**SEGURIDAD FIREWALL Y NAC**

**ESPECIFICACIONES TÉCNICAS**

**ÍNDICE**

[1 SERVICIOS DE SEGURIDAD PERIMETRAL DE RED 4](#_Toc21013992)

[2 CARACTERÍSTICAS DEL SERVICIO 4](#_Toc21013993)

[2.1 PARA LOS SERVICIOS DE SEGURIDAD EL PROVEEDOR DEBERÁ OFERTAR EN SU PROPUESTA TÉCNICA LAS SIGUIENTES FUNCIONES: 4](#_Toc21013994)

[3 CARACTERÍSTICAS MÍNIMAS DE LOS EQUIPOS 7](#_Toc21013995)

[3.1 FIREWALL TIPO 1 7](#_Toc21013996)

[3.2 FIREWALL TIPO 2 8](#_Toc21013997)

[4 SERVICIO DE CONTROL DE ACCESO A LA RED (NAC) 9](#_Toc21013998)

[5 CAPACIDADES 9](#_Toc21013999)

[6 GARANTÍAS, SOPORTE Y ACTUALIZACIÓN PARA ADQUISICIÓN DE EQUIPOS 10](#_Toc21014000)

[6.1 GARANTÍA HARDWARE 10](#_Toc21014001)

[6.2 GARANTÍA DE SOFTWARE. 10](#_Toc21014002)

[7 GARANTÍA SOPORTE Y ACTUALIZACIÓN PARA ARRENDAMIENTO DE EQUIPOS 10](#_Toc21014003)

[7.1 GARANTÍA HARDWARE 11](#_Toc21014004)

[7.2 GARANTÍA DE SOFTWARE. 11](#_Toc21014005)

[8 SOPORTE TÉCNICO PARA HARDWARE Y SOFTWARE. 11](#_Toc21014006)

[9 MEDIOS PARA REPORTAR FALLAS Y HACER EFECTIVAS LAS GARANTÍAS: 11](#_Toc21014007)

[10 CONSIDERACIONES PARA EL PROCEDIMIENTO DE CONTRATACIÓN 12](#_Toc21014008)

[10.1 ADQUISICIÓN 12](#_Toc21014009)

[10.2 ARRENDAMIENTO 12](#_Toc21014010)

[11 CERTIFICACIONES 13](#_Toc21014011)

[12 CAPACITACIÓN. 13](#_Toc21014012)

[13 INSTALACIÓN 13](#_Toc21014013)

[14 ENTREGABLES 14](#_Toc21014014)

[14.1 MEMORIA TÉCNICA 14](#_Toc21014015)

[15 SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN Y MIGRACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD FIREWALL Y NAC 15](#_Toc21014016)

[16 TRANSICIÓN DE LOS SERVICIOS POR TÉRMINO DE CONTRATO DE ARRENDAMIENTO 16](#_Toc21014017)

[17 MESA DE SERVICIO PARA SEGURIDAD FIREWALL Y NAC 17](#_Toc21014018)

# SERVICIOS DE SEGURIDAD PERIMETRAL DE RED

El servicio deberá incluir como mínimo los elementos de hardware, software y funcionalidades requeridas en estas especificaciones técnicas. Como referencia y para garantizar la operación del servicio de seguridad de red, EL PROVEEDOR deberá ofertar en su propuesta, soluciones en donde el fabricante esté ubicado y reconocido dentro de los cuadrantes de Gartner, el más reciente divulgado a la fecha de la publicación de la convocatoria, o en algún otro reporte reconocido por la industria a nivel internacional.

De ser requerido por ENTIDAD se deberá implemente un esquema de alta disponibilidad activo/pasivo, en el cual el firewall activo pueda procesar todo el tráfico

EL PROVEEDOR en su propuesta deberá considerar en partidas separadas el hardware y de software a fin de tener la mejor oferta y servicio.

# CARACTERÍSTICAS DEL SERVICIO

EL PROVEEDOR deberá incluir en su propuesta, todo el Licenciamiento, Hardware y Software necesario, para proporcionar de inicio, la totalidad de Servicios de Seguridad con funcionalidades asociadas que se requieran, conforme a los perfiles y cantidades indicadas para cada tipo de Firewall. Deberá soportar configuraciones en alta disponibilidad.

