DE TARIFICACIÓN

El servicio de tarificación propuesto por el prestador de serviciosdeberá tener las siguientes características:

* La administración del servicio de tarificación será llevada a cabo por el prestador de servicios
* El prestador de serviciosdeberá proporcionar a La SCJN un acceso de solo lectura a la herramienta de administración que le permita la consulta y obtención de reportes del sistema de tarificación.
* El servicio se proveerá de manera centralizada con capacidad mínima de 1000 extensiones y 100 sitios remotos.
* El sistema permitirá la carga de los planes tarifarios de los principales carriers de telefonía convencional.
* El prestador de serviciosrealizará la puesta en marcha del servicio de tarificación, incluyendo todo el software, hardware, licencias, sistemas operativos y cualquier otro elemento necesario para la correcta operación del sistema de tarificación.
* El sistema tendrá la capacidad de agrupar varias extensiones o códigos de autorización que pertenezcan a un mismo usuario.
* El sistema realizará el proceso de llamadas de todo tipo: entrantes, locales, larga distancia nacional, internacional, celulares, Lada 800, etc.
* El sistema tendrá la capacidad de almacenaje del histórico de llamadas por al menos un año.
* El tarificador deberá poder establecer presupuestos mensuales de gasto telefónico, ya sea por: Monto de gasto, Número de llamadas, Tiempo de uso.
* Se deberán poder generar reportes básicos, basados en diferentes criterios que el administrador del servicio podrá indicar a su elección.
* Detallado por extensión o grupos de extensión.
* Detallado por clave o código de autorización.
* Resumen por Unidad Administrativa.
* Resumen por Coordinación (Dirección General).
* Por Entidad Federativa.
* Por Fechas.
* Por números telefónicos más marcados.
* Por Tipos de llamadas, Nacionales, Internacionales, celulares, locales, locales propias de conmutador.
* Por Operador o Compañía Telefónica Pública.
* El sistema no se debe limitar a los reportes antes señalados, la DGTI podrá solicitar reportes personalizados.
* Capacidad de configurar reportes personalizados que se generen en forma manual y/o automática en las fechas y horas previamente programadas por el administrador del sistema, así como poder personalizar la configuración de encabezado, título, logotipos y enviarlo a través de correo electrónico.
* El sistema debe contar con una selección de filtros para la emisión de reportes, permitiendo el filtrado por fecha, hora, extensión, código de autorización, departamento, división, áreas, tipos de llamadas (Larga Distancia Internacional, Mundial, Locales, Celulares, Entrantes, transferencias internas y externas, indicando el origen y fin), corporación, dígitos marcados, llamadas entrantes, llamadas salientes, duración, costo por llamada, código de cuenta, duración de llamada, código de acceso.
* Las llamadas realizadas a través de clave o código de autorización, deberán ser registradas al usuario dueño de dicha clave o código, independientemente de la extensión desde donde haya generado la llamada. Por lo tanto, no deberá asignarse ningún costo adicional a las extensiones desde donde se haya realizado la llamada.
* El sistema debe emitir los diversos tipos de reportes, en forma manual y/o automática hacia archivo (Word, PDF o Excel), pantalla e impresora, y permitir el ordenamiento de la información en forma individual (capacidad de hacer reportes particulares por usuario, por extensión y por código, de forma específica).
* Debe operar con el plan de numeración telefónica, así como los esquemas de tarifas de las redes públicas.
* Debe tener la capacidad de soportar los planes, actuales y futuros, de numeración de la red telefónica pública.

# INTEGRACIÓN DE LAS PLATAFORMAS DE TELEFONÍA EXISTENTE Y NUEVA

La SCJN cuenta actualmente con un conmutador Avaya que provee servicios de telefonía a las oficinas siguientes: Sede, 16 de Septiembre, Revolución y CENDI. Esta plataforma telefónica junto con sus aplicaciones no será reemplazada, por lo cual el prestador de serviciosserá responsable de la integración telefónica de esta plataforma con la nueva infraestructura de telefonía.

El prestador de serviciosdeberá considerar todo lo necesario tanto en hardware, software y licenciamiento en la infraestructura propuesta, para la integración a la citada plataforma Avaya cumpliendo con al menos lo siguiente:

* Se podrán realizar llamadas entre extensiones de ambos sistemas telefónicos.
* Sera posible realizar transferencias desde un teléfono perteneciente a una plataforma con destino hacia un teléfono perteneciente al otro conmutador y viceversa
* Sera posible integrar un teléfono perteneciente a un conmutador a una conferencia iniciada en un conmutador diferente al del teléfono mencionado.

La cantidad de llamadas simultáneas entre plataformas corresponderá al 10% de la cantidad total de usuarios del nuevo servicio de telefonía solicitado en el presente documento.

# SERVICIOS DE RED LAN EXTENDIDA

La SCJN solicita un servicio de red LAN para la interconexión de los nuevos servicios, la cual se llamará LAN Extendida para diferenciar de la red existente. Dicha red LAN Extendida deberá de interconectarse con la red existente para permitir la convivencia e interoperabilidad entre flujos de tráfico de datos, voz y video sin deteriorar su procesamiento.

La SCJN requiere que los equipos que proporcionen el servicio de red LAN extendida sean suministrados, instalados, configurados y mantenidos por parte del prestador de servicios durante la vigencia del Contrato.

La instalación de los equipos que proporcionen el servicio de la red LAN extendida deberá incluir el suministro, etiquetado y acomodo de los cordones de parcheo en los organizadores de los racks que corresponda.

Con el objetivo de asegurar la continuidad de la operación de La SCJN, el prestador de servicios deberá contemplar en su propuesta que la solución de los servicios de red LAN extendida y WLAN, nuevos y de última generación.

El servicio deberá de proporcionar puertos de red con velocidades de 10/100/100 RJ45 cobre para la conexión de los dispositivos finales de la SCJN y la conexión de los equipos propuestos por el prestador de servicios.

# CARACTERÍSTICAS GENERALES DEL SERVICIO DE RED LAN EXTENDIDA

Todos los equipos propuestos deberán tener instalada la última versión de software liberada y estable.

