SENADO
REPÚBLICA DOMINICANA

"Año de la Consolidación de la Seguridad Alimentaria"

Procedimientos de Licitaciones, regidos por la Ley No. 340-06 y su reglamento 543-12
Y resolución PNP-01-2020

ESPECIFICACIONES TÉCNICAS Y TÉRMINOS DE REFERENCIA

ACTUALIZACIÓN PARA INTERCAMBIO DE PLATAFORMA DE SEGURIDAD PERIMETRAL DEL SENADO DE LA REPÚBLICA

PROCEDIMIENTO DE SELECCIÓN

COMPARACIÓN DE PRECIOS

Referencia: SEN-CCC-CP-2021- 001.

Santo Domingo, Distrito Nacional
República Dominicana
12 DE FEBRERO DE 2021

SENADO DE LA REPÚBLICA • COMITÉ DE COMPRAS Y CONTRATACIONES • Santo Domingo, Rep. Dom.

1.1 Objetivos y Alcance

El objetivo del presente documento es establecer el conjunto de cláusulas jurídicas, económicas, técnicas y administrativas, de naturaleza reglamentaria, por el que se fijan los requisitos, exigencias, facultades, derechos y obligaciones de las personas naturales o jurídicas, nacionales o extranjeras, que deseen participar en el procedimiento de comparación de precios para la **actualización para intercambio de plataforma de seguridad perimetral del Senado de la República** , llevada a cabo por **EL SENADO DE LA REPÚBLICA. Referencia: SEN-CCC-CP-2021- 001.**

Este documento constituye la base para la preparación de las Ofertas. Si el Oferente/Proponente omite suministrar alguna parte de la información requerida en los presentes términos de Referencia y Condiciones Específicas o presenta una información que no se ajuste sustancialmente en todos sus aspectos al mismo, el riesgo estará a su cargo y el resultado podrá ser el rechazo de su Propuesta.

1.2 Precio de la Oferta

Los precios cotizados por el Oferente en el Formulario de Presentación de Oferta Económica deberán ajustarse a los requerimientos que se indican a continuación.

Todos los lotes y/o artículos deberán enumerarse y cotizarse por separado en el Formulario de Presentación de Oferta Económica. Si un formulario de Oferta Económica detalla artículos pero no los cotiza, se asumirá que está incluido en la Oferta. Asimismo, cuando algún lote o artículo no aparezca en el formulario de Oferta Económica se asumirá de igual manera, que está incluido en la Oferta.

El desglose de los componentes de los precios se requiere con el único propósito de facilitar a la Entidad Contratante la comparación de las Ofertas.

El precio cotizado en el formulario de Presentación de la Oferta Económica deberá ser el precio total de la oferta, excluyendo cualquier descuento que se ofrezca.

Los precios cotizados por el Oferente serán fijos durante la ejecución del Contrato y no estarán sujetos a ninguna variación por ningún motivo, salvo lo establecido en los términos de referencia presente.

1.3 Moneda de la Oferta

El precio en la Oferta deberá estar expresado en moneda nacional, (Pesos Dominicanos, RD$), a excepción de los Contratos de suministros desde el exterior, en los que podrá expresarse en la moneda del país de origen de los mismos.

De ser así, el importe de la oferta se calculará sobre la base del tipo de cambio vendedor del BANCO CENTRAL DE LA REPÚBLICA DOMINICANA vigente al cierre del día anterior a la fecha de recepción de ofertas.

1.23.1 Garantía de la Seriedad de la Oferta

Correspondiente al uno por ciento (1%) del monto total de la Oferta.

PÁRRAFO I. La Garantía de Seriedad de la Oferta será de cumplimiento obligatorio y vendrá incluida dentro de la Oferta Económica. La omisión en la presentación de la Oferta de la Garantía de Seriedad de Oferta o cuando la misma fuera insuficiente, conllevará la desestimación de la Oferta sin más trámite.

1.23.2 Garantía de Fiel Cumplimiento de Contrato

Los Adjudicatarios cuyos Contratos excedan el equivalente en Pesos Dominicanos de **Diez Mil Dólares de los Estados Unidos de Norteamérica con 00/100 (US$10.000,00)**, están obligados a constituir una Garantía Bancaria o Pólizas de Fianzas de compañías aseguradoras de reconocida solvencia en la República Dominicana, con las condiciones de ser incondicionales, irrevocables y renovables, en el plazo de **cinco (5) días hábiles**, contados a partir de la Notificación de la Adjudicación, por el importe del **CUATRO POR CIENTO (4%)** del monto total del Contrato a intervenir, a disposición de la Entidad Contratante, cualquiera que haya sido el procedimiento y la forma de Adjudicación del Contrato. En el caso de que el adjudicatario sea una Micro, Pequeña y Mediana empresa (MIPYME) el importe de la garantía será de un **UNO POR CIENTO (1%).** La Garantía de Fiel Cumplimiento de Contrato debe ser emitida por una entidad bancaria de reconocida solvencia en la República Dominicana.