## PARA LOS SERVICIOS DE SEGURIDAD EL PROVEEDOR DEBERÁ OFERTAR EN SU PROPUESTA TÉCNICA LAS SIGUIENTES FUNCIONES:

1. **Control de políticas**
2. Permite a los usuarios configurar políticas de seguridad en función del tiempo, usuario / grupo de usuarios / grupo de seguridad, protocolo de capa de aplicación, ubicación geográfica, dirección IP, puerto, grupo de nombre de dominio, categoría de URL, tipo de acceso, tipo de terminal, grupo de dispositivos.
3. Deben de ser capaces de manejar protocolos tales como RADIUS o KERBEROS.
4. **Enrutamiento**
5. Admite rutas estáticas, enrutamiento basado en políticas y protocolos de enrutamiento dinámicos como RIP, OSPF, BGP e IS-IS (opcional) en sus últimas versiones estables.
6. El enrutamiento basado en políticas admite las siguientes condiciones coincidentes: dirección IP de origen, dirección IP de destino, tipo de servicio, tipo de aplicación, usuario / grupo de usuarios / grupo de seguridad, interfaz de entrada y prioridad DSCP.
7. Deberá de soportar la encapsulación de tráfico IPv4 e IPv6
8. **Protocolos Avanzados de VPN**
9. Especificaciones IKE
10. Versión 1, Versión 2
11. Modo de Negociación: Automático, Main, Aggressive (soportado únicamente en topología hub and spoke (star))
12. Encriptación: AES-256, AES-192, AES-128, 3DES, DES
13. Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5
14. Integridad Hash: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES
15. PRF: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES-128
16. Grupo DH: 1,2,5,14,15,16,18,19,20,21
17. Especificaciones IPSec
18. Modo de encapsulación: Automático, Transport, Tunnel
19. Protocolo de seguridad: ESP, AH, AH-ESP
20. ESP Encriptación: GCM256, GCM192, GCM128, GMAC256, GMAC192, GMAC128, AES-256, AES-192, AES-128, 3DES, DES
21. ESP Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5
22. PFS: 1,2,5,14 opcional,15 opcional,16 opcional,18,19,20,21
23. DPD modos: Periodic, On-Demand
24. L2TP
25. L2TP over IPSec
26. GRE
27. Multipoint ) (opcional
28. **Identificación de aplicaciones**
29. **IPv6**
30. Soporta el protocolo IPv6.
31. Compatible con IPv6 sobre túneles GRE de IPv4 y túneles 6RD.
32. **Control de tráfico**
33. Admite políticas de control de tráfico basadas en el protocolo de la capa de aplicación, incluida la configuración del ancho de banda máximo, el ancho de banda garantizado y la prioridad del tráfico del protocolo.
34. Admite garantía de ancho de banda basada en usuarios y direcciones IP.
35. Admite el número máximo de conexiones por dirección IP o usuario.
36. Admite el tráfico basado en la ubicación geográfica y el análisis de amenazas.
37. Soporta la gestión de cuotas de tráfico de usuarios.
38. Soporta traffic shaping.
39. Proporcionar protección y soporte al menos a las siguientes tecnologías de Voz sobre IP: SIP, H.323, H.460, ICE / STUN para tráfico cifrado y calidad de servicio.
40. **Gestión de políticas**
41. Admite la prevención de fugas de datos para identificar y filtrar archivos y contenido (diferentes tipos de información, como tarjetas de identificación, tarjetas de crédito, tarjetas de débito y de seguridad social) en tránsito.
42. Admite el filtrado de URL mediante la implementación de un servidor de URL local.
43. Admite el filtrado de DNS para mejorar el rendimiento del filtrado de páginas web.
44. Es compatible con SafeSearch para filtrar el contenido no saludable devuelto por los motores de búsqueda como Google.
45. Las reglas de firewall deberán poder tener vigencia con base a fechas (incluyendo día, mes y año).
46. **NAT**
47. Admite funciones NAT completas y NAT ALG para múltiples protocolos de capa de aplicación, incluidos ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, QQ, MSN y MMS.
48. Admite monitorear el NAT.
49. Hacer traslación de direcciones estático, uno a uno.
50. Hacer traslación de direcciones dinámico, muchos a uno.
51. Soportar NAT Traversal (opcional)
52. **Prevención de intrusiones y antivirus.**
53. Admite la personalización de plantillas de políticas de prevención de intrusiones basadas en escenarios.
54. Admite la prevención de craqueo de fuerza bruta para servicios de aplicaciones comunes (HTTP, FTP, SSH, SMTP e IMAP, VoIP, SIP) y software de base de datos (MySQL, Oracle y MSSQL).
55. Admite el filtrado basado en nombres de dominio malintencionados para bloquear C&C.
56. Admite antivirus para protocolos como HTTP, FTP, SMTP, POP3, IMAP y NFS.
57. Soporte de detección y bloqueo de ataques.
58. **Protección de seguridad de tráfico cifrado.**
59. Descifra el tráfico HTTPS, POP3S, SMTPS e IMAPS y realiza filtrado de datos, auditoría y protección de seguridad en el tráfico descifrado.
60. Soporta descifrado refinado basado en categorías de URL para mejorar el rendimiento del descifrado.
61. Descifra el tráfico y lo refleja en dispositivos de terceros para auditoría y detección de seguridad.
62. **Autenticación de usuario de acceso a la red**
63. Compatible con AD (directorio activo) SSO (Single Sing-On), RADIUS SSO (Single Sing-On), autenticación NTLM, sin autenticación, autenticación MAC y autenticación SMS.
64. Es compatible con grupos de seguridad dinámicos para autorizar dinámicamente organizaciones horizontales.
65. Soporta múltiples dominios de autenticación para cumplir con los requisitos de administración independiente y autenticación de múltiples sucursales.
66. Soporta la personalización de la página del portal y cuestionarios para promover el marketing.
67. **Gestión centralizada**.
68. Admite la actualización mediante una unidad flash USB para reducir los costos de O&M (opcional).
69. Proporciona interfaces API de integración hacia el norte, como RESTCONF y NETCONF para conectarse a plataformas de administración de terceros.
70. Soportar los protocolos SNMP RFC 1157, SNMPv2c o SNMPv3
71. **Autenticación 802.1X**
72. Admita el paso del proceso de la autenticación 802.1X para garantizar la seguridad del acceso a la red Wi-Fi o en la LAN.
73. **Selección de enlace ascendente inteligente**
74. Selecciona de forma inteligente los enlaces del operador en función de las direcciones IP de destino, admite la configuración de la interfaz activa / en espera y el equilibrio de carga por porcentaje
75. Soportar QoS basada en colas inteligentes.