Para todos los Sitios los equipos deberán de cumplir con las siguientes características:

|  |  |
| --- | --- |
| **SWITCH** | |
| **Categoría** | **Descripción** |
| Tipo de gabinete: | Switch 1 UR |
| Tipo de sistema operativo: | Sistema operativo base con funciones de ruteo básico, descritas en la, sección funcionalidades de capa 2 y capa 3. |
| Fuente de alimentación: | Fuentes de Poder AC. |
| Throughput: | Capacidad de conmutación: 176 Gbps  Tasa de reenvío: 130Mpps |
| Puertos Gigabit Ethernet base-T Mínimos Requeridos | 48 Puertos 10/100/1000 Ethernet PoE+ |
| Puertos de Uplink Gigabit Ethernet Base-X y puertos SFP Mínimos requeridos | 2 Puertos adicionales a los de cobre, tipo SFP/SFP+ con soporte de transceivers (1 G/10G) en fibra óptica. |
| Direcciones MAC | 32,000 |
| Rutas IPv4 | 24,000 |
| VLAN | 8 colas de priorización por puerto.  Soporte de al menos 4,000 VLAN ID según el estándar 802.1 Q. |
| Protocolos de administración | Interface de línea de comandos, SNMPv3.  Capacidad instalada de sFlow y/o NetFlow.  Funcionalidad de puerto espejo  RMON con 4 grupos de RMON(historial, estadísticas, alarmas y eventos) |
| Protocolos de autenticación de administradores | Soporte de múltiples niveles de privilegios de acceso por consola para los de administradores ya sea local o remotamente por SSH v2.  Soporte autenticación Radius o Tacacs+ |
| Funcionalidades de Capa 2 y capa 3 | IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) encompasses.  IEEE 802.1D Spanning Tree Protocol (STP).  IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).  Soporte de 802.1Q VLAN.  Soporte de IEEE 802.3ad (LACP).  Protocolos de enrutamiento RIP v1/v2, RIPng, y OSPFv2, OSPF v3.  Soporte de IGMPv2, IGMPv3 Snooping, PIM-SM, PIM-SSM, PIM-DM.  Capacidad instalada de VRRP o HSRP. |
| Funcionalidades de seguridad | IEEE 802.1x  DHCP Snooping  DHCP Guard  Seguridad por Puerto  Inspección ARP  Políticas de QoS  Listas de Acceso  BPDU Guard |
| Soporte de estándares: | IEEE 802.3af and 802.3at.  IEEE 802.1D.  IEEE 802.1p.  IEEE802.1Q VLAN  IEEE 802.1x.  IEEE 802.3x.  IEEE 802.1 s, 802.1 w.  IEEE 802.1 p CoS.  IEEE 802.3z Gigabit Ethernet.  IEEE 802.3ad.  RMON I and II standards  IEEE 802.3af  IEEE 802.3at  IEEE 802.1as  IEEE 802.3bz  IEEE 802.1X-Rev |
| Cumplimiento Electromagnético | ICES-003 Class A  EN 55022 Class A  CISPR 22 Class A |

Para los Sitios puntos de consolidación de infraestructura y servicios se requiere que los equipos cumplan con las siguientes características:

|  |  |
| --- | --- |
| **SWITCH Puntos de consolidación de infraestructura y servicios** | |
| **Categoría** | **Descripción** |
| Tipo de gabinete: | Switch 1 UR  Con funcionalidad de protocolos tanto de capa 2 como de capa 3 avanzado. |
| Tipo de procesamiento: | Capacidad de conmutación: 800 Gbps  Tasa de reenvío: 250Mpps |
| Alta disponibilidad | Contar con la capacidad de agrupar 2 switches formando un switch virtual o switch clustering, proporcionando una topología libre de loops en capa 2, proporcionando carga compartida sobre los enlaces, proporcionando una operación Activo-Activo para L2 y L3.  Reinicio de protocolos de ruteo sin interrumpir el direccionamiento de paquetes para IPv4 ni multicast. |
| Fuentes de alimentación: | Fuentes de Poder AC redundantes. |
| Enfriamiento | De enfrente hacia atrás |
| Puertos: | 40 puertos 1G/10G SFP+  1 puerto de administración 10/100/1000 Base-T |
| Protocolos de administración: | Administración por Interface de línea de comandos (CLI), SNMPv3  Capacidad instalada de sFlow y/o NetFIow para visibilidad en capa 2,3 y 4.  Soporte de Port Mirror local y remoto. |
| Protocolos de autenticación de administradores: | Soporte de múltiples niveles de privilegios de acceso por consola, ya sea local o remotamente por SSH v2. |
| Funcionalidades de capa 2 y capa 3: | 802.1 Q VLAN.  Agregación de enlace IEEE 802.3ad (LACP).  802.1d Spanning Tree Protocol.  802.1w Rapid Spanning Tree Protocol.  802.1s Múltiple Spanning-Tree Protocol.  Soporte de al menos 4,000 VLAN  50,000 entradas MAC.  Soporte IPv4 y IPv6  Protocolos de ruteo dinámico; RIP v1/v2, OSPFv2, OSPFv3,IS-IS, BGP  Soporte de IGMPv2, IGMPv3 Snooping, PIM-SM y DVMRP en IPv4 y MLD en IPv6.  Calidad de Servicio con 8 colas por puerto  NFS o SSO  Jumbo Frame de 9216 bytes  CIR, PIR  Rate limit basado en flujos |
| Funcionalidad de seguridad: | Seguridad por puerto  Listas de acceso por VLAN, rutas y puerto  IEEE 802.1x  Portección de ataques DoS  VLANs Privadas  Control de tormentas de tráfico  DHCP Snooping |
| Soporte de estándares: | Ethernet IEEE 802.3  10Gigabit Ethernet IEEE 802.3ae.  IEEE 802.3ad (LACP).  IEEE 802.1p CoS.  RMON I y II  47CFR Part 15 (CFR 47) Class A  CISPR22 Class A  EN55022 Class A  ICES003 Class A  EN55024  CISPR24  GR-63-Core (NEBS) Level 3 |
| Certificados de seguridad | UL 60950-1 Second  CAN/CSA-C22.2 No. 60950-1  EN 60950-1  IEC 60950-1  AS/NZS 60950-1 |

Todos los equipos Switch que forman parte del proyecto deberán ser de la misma marca.

# SERVICIOS DE RED INALÁMBRICA PARA CASAS DE LA CULTURA

La SCJN requiere de un servicio de movilidad para que los usuarios de la institución puedan realizar sus funciones con mayor libertad dentro de las mismas instalaciones de los sitios Tipo 2 Y 3, de la misma dependencia. Dicho servicio de movilidad podrá proporcionarse para los dispositivos móviles institucionales tales como Laptops, smartphones y tabletas.

El prestador de servicios deberá proporcionar los servicios de implementación y puesta a punto de los equipos de acceso para dar el servicio requerido de conectividad inalámbrica corporativa en los sitios Tipo 2 y 3.