La no comparecencia del Oferente Adjudicatario a constituir la Garantía de Fiel Cumplimiento de Contrato, se entenderá que renuncia a la Adjudicación y se procederá a la ejecución de la Garantía de Seriedad de la Oferta.

Cuando hubiese negativa a constituir la Garantía de Fiel Cumplimiento de Contrato, la Entidad Contratante, como Órgano de Ejecución del Contrato, notificará la Adjudicación de los renglones correspondientes al Oferente que hubiera obtenido la siguiente posición en el proceso de Adjudicación, conforme al Reporte de Lugares Ocupados. El nuevo Oferente Adjudicatario depositará la Garantía y suscribirá el Contrato de acuerdo al plazo que le será otorgado por la Entidad Contratante, mediante comunicación formal.

1.4 Devolución de las Garantías

a) **Garantía de la Seriedad de la Oferta:** Tanto al Adjudicatario como a los demás oferentes participantes una vez integrada la garantía de fiel cumplimiento de contrato.

b) **Garantía de Fiel Cumplimiento de Contrato:** Una vez cumplido el contrato a satisfacción de la Entidad Contratante, cuando no quede pendiente la aplicación de multa o penalidad alguna.

1.5 Consultas

Los interesados podrán solicitar a la Entidad Contratante aclaraciones acerca del Pliego de Condiciones Específicas, hasta la fecha que coincida con el **CINCUENTA POR CIENTO (50%)** del plazo para la presentación de las Ofertas. Las consultas las formularán los Oferentes por escrito, sus representantes legales, o quien éstos identifiquen para el efecto. La Unidad Operativa de Compras y Contrataciones, dentro del plazo previsto, se encargará de obtener las respuestas conforme a la naturaleza de la misma.

Las Consultas se remitirán al Comité de Compras y Contrataciones, dirigidas a:

COMITÉ DE COMPRAS Y CONTRATACIONES
SENADO DE LA REPUBLICA DOMINICANA
Referencia: SEN-CCC-CP- 2021-001

Dirección: Av. Enrique Jiménez Moya, esquina Juan de Dios Ventura Simó, Centro de los Héroes de Constanza, Maimón y Estero Hondo, Santo Domingo de Guzmán, Distrito Nacional, Republica Dominicana
Teléfonos: 809-532-5561
Correo electrónico: compra (@ senado.gob.do

1.6 Circulares

El Comité de Compras y Contrataciones podrá emitir Circulares de oficio o para dar respuesta a las Consultas planteadas por los Oferentes/Proponentes con relación al contenido del presente Pliego de Condiciones, formularios, otras Circulares o anexos. Las Circulares se harán de conocimiento de todos los Oferentes/Proponentes. Dichas circulares deberán ser emitidas solo con las preguntas y las respuestas, sin identificar quien consultó, en un plazo no más allá de la fecha que signifique el **SETENTA Y CINCO POR CIENTO (75%)** del plazo previsto para la presentación de las Ofertas y deberán ser notificadas a todos los Oferentes que hayan adquirido el Pliego de Condiciones Específicas y publicadas en el portal institucional.

1.7 Enmiendas

De considerarlo necesario, por iniciativa propia o como consecuencia de una Consulta, el Comité de Compras y Contrataciones podrá modificar, mediante Enmiendas, el Pliego de Condiciones Específicas, formularios, otras Enmiendas o anexos. Las Enmiendas se harán de conocimiento de todos los Oferentes/Proponentes y se publicarán en el portal institucional.

Tanto las Enmiendas como las Circulares emitidas por el Comité de Compras y Contrataciones pasarán a constituir parte integral del presente Pliego de Condiciones y en consecuencia, serán de cumplimiento obligatorio para todos los Oferentes/Proponentes.

2.1 Objeto de la Licitación

Constituye el objeto de la presente convocatoria la **actualización para intercambio de plataforma de seguridad perimetral del Senado de la República,** de acuerdo con las condiciones fijadas en el presente término de referencia y especificaciones técnicas.

2.2 Procedimiento de Selección

COMPARACIÓN DE PRECIOS DE ÚNICA ETAPA

2.3 Fuente de Recursos

SENADO DE LA REPÚBLICA de conformidad con el Artículo 32 del Reglamento No. 543-12 sobre Compras y Contrataciones Públicas de Bienes, Servicios y Obras, ha tomado las medidas previsoras necesarias a los fines de garantizar la apropiación de fondos correspondiente, dentro del Presupuesto del año 2021 que sustentará el pago de todos los bienes adjudicados y adquiridos mediante la presente Licitación. Las partidas de fondos para liquidar las entregas programadas serán debidamente especializadas para tales fines, a efecto de que las condiciones contractuales no sufran ningún tipo de variación durante el tiempo de ejecución del mismo.