# CARACTERÍSTICAS MÍNIMAS DE LOS EQUIPOS

Las funcionalidades y características antes descritas aplican para cada uno de los tipos de Firewall requeridos.

## FIREWALL TIPO 1

Las especificaciones son las mínimas más no limitativas.

|  |  |
| --- | --- |
| Indicador | Requisito de especificación técnica |
| Requisitos de configuración física. | ≥ 2,000 Usuarios de VPN SSL simultáneos,  ≥ 10,000 Túneles de VPN IPSec  ≥ 150 Firewalls virtuales |
| Arquitectura de hardware | □ Fuentes de poder **redundantes** |
| Requisitos de interfaces | ≥ 12 Número máximo de puertos  ≥ 8 Puertos 10/100/1000 base T GE.  ≥ 4 Puertos ópticos 1GE SFP |
| □ Tarjetas de bypass de puertos eléctricos |
| Requisitos de desempeño | ≥ 8 Gbps Rendimiento IPv4 de Firewall (Throughput).  ≥ 8 Gbps Rendimiento IPv6 de Firewall (Throughput).  ≥16 Gbps Rendimiento Protección Real de Firewall (EMIX Throughput) (opcional).  ≥ 4 Gbps Rendimiento inspección SSL.  ≥ 5,000,0000 Número de conexiones simultáneas.  ≥ 5,000 Número de conexiones simultáneas SSL VPN (Throughput).  ≥ 5,000 Número de conexiones nuevas por segundo.  ≥512 Mb IPsec VPN Throughput (AES-128+SHA1, 1420-byte).  ≥ 5,000 Número máximo de IPSec túneles (site to site).  ≥ 5,000 Número máximo de IPSec túneles (client to site).  ≥ 5,000 Número máximo de Políticas de seguridad. |
| VLANs | ≥ 1,024 Número máximo de Vlans. |

Tabla 1. Firewall Tipo 1

## FIREWALL TIPO 2

Las especificaciones son las mínimas más no limitativas.