La SCJN requiere como funcionalidad la autenticación y autorización de los usuarios de la institución mediante 802.1X a través del Directorio Activo propiedad de La SCJN**.**

El prestador de servicios deberá incluir todo lo necesario para que el equipo quede operando correctamente, incluyendo las licencias y habilitación de funcionalidades.

El prestador de servicios deberá proporcionar para el servicio de red inalámbrica de Casas de la Cultura:

* Elaboración de plan de trabajo
* Instalación y aceptación de servicio

Para tener una mejor cobertura de la señal inalámbrica serequiere el prestador de servicios adjudicado realice site survey para la correcta ubicación de los Puntos de acceso en todos los sitios Tipo 2 y 3.

|  |  |  |
| --- | --- | --- |
| **Sitio ID** | **Cantidad de Sitios** | **Punto de Acceso Inalámbrico para interior (Access Point) POR SITIO** |
| TIPO 2 y 3 | 45 | 4 |

El servicio deberá contar con controladoras para administración centralizada para los puntos de acceso y redundancia geográfica en puntos de consolidación de infraestructura y servicios para dar alta disponibilidad.

El cableado estructurado categoría 6 hacia los puntos de acceso deberá contemplar el mínimo de modificaciones en los inmuebles dado que los sitios son catalogados como***Propiedad de la Nación y Patrimonio Histórico.***

# CARACTERÍSTICAS GENERALES DEL SERVICIO DE RED WLAN

|  |  |
| --- | --- |
| **CONTROLADOR INALÁMBRICO** | |
| **Categoría** | **Descripción** |
| Características Generales | Administración simultanea de 500 puntos de acceso.  Rendimiento sin bloqueo para 802.11n y optimizado para redes 802.11ac.  Fuentes redundantes.  Soporte de redes en malla.  Presenta información en tiempo real de los puntos de acceso conectados y usuarios. |
| Unidades de Rack | 1 U |
| Administración | Vía Web: HTTP/HTTPS  Línea de comandos: Telnet, Secure Shell (SSH), puerto serial |
| Puertos físicos | 8 puertos compatibles con 1000 BASE-T, 1000Base-SX y 1000Base-LH. |
| Normatividad | UL 60950-1:2003  EN 60950:2000 |
| Estándar | IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac.   IEEE 802.1X  IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Vtagging, and IEEE 802.1AX Link Aggregation. |
| RFC | RFC 768 UDP  ● RFC 791 IP  ● RFC 2460 IPv6  ● RFC 792 ICMP  ● RFC 793 TCP  ● RFC 826 ARP  ● RFC 1122  ● RFC 1519 CIDR  ● RFC 1542 BOOTP  ● RFC 2131 DHCP |
| CIFRADO | WEP and TKIP-MIC: RC4 40, 104 and 128 bits (para llaves estaticas y compartidas)  AES: CBC, CCM, CCMP  DES: DES-CBC, 3DES  SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit  DTLS: AES-CBC  ●  IPSec: DES-CBC, 3DES, AES-CBC |

|  |  |
| --- | --- |
| **Punto de Acceso Inalámbrico para interior (Access Point)** | |
| **Categoría** | **Descripción** |
| Características Generales | La solución inalámbrica será de la última generación que soporte el protocolo inalámbrico 802.11 ac.  Radios 2.4 y 5 GHz, dual- band.  4x4 MIMO con cuatro flujos espaciales.  Antenas Internas Omndireccionales 2.4GHz con ganancia de 3dBi y 5GHz con ganancia de 5dBi.  Será capaz de ser controlado y administrado de forma centralizada incluyendo las funciones de actualización de configuraciones y software.  Dos puertos Gigabit Ethernet.  PoE: Compatibilidad con 802.3af. |
| Seguridad | 802.1X.  802.11i, Wi-Fi Protected Access 2 (WPA2), WPA Advanced Encryption Standard (AES)  ● Tipos de Extensible Authentication Protocol (EAP):  ◦   EAP-Transport Layer Security (TLS)  ◦   EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)  ◦   Protected EAP (PEAP) v0 o EAP-MSCHAPv2  ◦   EAP-Flexible Authentication via Secure Tunneling (FAST)  ◦   PEAP v1 o EAP-Generic Token Card (GTC)  ◦   EAP-Subscriber Identity Module (SIM) |
| Estándares | IEEE 802.11a/b/g, 802.11n, 802.11h, 802.11d, 802.1 ac  IEC 60950-1  EN 60950-1  EN 50155  UL 60950-1  Wi-Fi Multimedia (WMM) |

El servicio de red inalámbrica deberá permitir la configuración de invitados utilizando la salida a Internet solicitada en cada sitio para usuarios externos o visitantes de las Casas de Cultura mediante una red lógica independiente a la red institucional, esto para garantizar la seguridad de la información de la red de la SCJN.

El servicio de red inalámbrica independiente deberá utilizar la salida a internet solicitada para cada sitio

La SCJN requiere proporcionar el servicio de red inalámbrico con salida a internet de manera libre a invitados que lleguen a las Casas de Cultura.

El servicio de internet inalámbrico para usuarios invitados aun cuando deberá de ser libre deberá de proporcionar el servicio de seguridad básica mediante un portal cautivo en el cual los usuarios podrán tener acceso mediante un registro de correo electrónico, además deberá de proporcionar el servicio de filtrado de contenido para visualizar el uso del ancho de banda de los usuarios y poder delimitar acceso a páginas maliciosas.

El prestador de servicios deberá de proporcionar el acceso a Internet mediante un enlace dedicado de 10 Mbps para ofrecer la conectividad a los usuarios invitados. El enlace de internet deberá de tener las características mencionadas en la descripción de **REQUERIMIENTOS ESPECÍFICOS PARA EL SERVICIO DE ACCESO A INTERNET**

El servicio deberá de proporcionar un Dashbord para configuración y visualización del comportamiento de la red inalámbrica y los dispositivos de los usuarios, se podrán agregar mapas de calor donde se visualice cada uno de los puntos de acceso. Para ello el servicio podrá ser administrado directamente por la SCJN ó por el Centro de Operaciones propuesto por el prestador de servicios.

Se deberán de presentar reportes y analíticos detallados con la información visualizada dentro de la herramienta, los cuales deberán de entregarse en los reportes mensuales.

Todos los equipos de la solución de red inalámbrica utilizados para la Red Privada Virtual de la Suprema Corte de Justicia de la Nación, deberán ser de la misma marca.