|  |  |
| --- | --- |
| Indicador | Requisito de especificación técnica |
| Requisitos de configuración física. | ≥10,000 Usuarios de VPN SSL simultáneos.  ≥20,000 Túneles de VPN IPSec  ≥ 250 Firewalls virtuales |
| Arquitectura de hardware | □ Fuentes de poder **redundantes** |
| Requisitos de interfaces | ≥ 12 Número máximo de puertos  ≥ 8 Puertos 10/100/1000 base T GE.  ≥ 4 Puertos ópticos 1GE SFP  ≥ 2 Puertos 10GE SFP |
| □ Tarjetas de bypass de puertos eléctricos |
| Requisitos de desempeño | ≥ 10 Gbps Rendimiento IPv4 de Firewall (Throughput).  ≥ 10 Gbps Rendimiento IPv6 de Firewall (Throughput).  ≥ 20 Gbps Rendimiento Protección Real de Firewall (EMIX Throughput).  ≥ 10 Gbps Rendimiento inspección SSL.  ≥ 8,000,000 Número de conexiones simultáneas.  ≥ 10,000 Número de conexiones simultáneas SSL VPN (Throughpu).  ≥ 70,000 Número de conexiones nuevas por segundo.  ≥ 1 Gb IPsec VPN Throughput (AES-128+SHA1, 1420-byte).  ≥ 10,000 Número máximo de IPSec túneles (site to site).  ≥ 10,000 Número máximo de IPSec túneles (client to site).  ≥ 10,000 Número máximo de Políticas de seguridad. |
| VLANs | ≥ 1,024 Número máximo de Vlans. |

Tabla 1. Firewall Tipo 2

# SERVICIO DE CONTROL DE ACCESO A LA RED (NAC)

La solución de control de acceso debe ser compatible con las plataformas de LAN y WLAN.

# CAPACIDADES

Capacidad de operar en modo HA activo-pasivo.

* Soporte incluido para la cantidad de dispositivos definidos en el Apéndice A, autenticados de forma simultánea con capacidad para generar un cluster (o similar) que permita operar a la totalidad de dispositivos NAC como una sola entidad.
* Soportar al menos 2 puertos Gigabit Ethernet base-T.
* Soportar administración vía web (http, https).
* Debe identificar los dispositivos que intentan conectarse a la red, para validar si cumplen con los requerimientos mínimos para su acceso a la red.
* Soportar un cliente que supervisará las políticas establecidas y se realizará la remediación al dispositivo para dar cumplimiento a las políticas de acceso.
* Soporte de autenticación estará basada en 802.1X.
* Soportar integración con LDAP.
* Soportar portal de autenticación para invitados.
* Soportar bypass en caso de contingencia.
* Soporte de protocolos de autenticación de RADIUS:
* PAP
* CHAP
* MS-CHAP
* EAP-TTLS
* PEAP
* EAP-MSCHAPv2
* EAP-TLS

Debe mostrar información de los terminales conectados:

* Dirección MAC
* Dirección IP
* Tipo de dispositivo
* Tipo de autenticación
* Perfil
* Fecha de registro.

# GARANTÍAS, SOPORTE Y ACTUALIZACIÓN PARA ADQUISICIÓN DE EQUIPOS

Para todos los componentes de la solución ofertada se deberán otorgar las siguientes garantías, soporte técnico y actualización para los equipos y software.

## GARANTÍA HARDWARE

Garantía de 3 años por parte del fabricante del equipo, deberá incluir repuestos y mano de obra en sitio para todos los elementos descritos.

Características que deberá cubrir:

* El fabricante y el proveedor se comprometen a dar cumplimiento a la garantía.
* El servicio se prestará en las instalaciones de LA ENTIDAD requirente.
* Garantía en sitio para todos los componentes de la solución ofertada, con cobertura 24X7X365, con tiempo de respuesta de 4 horas mismo día y con sustitución de los mismos por parte del fabricante del equipo.
* El tiempo de reparación será día siguiente laboral. Sí excede este lapso, el proveedor deberá entregar un equipo de respaldo equivalente mientras se soluciona el problema.
* Si la reparación excede de 30 días naturales, el proveedor entregará a cambio un equipo nuevo con las características iguales al adquirido u otro equipo de mayores características.
* Carta del fabricante del hardware donde garantice la existencia de refacciones por lo menos durante los siguientes cinco años a partir de la fecha de entrega de los bienes

## GARANTÍA DE SOFTWARE.

* Garantía de software durante la vigencia de la garantía, en sitio para todo el software de la solución ofertada.
* Soporte telefónico 24X7X365, con tiempo de respuesta máximo de 15 minutos.
* Servicios de actualización de versiones y medios magnéticos (instalación y documentación) durante la vigencia de la garantía.