# CARACTERÍSTICAS GENERALES DEL SERVICIO DE RED INALÁMBRICA INVITADOS

El prestador de serviciosdeberá considerar en su propuesta los siguientes componentes como un servicio administrado:

* Access Points administrados desde los puntos de consolidación de infraestructura y servicios.
* Portal de autenticación (Portal Cautivo).
* Reporte de Tráfico y Uso (Interfaz Gráfica).
* Historia de Dispositivos (Interfaz Gráfica).
* Indicadores Presence Analytics (Interfaz Gráfica).
* Configuración de SSID de la red Institutional y para Invitados.
* Acceso a la interfaz gráfica con nivel de monitoreo.
* Publicación de la imagen de SCJN en la página de bienvenida o portal cautivo (autentificación).
* Filtrado de contenido por categoría y URL.

El prestador de servicios deberá garantizar la separación de los tráficos provenientes de la SCJN de los usuarios invitados para los cuales solo se proporcionara internet.

# PUNTOS DE CONSOLIDACIÓN DE INFRAESTRUCTURA Y SERVICIOS PARA REDUNDANCIA GEOGRÁFICA DE SERVICIOS DE INTERNET, TELEFONÍA IP, VIDEOCONFERENCIA Y RED INALÁMBRICA

La SCJN solicita que los servicios propuestos por el prestador de servicios se proporcionen de manera centralizados en puntos de consolidación de infraestructura y servicios propios donde se alojen las plataformas principales de servicio. Los servicios centralizados se requiere se encuentren en alta disponibilidad con redundancia geográfica de los mismos para garantizar la continuidad de la operación.

# DESCRIPCIÓN DE LOS PUNTOS DE CONSOLIDACIÓN DE INFRAESTRUCTURA Y SERVICIOS.

Los puntos de consolidación de infraestructura y servicios, propuestos por el prestador de los mismos deberán de contar con las siguientes características:

Deberá contar con una infraestructura de alojamiento diseñada para operar como un punto de consolidación de infraestructura y servicios de Alta Disponibilidad dentro de la República Mexicana.

Deberá estar certificado como ICREA Nivel 3 por el International Computer Room Expert Association o Tier III, solo para el punto de consolidación principal.

El prestador de servicios deberá proveer los Servicios de puntos de consolidación de infraestructura y servicios de forma permanente e in-interrumpida durante la prestación de los servicios.

El prestador de servicios deberá considerar dentro de su propuesta técnica dos puntos de consolidación de infraestructura y servicios, que se ubiquen en diferentes estados de la república mexicana. Cada uno de los espacios ofertados deberá contar con los servicios auxiliares necesarios para la operación de los equipos que darán servicio a la infraestructura de la SCJN, que se solicitan en el presente proyecto.

El prestador de servicios podrá habilitar los servicios en una ubicación que deberá incluir como mínimo lo siguiente:

* Facilidades necesarias para proveer el servicio.
* Servicio de instalación.
* Energía.
* Servicio de técnico especializado.

# INFRAESTRUCTURA AUXILIAR PARA LOS SERVICIOS

El prestador de servicios deberá contemplar dentro de su diseño la infraestructura auxiliar que se describe en esta sección, y la cual forma parte del servicio solicitado.

CABLEADO ESTRUCTURADO PARA EQUIPOS ACCESS POINT

Suministro e instalación de nodo de cableado estructurado categoría 6 que incluye:

Cableado del tipo UTP cat. 6, jack, panel de parcheo, placas, dos patch cord, canalización, pruebas y todo lo necesario para que el nodo opere correctamente a una distancia máxima de 90 metros.

Esto aplica para los sitios que contienen servicios de red inalámbrica (Tipo 2 y Tipo 3).

**ACOMETIDA DE MEDIOS**

Suministro e instalación de acometidas de medios desde el primer registro del prestador de servicios, hasta el SITE de los edificios de SCJN.

Debe de incluir: Canalización y cableado de fibra óptica, ambos rematados en sus extremos.

Esto aplica para el total de sitios.

**RACK**

Suministro e Instalación de rack, charola, tira de 4 contactos dúplex, accesorios de aterrizaje, organizador vertical y 2 horizontales.

Esto aplica para el total de sitios.

**TIERRA FÍSICA**

Suministro e instalación de sistema de tierra física, a una distancia promedio de 50 metros,

Debe de incluir: ductería PVC, cable calibre 6 AWG color verde, zapatas ponchables de doble ojillo, cañón largo barra de cobre y todo lo necesario para su correcta instalación, fijación y funcionamiento, con una impedancia menor ó igual a 5 Ohms. Se debe de conectar el gabinete a la nueva tierra.

Esto aplica para el total de sitios.

**PATCH CORD**

Se debe de incluir Patch cord de 3 metros categoría 6 de fábrica y Jumper de fibra óptica multimodo de 3 metros dúplex necesarios para interconectar todos los equipos de la solución propuesta.

Esto aplica para el total de sitios.

**ALIMENTACIÓN ELÉCTRICA**

Se deberá de proporcionar suministro e instalación de Alimentación eléctrica 127 volts (1 línea) para IDF, además deberá considerar un contacto eléctrico dúplex para IDF a pie de gabinete para energizar la barra de contactos eléctrica a 127 volts para la alimentación de los equipos, en el caso de los sitios Tipo 1 y 2 se deberá considerar la barra de contactos con conector NEMA L6-30P a 220 volts, para la alimentación de los equipos.

Esto aplica para el total de sitios.

**SISTEMA DE RESPALDO UPS**

Se deberá de suministrar e instalación el respaldo de energía (UPS) el cual debe de incluir: Tarjeta de monitoreo, configuración, con 4 minutos de respaldo a plena carga del tipo On Line, para respaldo de energía de los equipos a suministrar en caso de falla eléctrica.

Esto aplica para el total de sitios.

**MANTENIMIENTOS**

Se requiere que el prestador de servicios proporcione el mantenimiento preventivo de la Infraestructura Auxiliar que considere durante la vigencia del servicio.

Se requiere que el prestador de servicios proporcione el mantenimiento correctivo de la Infraestructura Auxiliar durante todo el periodo del contrato y deberá de incluir refacciones o sustitución en caso de falla.

Esto aplica para el total de sitios.

**MEMORIA TÉCNICA**

El prestador de servicios deberá de proporcionar al final de los trabajos de instalación una Memoria Técnica en papel y medio electrónico, reflejando los aspectos técnicos de la infraestructura auxiliar implementada por sitio que deberá de incluir los siguientes rubros:

• Planos esquemáticos que incluyan ubicación de los servicios y trayectorias de canalizaciones.

• Diagramas esquemáticos de conexión.

Esto aplica para el total de sitios.

**APOYO A MIGRACIÓN**

El prestador de servicios deberá de cubrir el rubro de apoyo para realizar las migraciones correspondientes en cada uno de los sitios.

Esto aplica para el total de sitios.

Todas las instalaciones de equipo nuevo (eléctricas, telecomunicaciones o infraestructura) de los Centros de Datos de la Suprema Corte de justicia de la Nación, deberán de ser aprobados por la Dirección de Infraestructura y Seguridad de la DGTI, apegado a las políticas de seguridad de los Centros de Datos.

**Tabla Resumen de infraestructura Auxiliar por sitio:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Tipo de Sitio | | | | | | |
|  |  |  |  |  |  |  |  |  |
| Concepto |  | Tipo 2 y 3 | | Tipo 1, 4, 5 y 6. | | | Punto de Cons. 1 | Punto de Cons. 2 |
|  |  |  |  |  |  |  |  |  |
| Cableado estructurado para equipos Access Point |  | **X** | |  | | |  |  |
| Acometida de medios |  | **X** | | **X** | | | **X** | **X** |
| Gabinete |  | **X** | | **X** | | | **X** | **X** |
| Tierra Física |  | **X** | | **X** | | | **X** | **X** |
| Patch cord categoría 6 de fábrica |  | **X** | | **X** | | | **X** | **X** |
| Alimentación eléctrica |  | **X** | | **X** | | | **X** | **X** |
| Sistema de respaldo UPS |  | **X** | | **X** | | | **X** | **X** |
| Mantenimientos |  | **X** | | **X** | | | **X** | **X** |
| Memoria Técnica |  | **X** | | **X** | | | **X** | **X** |
| Apoyo a migración |  | **X** | | **X** | | | **X** | **X** |

# 

# SERVICIOS ADMINISTRADOS DE RED Y SEGURIDAD

# CENTRO DE OPERACIONES DE RED

Con la finalidad de facilitar a la SCJN un punto único de contacto (NOC por sus siglas en inglés), el prestador de servicios deberá brindar a través de un Centro de Operaciones de Red, servicios administrados para dar una respuesta efectiva a los incidentes presentados en los distintos servicios que son requeridos.

Los procesos del Centro de Operaciones de Red deberán estar diseñados bajo las mejores prácticas de ITIL y deberán estar certificados bajo la norma internacional ISO/IEC 20000:2011 e ISO/IEC 27001:2013. Lo cual será comprobable por medio de los certificados oficiales de ISO/IEC ya mencionados con un alcance en dicha certificación sobre la administración, gestión y monitoreo de redes de voz, datos, video e internet.

El Centro de Operaciones deberá proporcionar una mesa de servicio con cobertura 7x24x365, atendida por personal competente y orientado al cumplimiento de los objetivos de niveles de servicio, quienes deberán recibir, registrar, analizar y resolver los incidentes dando seguimiento al mismo hasta el restablecimiento del servicio afectado.

# DESCRIPCIÓN DEL SERVICIO Y SUS PROCEDIMIENTOS.

El prestador de servicios deberá proporcionar, por medio del Centro de Operaciones solicitado, los servicios de Administración de fallas, atención a ABCs (altas, bajas, cambios) y monitoreo del desempeño de los equipos.

Deberá realizar las actividades asociadas al servicio administrado comprendiendo las siguientes tres actividades:

1. Administración de Fallas: Para la detección y solución de las fallas que se presenten en el servicio.
2. Atención a Altas, Bajas y Cambios: Para el manejo de la información relativa a las configuraciones relacionadas con Altas, Bajas y Cambios de los equipos de red.
3. Monitoreo del Desempeño: Para la medición y determinación de los niveles de operación del servicio, en general.

Deberá de entregar el esquema de atención y los procedimientos correspondientes.

# ADMINISTRACIÓN DE FALLAS

El objetivo de la administración de fallas que proporcione el prestador de servicios deberá detectar, registrar, notificar y solucionar los incidentes que ocurran en la red, para mantenerla operando adecuadamente.

La administración de fallas deberá involucrar la determinación de los síntomas y el aislamiento del incidente, seguida de la reparación del mismo con pruebas de la solución y, finalmente, el registro de toda la información obtenida durante el proceso.

En la administración de fallas indicar el tipo de documentos que el prestador de servicios entregará para cada caso que se presente (antes, durante y después de las fallas) y las metodologías y/o procedimientos a seguir.

**Funciones**

* Descubrimiento y mapeo geográfico de los dispositivos de la red.

Por medio de una herramienta de monitoreo, se deberá detectar la presencia de todos los dispositivos activos de la red y se deberá generar un mapa geográfico.

* Monitoreo del servicio.

Se deberá tener un monitoreo continuo de la actividad de los dispositivos del servicio, mediante una representación gráfica de la herramienta de monitoreo, donde se indique, por medio de diferentes colores, el estado operacional de cada dispositivo.

* Detección y administración de incidentes.

Se deberá tener una detección proactiva de incidentes en los elementos de red en base a la detección de alarmas. Los dispositivos de red deberán tener la capacidad de alertar al sistema de administración y monitoreo, mediante la generación de una alarma al enviar un “trap”, cuando ocurre una falla en el sistema, de tal manera que se puedan tomar acciones correctivas.

* Solución de incidentes.

Una vez detectada una situación de falla, se deberá abrir un caso o ticket en la herramienta de administración de incidentes y se deberá iniciar el proceso de solución de la misma, el cual deberá incluir soporte de primero, segundo y tercer nivel, de la siguiente manera:

1. **Soporte de Primer Nivel:**

Para los equipos de voz y video, se deberá proporcionar en sitio por medio de un servicio de ingeniería en un horario de 9:00hrs a 19:00hrs en el sitio de 16 de septiembre o Pino Suarez, de Lunes a Viernes, fuera de este horario deberá proporcionarse remotamente a través del Centro de Operaciones, el cual deberá contar con ingenieros especializados en los equipos incluidos en la solución.

Para el resto del equipamiento de red, se deberá proporcionar el soporte de primer nivel de forma remota desde el Centro de Operaciones de red de “EL PRESTADOR DE SERVICIOS”.

1. **Soporte de Segundo Nivel:**

Cuando la falla de un equipo no pueda ser resuelta remotamente, la falla deberá ser canalizada a un ingeniero de soporte de “EL PRESTADOR DE SERVICIOS” que deberá acudir con las herramientas y refacciones necesarias a la localidad donde se suscitó la falla.

1. **Soporte de Tercer Nivel:**

De ser necesario para la solución de la falla, el centro de operaciones deberá escalar el problema al fabricante del equipo en cuestión.

**Herramientas**

El prestador de servicios deberá contar con al menos las siguientes herramientas para la administración de fallas:

* Consola gráfica de monitoreo y detección de incidentes.