# GARANTÍA SOPORTE Y ACTUALIZACIÓN PARA ARRENDAMIENTO DE EQUIPOS

Para todos los componentes de la solución ofertada se deberán otorgar las siguientes garantías, soporte técnico y actualización para los equipos y software.

## GARANTÍA HARDWARE

* Garantía durante la vigencia del contrato, en sitio para todos los componentes de la solución ofertada, con cobertura 24X7X365, con tiempo de respuesta de 4 horas mismo día y con sustitución de los mismos por parte del fabricante del equipo.

El tiempo de reparación será día siguiente laboral. Sí excede este lapso, el proveedor deberá entregar un equipo de respaldo equivalente mientras se soluciona el problema.

* Carta del fabricante del hardware donde garantice la existencia de refacciones por lo menos durante la vigencia del contrato.

## GARANTÍA DE SOFTWARE.

* Garantía de software durante la vigencia del contrato, en sitio para todo el software de la solución ofertada.
* Soporte telefónico 24X7X365, con tiempo de respuesta máximo de 15 minutos.
* Servicios de actualización de versiones y medios magnéticos (instalación y documentación) durante la vigencia del contrato.

# SOPORTE TÉCNICO PARA HARDWARE Y SOFTWARE.

* El fabricante o los fabricantes que se contemplen en la solución deberán contar con una oficina de representación debidamente conformada en México para proveer el soporte técnico de campo solicitado.
* Servicio de asistencia telefónica, con tiempo máximo de respuesta de 15 minutos.
* Servicio de asistencia en Internet.
* Servicio de asistencia técnica vía remota o Internet en caso de ser necesario.
* Plan de escalamiento de fallas.
* Soporte del fabricante en sitio en caso de que el problema no se resuelva en 8 horas.

# MEDIOS PARA REPORTAR FALLAS Y HACER EFECTIVAS LAS GARANTÍAS:

* El procedimiento de recepción de reportes y atención de fallas de los equipos.
* Se debe de indicar una línea telefónica del fabricante o centro de atención telefónica certificado o aprobado por el fabricante sin costo de llamada para el usuario, como uno de los canales para hacer efectiva la garantía.
* Se debe de especificar un correo electrónico de atención, como uno de los canales para hacer efectiva la garantía.

# CONSIDERACIONES PARA EL PROCEDIMIENTO DE CONTRATACIÓN

## ADQUISICIÓN

* Presentar carta original por parte del fabricante manifestando bajo protesta de decir verdad, dirigida a LA ENTIDAD, que el equipo propuesto está basado en estándares internacionales y no maneja protocolos propietarios para su correcta operación
* Presentar carta original del fabricante de manifestación bajo protesta de decir verdad, dirigida a LA ENTIDAD, en donde el fabricante se declara obligado solidario con el proveedor participante en él suministro, instalación, configuración, puesta a punto y funcionalidades de los equipos propuestos.
* Presentar carta original del fabricante de manifestación bajo protesta de decir verdad, dirigida a LA ENTIDAD, donde garantice la existencia de refacciones por lo menos durante los siguientes cinco años a partir de la fecha de entrega de los bienes.
* Presentar carta original del fabricante de manifestación bajo protesta de decir verdad, dirigida a LA ENTIDAD que acredite al proveedor participante como distribuidor autorizado de los bienes.
* Carta del fabricante en la que se relacionen sus centros de servicio autorizados, los cuales podrán ser a través de Distribuidores Autorizados.
* Carta original del fabricante en la que se manifieste bajo protesta de decir verdad que cuentan con la infraestructura técnica, de servicio y refacciones para el mantenimiento de los equipos objeto del proceso de adjudicación, por cuando menos 5 años a partir de la fecha de entrega de los bienes.
* Los equipos suministrados, deberán contar con la ficha técnica, los manuales, instructivos, catálogos, y/o folletos en idioma español que sean necesarios para el conocimiento y óptimo uso, aprovechamiento, operación y funcionamiento de los mismos.
* Para el proceso de adjudicación, se podrán presentar folletos y/o información bajada de Internet donde aparezcan las especificaciones ofertadas proporcionando la URL para verificación. En caso de que alguna especificación no aparezca en la documentación impresa y electrónica se deberá anexar carta del fabricante, firmada bajo protesta de decir verdad, donde incluya la o las especificaciones técnicas faltantes