Esta herramienta deberá consistir en una consola que realiza las funciones de descubrimiento y mapeo de los elementos y dispositivos de la red. Cada elemento o dispositivo deberá ser desplegado en forma gráfica en una pantalla, indicando, por medio de colores su estado operacional. Los dispositivos de la red deberán ser configurados para enviar notificaciones o traps SNMP a la consola en la ocurrencia de incidentes. Al ser recibida la notificación, el elemento gráfico que representa a dicho dispositivo deberá cambiar a un color diferente, dependiendo de la definición de umbrales que se realice para las alarmas específicas con la SCJN.

* Herramienta para el registro y administración de incidentes.

La herramienta de administración de incidentes o “trouble ticket” deberá permitir el registro de los incidentes y darles continuidad hasta su solución, indicando fecha y hora de apertura del caso, tiempo de atención y fecha y hora de cierre del caso.

Ambas herramientas deberán poder ser visualizadas por La SCJNa través de un Portal web tipo “Dashboard”, con 4 accesos simultáneos, y con seguridad.

# ATENCIÓN A ALTAS BAJAS Y CAMBIOS.

La atención a altas bajas y cambios tiene como fin el manejo y control de la información relativa a los movimientos ABC de los dispositivos. El prestador de servicios deberá garantizar que todos los movimientos a los dispositivos de la red (altas, bajas, cambios), se realicen mediante el uso correcto de los procesos de gestión de cambios, liberaciones y configuraciones para asegurar el cumplimiento de los niveles de servicio establecidos.

Los alcances son:

* Altas, bajas y cambios, vía acceso remoto, a los equipos de la red
* Control y administración de bitácoras de los equipos de la red.
* Control, mantenimiento y actualización de inventarios.
* Administración de los Niveles de Servicio y control de cambios
* Administración, mantenimiento, actualización y respaldo de configuraciones de los equipos

La administración de configuraciones debe tener como fin el manejo y control de la información relativa al inventario de dispositivos de la red, así como de sus configuraciones, de tal manera que los cambios de configuración y actualizaciones de versión de hardware y software no tengan impacto en la operación de la red.

Cada elemento de red tiene una variedad de información, en diferentes versiones, asociada a éste. Un sistema de administración de configuraciones deberá almacenar toda esta información en una base de datos de fácil acceso, la cual deberá ser consultada en el momento en que ocurra un problema en la red, para ayudar a resolverlo.

**Funciones:**

* Deberá administrar la nomenclatura. Identifica por nombre de los elementos de la red (equipos, interfaces, DLCIs, direccionamiento IP, etc.).
* Deberá asegurar la integridad de las configuraciones.
* Deberá resguardar y respaldar las configuraciones de los equipos de la red, en servidores o dispositivos de almacenamiento.
* Deberá llevar una administración de inventarios
* Deberá utilizar la funcionalidad de descubrimiento de elementos de red, para mantener una base de datos con información detallada de cada equipo de la red, incluyendo:
  + Ubicación
  + Modelo de hardware
  + Módulos instalados
  + Software instalado
  + Versiones de HW y SW
  + Números de serie

El prestador de servicios deberá de entregar el procedimiento o la metodología utilizada para el control de cambios.

# MONITOREO DEL DESEMPEÑO

El objetivo del monitoreo del desempeño deberá ser la medición y recolección de información estadística relativa a diversos parámetros de operación dispositivos y enlaces asociados al servicio administrado con objeto de determinar su nivel de desempeño.

**Funciones**

* Se deberá realizar una recolección periódica de diferentes valores de desempeño de los servicios mediante mecanismos de sondeo periódico (poleo estándar de 5 minutos) en cada dispositivo, para la medición de parámetros concernientes al comportamiento de dichos dispositivos, tales como:
  + Mediciones de desempeño de equipo:

Deberá dar a conocer el nivel de funcionamiento interno de los dispositivos de red para determinar la necesidad de reemplazar o incrementar la capacidad de los mismos para atender suficientemente las demandas de la red.

* + Mediciones de rendimiento:

Deberá permitir conocer el desempeño del servicio para transmitir y/o recibir información y son la guía para la vigilancia del cumplimiento de los Niveles de Servicio (SLA’s) comprometidos.

* + Mediciones de tráfico y utilización de los medios:

Deberá definir las características bajo las cuales están trabajando los elementos que componen la red. Permitirá a la SCJN obtener parámetros para visualizar las tendencias de su comportamiento con el fin de planear y decidir sobre las estrategias de crecimiento y mantenimiento de su red.

Almacenamiento y representación gráfica de la información recolectada. Esta información deberá ser utilizada para la visualización a través de la herramienta de autoservicio “Dashboard” para la cual se deberá proporcionar 3 usuarios y contraseñas a los administradores definidos por la SCJN. La información deberá estar disponible en línea en el portal por un mes, y deberá estar disponible para descargar por parte del usuario determinado.

# REPORTES

Se deberán entregar de forma mensual, como máximo en los primeros 7 días hábiles del mes, los siguientes reportes:

1. **Reporte de Desempeño**. Deberá permitir que se conozca el desempeño de los componentes de la red.

**CPE**

* TOP Utilización CPU
* TOP Utilización memoria
* TOP Disponibilidad
* Utilización CPU, Memoria
* Disponibilidad

**Medio de transmisión**

* TOP Utilización ancho de banda (entrada y salida)
* TOP Latencia
* TOP Errores
* TOP Descartes
* Utilización ancho de banda de entrada y salida
* Errores y Descartes
* TOP Utilización ancho de banda por calidad de servicio
* Utilización ancho de banda por calidad de servicio

1. **Reporte Ejecutivo,**  deberá integrar los siguientes componentes:

* Datos generales del proyecto
* Cumplimiento de niveles de servicio
* Histórico de indicadores.
* Disponibilidad,
* Índice de falla,
* % Incidentes resueltos < 7 h,
* Incidentes resueltos > 7 h,
* % Proactividad,
* Sitios reincidentes,
* Índice de sitios reincidentes,
* Sitios fuera de disponibilidad y MTTR

1. **Reporte Operativo,** deberá integrar los siguientes componentes:

* Comportamiento a tres meses en sitios, equipamiento y medio de transmisión
* Distribución por tipo de reporte
* Distribución de incidentes por responsable
* Distribución de incidentes por prioridad
* Proactividad (sobre elementos monitoreables)
* Distribución por tiempo de solución
* Distribución por tiempo de solución de fallas de energía
* Clasificación por código de cierre
* Sitios reincidentes

1. **Reporte de Disponibilidad,** deberá integrar los siguientes componentes:

* Disponibilidad de la Red
* Disponibilidad por tipo de sitio
* Distribución de sitios fuera o dentro de disponibilidad
* Sitios fuera de disponibilidad
* Disponibilidad por sitio

1. **Presentación ejecutiva**. Deberá permitir que se conozca de una manera rápida el desempeño y comportamiento de la Red, mediante una presentación que concentre lo más relevante del reporte de desempeño y los reportes de comportamiento.

Deberá integrar los siguientes componentes:

* Indicadores
* Análisis operativo
* Análisis performance
* Recomendaciones
* Información adicional

La Dirección General de Tecnologías de la Información podrá solicitar cualquier reporte a la medida cuando lo considere pertinente.

# NIVELES DE SERVICIO DEL NOC

A continuación se describen los niveles de servicio que se deberán proporcionar por parte del NOC:

|  |  |  |
| --- | --- | --- |
| **CONCEPTO** | **DESCRIPCIÓN** | **NIVEL DE SERVICIO** |
| Disponibilidad | Es la disponibilidad sobre todos los componentes del servicio que proporciona el NOC. | 99% |
| Asertividad en el diagnóstico | Es el porcentaje de incidentes en el que el diagnóstico inicial está de acuerdo a la solución de la falla | 90% |
| Tiempo máximo de contestación de llamadas | Es el porcentaje de llamadas en las que el tiempo máximo de contestación es de 30 segundos a partir de que el IVR transfiere la llamada y es contestada por un operador. | 95% |
| Abandono de llamadas | Es el porcentaje de llamadas no contestadas en relación al total de llamadas entrantes. | < 5% |
| Tiempo de Inicio de Atención | Es el porcentaje de incidentes en los que el tiempo máx. para el inicio de atención es de 15 minutos ya sea que este provenga de una detección proactiva o por una petición de la SCJN | 95% |
| Proactividad | Es el porcentaje de incidentes detectados de forma oportuna por inactividad o pérdida de conectividad en los dispositivos monitoreables | 95% |
| Retroalimentación | Porcentaje de casos retroalimentados durante la primera hora. | 95% |

Como parte de los entregables mensuales, se deberá entregar un reporte de cumplimiento de los niveles de servicio del NOC.

# CENTRO DE OPERACIONES DE SEGURIDAD - SOC

Es requisito que el prestador de servicios aplique a sus procesos de operación de todos los servicios solicitados la metodología denominada ITIL (Information Technology Infrestructure Library), así como el estándar de seguridad de la información ISO 27000, deberá asumir las siguientes responsabilidades mostradas en forma enunciativa y no limitativa:

* Administración de los equipos que confirman la solución de Seguridad Informática para la Red Privada Virtual de la SCJN.
* Administración de la disponibilidad y continuidad de los servicios de seguridad informática.
* Administración de incidentes de seguridad informática.
* Administración de cambios de los servicios de seguridad informática.
* Administración de los servicios y reportes de seguridad informática.
* Administración del mantenimiento preventivo y correctivo de los equipos de seguridad.
* Gestión de vulnerabilidades de todos los equipos que integrarán el servicio de Red Privada Virtual de la SCJN.

El prestador de servicios deberá proporcionar un servicio de Centro de Operaciones de Seguridad, el cual se encargará de la atención de reportes, fallas, incidentes, mantenimientos y requerimientos en la infraestructura de seguridad informática que dará soporte a los servicios de la Red Privada Virtual de la SCJN.

* El SOC del prestador de servicios se encargará del monitoreo, identificación, análisis, registro y resolución de cualquier incidente en materia de seguridad informática que pudieran llegar a comprometer la disponibilidad e integridad de los servicios de la Red Privada Virtual de la SCJN
* El SOC del prestador de servicios deberá estar conformado por personal altamente capacitado en las distintas ramas de seguridad informática, análisis forense, telecomunicaciones, auditoria informática, así como atención y respuesta a incidentes.
* El SOC del prestador de servicios deberá contar con las herramientas especializadas de hardware y software necesarias para atender cualquier incidente de seguridad informática de los servicios y portales web de la SCJN, entre las cuales se pueden mencionar las siguientes: correlacionador de eventos, escáner para análisis de flujos de red, herramientas de análisis forense, herramientas para análisis de logs, herramientas para análisis de malware, etc.

Condiciones necesarias para el Servicio de SOC:

* El SOC del prestador de servicios se encargará de analizar, evaluar y proponer a la SCJN mejoras o adecuaciones en las políticas y controles de los servicios que conforman la Seguridad informática para el servicio de la Red Privada Virtual de la SCJN.
* El SOC del prestador de servicios se encargará de realizar un proceso de análisis de vulnerabilidades sobre toda la infraestructura que integrarán el servicio de Red Privada Virtual de la SCJN, presentará los reportes de vulnerabilidades detectadas y establecerá y aplicará el plan de remediación correspondiente. Este proceso se deberá realizar al inicio de la prestación del servicio, así como un mínimo de cada 6 meses por la duración del contrato.
* El SOC del prestador de servicios se encargará de monitorear y analizar el tráfico de red del servicio de Red Privada Virtual de la SCJN, con la finalidad de identificar y mitigar cualquier tráfico anómalo o ataque informático.
* El SOC del prestador de servicios se encargará de recolectar, analizar y correlacionar los registros (logs) de los equipos que conforman la seguridad perimetral, telecomunicaciones y equipos de servicios, con la finalidad de identificar cualquier comportamiento anómalo.
* El SOC del prestador de servicios se encargará establecer y ejecutar un plan de atención y respuesta a incidentes de seguridad informática para los servicios de la Red Privada Virtual de la SCJN, mismo que será validado por el personal técnico que designe la SCJN.
* Ante un incidente de seguridad en la Red Privada Virtual de la SCJN, el SOC del prestador de servicios se encargará de determinar las causas y afectaciones del incidente, elaborará un informe detallado, propondrá y ejecutará las medidas de remediación necesarias.
* Notificación de incidentes:
* El servicio será proporcionado las 24 horas los 365 días del año.
* El prestador de servicios deberá contar con personal capacitado para identificar, atender y notificar cualquier incidente de seguridad en los servicios de la Red Privada Virtual de la SCJN
* Se deberá manejar el marco de referencia ISO 27000 para el establecimiento de controles de seguridad informática en los procesos de la Red Privada Virtual de la SCJN
* Se deberá manejar un proceso de atención y notificación de incidentes mediante la metodología ITIL.