## ARRENDAMIENTO

* Carta del PROVEEDOR en la que se manifieste bajo protesta de decir verdad que cuenta con la infraestructura técnica y de servicio; así como la existencia de refacciones para el mantenimiento de los bienes objeto del servicio de arrendamiento, por cuando menos durante la vigencia del contrato.
* Se deberá de indicar una línea telefónica o centro de atención telefónica del PROVEEDOR sin costo de llamada para el usuario, para el levantamiento de fallas de los equipos.

# CERTIFICACIONES

* Presentar carta vigente del fabricante que acredite al participante como distribuidor autorizado y certificado para la instalación, configuración y puesta a punto de los bienes que oferta.
* Presentar carta vigente del fabricante de los equipos propuestos de manifestación bajo protesta de decir verdad, dirigida a **LA ENTIDAD**, donde declara que el participante cuenta con personal certificado por el fabricante, para la instalación, configuración y puesta a punto del equipo que oferta.
* El proveedor participante deberá presentar original y copia del documento (Certificado) vigente otorgado por el fabricante de los equipos ofertados que acredite que el participante cuenta con al menos 2 ingenieros certificados en la solución propuesta.
* El participante deberá acreditar su experiencia en el suministro, instalación, configuración y puesta a punto de la solución propuesta servicios iguales o similares a los ofertados, referenciando 3 casos de instalaciones soportadas similares a la de la propuesta y avaladas por el fabricante, para lo cual deberán citar nombre, domicilio y teléfonos de los clientes que presente de referencia, los cuales podrán ser verificados por **LA ENTIDAD**.

# CAPACITACIÓN.

* Incluir transferencia de conocimiento de la solución propuesta impartido por el fabricante en un centro de capacitación autorizado por el mismo, para al menos dos personas, con una duración mínima de 40 horas. La transferencia de conocimiento deberá de incluir la operación, administración y configuración de los bienes propuestos. En esta se deberá incluir el temario del curso.
* Si el curso se imparte en un centro de capacitación, se deberá incluir carta vigente que lo avale como centro autorizado de capacitación por parte del fabricante del curso propuesto.
* La ubicación donde se realizará la capacitación será de común acuerdo con **LA ENTIDAD.**

# INSTALACIÓN

La instalación, configuración y puesta a punto de los bienes ofertados deberá ser realizada por parte del proveedor y avalada por el fabricante y de común acuerdo con **LA ENTIDAD**.

Debido a que estas especificaciones técnicas son generales para todas LAS ENTIDADES y DEPENDENCIAS de la Administración Pública Federal, es importante señalar los tiempos de implementación se establecerán en el Anexo Técnico Específico de LA ENTIDAD

Es importante mencionar que en el anexo técnico final se determinará lo siguiente:

* La ubicación física en donde se requiera desplegar los equipos con los que se implementará la solución.
* Se proporcionará el número de políticas de seguridad, objetos, perfiles de seguridad y reglas de NAT con las que se cuente, tanto en los firewalls como en los dispositivos NAC, de manera que se realice un estimado más certero del esfuerzo necesario para llevar acabo la migración.
* Se indicará el número de usuarios existentes detrás del firewall, así como la cantidad de segmentos a proteger.

# ENTREGABLES

## MEMORIA TÉCNICA

* EL PROVEEDOR de servicio deberá entregar la memoria técnica de la instalación de los componentes que forman parte de este servicio.
* EL PROVEEDOR incluirá en la memoria técnica el registro de las pruebas realizadas de alta disponibilidad.
* EL PROVEEDOR deberá incluir los diagramas de conectividad incluyendo entre otros, el número de puertos requeridos para la operación de las soluciones propuestas, el tipo de comunicación requerida (unidireccional o bidireccional), etc. Los diagramas se incluirán dentro de la memoria técnica en formato electrónico (Microsoft Office Visio).
* En caso de cambio de equipamiento o configuraciones en los mismos, la memoria técnica deberá ser actualizada por EL PROVEEDOR.
* EL PROVEEDOR de servicios deberá entregar la memoria técnica de los equipos que formen parte de la infraestructura tecnológica de servicios de aprovisionamiento, dicha memoria deberá contar con las siguientes características:
* Visión y Alcance
* Planeación y Diseño
* Situación Actual
* Especificación Funcional
* Requisitos Mínimos para la instalación
* Características de Software
* Características de hardware
* Diseño Conceptual y Físico
* Parámetros de Configuración para su correcta instrumentación
* Pruebas de Funcionamiento

# SERVICIOS DE INSTALACIÓN, CONFIGURACIÓN Y MIGRACIÓN DE LA INFRAESTRUCTURA DE SEGURIDAD FIREWALL Y NAC

EL PROVEEDOR de la infraestructura de Seguridad Firewall y NAC deberá realizar la instalación, configuración de los equipos propuestos en las instalaciones que LA ENTIDAD le indique.

EL PROVEEDOR deberá realizar la migración de la infraestructura actual a la infraestructura propuesta y actualizar la configuración para conectar e integrar la aplicación a la nueva infraestructura y ambientes de operación, en las instalaciones que LA ENTIDAD le indique.

Para realizar la migración hacia la infraestructura propuesta por EL PROVEEDOR, éste deberá entregar un plan de migración para cada una LAS ENTIDADES, quienes aprobarán dicho plan.

El plan de migración hacia la infraestructura propuesta deberá incluir dentro del entregable como mínimo los siguientes capítulos a desarrollar por parte de EL PROVEEDOR:

* + Estrategia de migración de la aplicación.
  + Estrategia de integración con otros servicios de LA ENTIDAD para las tareas de migración.
  + Análisis de Riesgos.
  + Plan de Mitigación de riesgos.
  + Actividades detalladas de migración.
  + Plan de trabajo de migración.
  + Ajustes. Se refiere a la actualización de configuraciones, flujos y otros elementos necesarios que determine EL PROVEEDOR para que infraestructura de Seguridad y NAC opere correctamente.
  + Liberación de la aplicación. Es responsabilidad de EL PROVEEDOR en coordinación con LA ENTIDAD la liberación de la infraestructura de Seguridad y NAC en modo productivo y de entregarla a LA ENTIDAD para que se encargue de la operación y continuidad operativa, previa entrega de la documentación.
  + EL PROVEEDOR ejecutará todas las actividades para lograr que las migraciones sean organizadas, apegadas a la planeación acordada y aprobada por LA ENTIDAD, garantizando la participación de los recursos humanos proporcionados, entre los que se encuentran, los arquitectos de migración, técnicos y administrador de proyectos, que deberán contar con experiencia y conocimiento técnico en la ejecución de proyectos de migración, así como las herramientas necesarias que faciliten la tarea; asegurando que dicha planeación se lleve a cabo bajo principios de eficiencia y eficacia que garanticen el cumplimiento de los objetivos planteados para el proyecto.
  + Dentro del plan de migración se deberá incluir la definición, desarrollo y mantenimiento de un plan de pruebas para confirmar que dicha migración fue exitosa y formará parte de los entregables para la validación de los servicios.
  + EL PROVEEDOR debe incluir en su propuesta una metodología de migración basada en mejores prácticas internacionales en la materia, soportada por los recursos humanos que apoyen, tanto en la definición estratégica de la migración, como en la ejecución y el seguimiento puntual de las actividades definidas en la estrategia.

# TRANSICIÓN DE LOS SERVICIOS POR TÉRMINO DE CONTRATO DE ARRENDAMIENTO

EL PROVEEDOR adjudicado deberá considerar en su propuesta, el apoyo para la migración de la infraestructura de Seguridad y NAC que se encuentren en LA ENTIDAD al concluir el contrato. estas consideraciones deberán ser:

* Al término del contrato, EL PROVEEDOR, deberá facilitar la transferencia de toda la información y respaldos de la infraestructura de Seguridad y NAC hacia la infraestructura que LA ENTIDAD indique, considerando para ello, personal técnico especializado asegurando la confiabilidad y confidencialidad de la información.
* Durante este proceso de transición EL PROVEEDOR, deberá considerar un mes de prórroga sin costo para LA ENTIDAD o DEPENDENCIA a partir de la conclusión del contrato.
* Cuando LA ENTIDAD se lo requiera deberá entregar toda la información y elementos necesarios ya sea para migrar la infraestructura de Seguridad y NAC a otra plataforma o únicamente para realizar una transferencia de proveedor de servicio sobre la misma plataforma, considerando al menos lo siguiente: accesos a la infraestructura de Seguridad y NAC, usuarios, contraseñas, llaves, rutas, respaldos, accesos a los repositorios y memorias técnicas, configuraciones entre otros con la finalidad de facilitar el proceso de migración a quien en ese momento sea el nuevo proveedor ganador.
* Deberá considerar que, durante el proceso de migración o transición, la operación de la infraestructura de Seguridad y NAC de LA ENTIDAD no deberá presentar fallas en su operación y que, en caso de requerir ventana de tiempo para concluir el proceso de migración, estas ventanas deberán ser programadas y solicitadas a LA ENTIDAD o DEPENDENCIA y no deberán ser mayor de 12 horas.
* EL PROVEEDOR que resulte ganador del presente proceso deberá formar parte activa de las mesas de trabajo para análisis del plan de migración que en su momento presente el nuevo proveedor y determinar la forma óptima de respaldar cada una de las Aplicaciones, su configuración y sus datos, con la finalidad de que la migración sea transparente.

# MESA DE SERVICIO PARA SEGURIDAD FIREWALL Y NAC

Debido a que estas especificaciones técnicas son generales para todas LAS ENTIDADES y DEPENDENCIAS de la Administración Pública Federal, es importante señalar las características de los servicios se establecerán en el Anexo Técnico Específico de LA ENTIDAD

El servicio de mesa de servicio para SEGURIDAD FIREWALL Y NAC se compone de los siguientes elementos:

* •El PROVEEDOR deberá entregar una matriz de escalamiento que permita al LA ENTIDAD contactar al personal designado por el PROVEEDOR para asegurar el cumplimiento y entrega conforme al presente documento. De igual manera, el PROVEEDOR deberá proporcionar un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.
* •El PROVEEDOR deberá llegar a un acuerdo con LA ENTIDAD con respecto a la herramienta de mesa de servicio que se utilizará y la logística relacionada con la puesta a punto de los equipos de cómputo y los espacios que utilizarán el personal designado por el PROVEEDOR con la finalidad de que las actividades se realicen de forma que se pueda garantizar la continuidad de los servicios que proporciona LA ENTIDAD. De igual manera, el PROVEEDOR y LA ENTIDAD deben acordar los estatus permitidos para las solicitudes e incidencias y las categorías de clasificación. Los estatus y categorías son indispensables para generar los reportes mensuales.
* •El PROVEEDOR deberá llegar a un acuerdo con LA ENTIDAD con respecto a las actividades de revisión de inventario físico y su calendarización y logística, con la finalidad de que las actividades se realicen de forma que se pueda garantizar la continuidad de los servicios que proporciona LA ENTIDAD.
* •EL PROVEEDOR deberá emplear la herramienta de mesa de servicio acordada con el LA ENTIDAD para registrar y dar atención y seguimiento a las solicitudes e incidencias (en relación con el servicio proporcionado) registradas por el personal designado por el LA ENTIDAD
* •El PROVEEDOR deberá entregar mensualmente un reporte indicando el estatus y clasificación de las solicitudes e incidencias atendidas en relación con el servicio proporcionado. De igual manera, el PROVEEDOR deberá entregar mensualmente un reporte de la disponibilidad de los canales de comunicación.
* •El PROVEEDOR deberá entregar un plan de mantenimiento preventivo que debe ejecutarse durante la vigencia del contrato. LA ENTIDAD debe validar el plan y llegar a un acuerdo con la finalidad de que las actividades se realicen de forma que se pueda garantizar la continuidad de los servicios que proporciona LA ENTIDAD.
* •El PROVEEDOR deberá entregar un plan de recuperación de bienes al término del contrato. LA ENTIDAD debe validar el plan y llegar a un acuerdo con la finalidad de que las actividades se realicen de forma que se pueda garantizar la continuidad de los servicios que proporciona LA ENTIDAD