Se deberán entregar de forma mensual, como máximo en los primeros 7 días hábiles del mes, los siguientes reportes:

* Reporte de disponibilidad de la infraestructura de seguridad informática, donde se incluya la disponibilidad por servicio.
* Reporte de tráfico malicioso y ataques de DDoS identificados por la herramienta durante el periodo. Se deberá indicar el país de origen y el tipo de tráfico identificado.
* Informe de políticas Firewall configuradas.
* Reporte ataques identificados por la infraestructura de seguridad durante el periodo. Se deberá indicar el país de origen y el tipo de tráfico identificado.
* Informe de ataques y comportamiento anómalos registrados durante el periodo.
* Reporte de vulnerabilidades así como su remediación
* Reporte de las actividades realizadas por el SOC durante el periodo de servicio.
* Informes de los incidentes de seguridad registrados en el periodo y su solución.

# NIVELES DE SERVICIO PARA LOS SERVICIOS SOLICITADOS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Niveles de servicio** | | | | |
| **ID** | **Descripción del servicio** | **Métrica** | **Periodicidad** | **Nivel de servicio solicitado** |
| 1 | Afectación de los servicios de la red VPN-MPLS, incluyendo equipos involucrados | Disponibilidad comprometida  Tipo 1 y 2 (Enlaces Redundantes) | 24x7x365 | >= 99.99 % Disponibilidad Mensual |
| Disponibilidad comprometida  Tipo 3, 4, 5 y 6 | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| 2 | Afectación de los servicios de internet, incluyendo equipos involucrados | Disponibilidad comprometida  Tipo 2 y 3 | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| Disponibilidad comprometida  Puntos de consolidación de infraestructura y servicios. | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| 3 | Afectación del servicio de Seguridad Perimetral, incluyendo equipos involucrados | Tiempo de solución comprometido | 24x7x365 | 6 horas tiempo máximo de solución |
| 4 | Afectación del servicio de Ciberseguridad, incluyendo equipos involucrados | Tiempo de solución comprometido | 24x7x365 | 6 horas tiempo máximo de solución |
| 5 | Afectación del Servicio de telefonía IP en el sistema central con redundancia geográfica, incluyendo equipos involucrados | Tiempo de solución comprometido.  Se considera como servicio activo siempre y cuando cualquiera de los componentes centrales de las dos ubicaciones este proporcionando el servicio de telefonía IP | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| 6 | Afectación de los componentes periféricos de telefonía | Tiempo de solución comprometido | 24x7x365 | 12 horas tiempo máximo de solución |
| 7 | Afectación del sistema central de Videoconferencia con redundancia geográfica, incluyendo equipos involucrados | Tiempo de solución comprometido  Se considera como servicio activo siempre y cuando cualquiera de los componentes centrales de las dos ubicaciones este proporcionando el servicio | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| 8 | Afectación de los componentes periféricos de videoconferencia (codec´s, pantallas, micrófonos, cámaras, etc.) | Tiempo de solución comprometido | 24x7x365 | 12 horas tiempo máximo de solución |
| 9 | Afectación del sistema central (controladoras) de la red inalámbrica en alta disponibilidad geográfica, incluyendo equipos involucrados | Tiempo de solución comprometido  Se considera como servicio activo siempre y cuando cualquiera de los componentes centrales de las dos ubicaciones este proporcionando el servicio | 24x7x365 | >= 99.92 % Disponibilidad Mensual |
| 10 | Disponibilidad de servicios periféricos de la Red inalámbrica corporativa | Tiempo de solución comprometido | 24x7x365 | 12 horas tiempo máximo de solución |
| 11 | Disponibilidad de la red inalámbrica de invitados, incluyendo equipos involucrados | Tiempo de solución comprometido | 24x7x365 | 12 horas tiempo máximo de solución |
| 12 | Disponibilidad del servicio de Red LAN, incluyendo equipos involucrados | Tiempo de solución comprometido | 24x7x365 | 4 horas tiempo máximo de solución |

# INSTALACIÓN DEL SERVICIO

* El prestador de servicios deberá de realizar la instalación, implementación y puesta a punto de todos los elementos solicitados dentro del servicio.
* El prestador de servicios deberá de proporcionar todos los insumos necesarios para la correcta instalación de la solución propuesta.
* El prestador de servicios deberá entregar los documentos donde presente la logística de instalación y un de plan de trabajo considerando lugares y tiempos de configuración e instalación; así como la fuerza laboral asignada.
* El prestador de servicios deberá de proporcionar al término de la implementación de los servicios la Memoria Técnica donde se plasme la visión y estatus final de cómo queda el servicio, incluyendo al menos las configuraciones, diagramas y relación de equipamiento.
* El prestador de servicios será responsable de contemplar los viáticos necesarios para el personal que asigne para dicha actividad.
* El prestador de servicios deberá incluir en una CMDB todos los equipos instalados.

# MANTENIMIENTO CORRECTIVO Y PREVENTIVO

# CORRECTIVO

Es responsabilidad del prestador de servicios realizar los mantenimientos correctivos necesarios de los elementos propuestos dentro de cada una de las soluciones de sus servicios incluyendo refacciones (software y hardware), mano de obra y se realizarán dentro de los tiempos establecidos de acuerdo a los niveles de servicio.

El prestador de servicios será responsable de contemplar los viáticos necesarios para el personal que asigne para dicha actividad.

# PREVENTIVO

Se deberá realizará mantenimiento preventivo a todos los elementos de la solución ofertada cuando el prestador de servicios lo considere necesario. Para esto se acordara un calendario de mantenimiento preventivo con La SCJN por lo menos 15 días hábiles de anticipación. Sin afectar tiempos críticos de la jornada laboral de los usuarios finales y sin representar costo adicional para la SCJN.

El servicio de mantenimiento preventivo deberá incluir refacciones y mano de obra así como la limpieza de los equipos. Por lo que el prestador de servicios debe de contar con la infraestructura necesaria que le permita proporcionar este servicio.

El prestador de servicios será responsable de contemplar los viáticos necesarios para el personal que asigne para dicha actividad.

Aprobaciones

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha de elaboración | | | 27/09/2017 |
| Rol | Nombre | Cargo | Firma |
| **Elaboración** | Ing. Luis Corro Ajungo | Subdirector de Área |  |
| **Revisión** | Mtro. Gonzalo Trujillo Marquez | Director de Área |  |
| **Revisión** | Lic. Javier Sánchez Valtierra | Director de Área |  |
| **Aprobación** | Lic. Martín Moriyama Nakaoka | Subdirector General |  |
| **Autorizó** | Lic. Enrique Gameros Hidalgo Monroy | Director General |  |