2.4 Condiciones de Pago

La Entidad Contratante no podrá comprometerse a entregar, por concepto de avance, un porcentaje mayor al veinte por ciento (20%) del valor del Contrato.

En caso de que el adjudicatario del contrato sea una Micro, Pequeña y Mediana empresa (MIPYME) la entidad contratante deberá entregar un avance inicial correspondiente al veinte por ciento (20%) del valor del contrato, para fortalecer su capacidad económica, contra la presentación de la garantía del buen uso del anticipo.

20% de inicial y 80% contra entrega final en el Senado de la República.

2.5 Cronograma de la Licitación[1]

ACTIVIDADES	PERÍODO DE EJECUCIÓN
1. Publicación llamado a participar en la licitación	Viernes 12 y lunes 15 de febrero del año 2021.
2. Período para realizar consultas por parte de los interesados	Viernes 12, lunes 15 y martes 16 de febrero del 2021 hasta las 12:00m
3. Plazo para emitir respuesta por parte del Comité de Compras y Contrataciones	Hasta el miércoles 17 de febrero del año 2021 hasta las 4:00p.m.
4. **Recepción de Propuestas: "Sobre A" y "Sobre B" y apertura de "Sobre A" Propuestas Técnicas**.	**Recepción de Propuestas: "Sobre A" y "Sobre B"** el viernes 19 de febrero del 2021 **desde 9:00a.m. hasta las 10:50am**. Salón Charles Summer 6to. Piso. **Apertura de "Sobre A" Propuestas Técnicas** el viernes 19 de febrero del 2021 en horario de **11:00am** Charles Summer 6to. Piso.
5. Verificación, Validación y Evaluación contenido de las Propuestas Técnicas "Sobre A"	Lunes 22 de febrero del 2021.
6. Notificación de errores u omisiones de naturaleza subsanables.	Martes 23 de febrero del año del año 2021.
7. Periodo de subsanación de ofertas	Miércoles 24 y jueves 25 de febrero del año 2021.
8. Período de Ponderación de Subsanaciones	Viernes 26 de febrero del 2021.
9. Notificación Resultados del Proceso de Subsanación y Oferentes Habilitados para la presentación de Propuestas Económicas "Sobre B"	Lunes 01 de marzo del 2021.
10. **Apertura y lectura de Propuestas Económicas "Sobre B"**	Martes 02 de marzo del 2021, en caso que se produzcan subsanaciones. De lo contrario se efectuarán en el mismo día de la apertura del Sobre A
11. Evaluación Ofertas Económicas "Sobre B"	Miércoles 3 de marzo de 2021
12. Adjudicación	Después de Evaluadas las ofertas

SENADO DE LA REPÚBLICA
COMITÉ DE COMPRAS Y CONTRATACIONES
Santo Domingo, Rep. Dom.

13. Notificación y Publicación de Adjudicación	Hasta el viernes 12 de marzo del 2021
14. Plazo para la constitución de la Garantía Bancaria de Fiel Cumplimiento de Contrato	Cinco días hábiles después de remitirse la notificación de adjudicación
15. Suscripción del Contrato	Lunes 15 de marzo de 2021
16. Publicación de los Contratos en el portal institución y en el portal administrado por el Órgano Rector.	Después de suscritos por las partes

2.6 Disponibilidad y Adquisición de los términos de referencias y especificaciones técnicas

Los términos de referencias y condiciones específicas estarán disponibles para quien lo solicite, en la sede central de la **SENADO DE LA REPÚBLICA DOMINICANA** ubicada en la Av. Enrique Jiménez Moya, esquina Juan de Dios Ventura Simó, Centro de los Héroes de Constanza, Maimón y Estero Hondo, Santo Domingo de Guzmán, Distrito Nacional, Republica Dominicana en el horario de 8:00am. A 4:00pm., en la fecha anteriormente indicada en el Cronograma y en la página Web de la institución https://senadord.gob.do/ para todos los interesados.

El Oferente que adquiera los términos de referencias y condiciones específicas a través de la página Web de la institución, **ww.senado.gob.do**, deberá enviar un correo electrónico a **compras@ senado.gob.do** o en su defecto, notificar al Departamento de Compras del Senado de la República Dominicana sobre la adquisición del mismo, a los fines de que la Entidad Contratante tome conocimiento de su interés en participar.

2.7 Conocimiento y Aceptación de las especificaciones técnicas y términos de referencia

El sólo hecho de un Oferente/Proponente participar en el proceso de comparación de precios, implica pleno conocimiento, aceptación y sometimiento por él, por sus miembros, ejecutivos y su Representante Legal, a los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente Pliego de Condiciones, el cual tienen carácter jurídicamente obligatorio y vinculante.

2.8 Fichas Técnicas

1. Actualización para intercambio de Plataforma de Seguridad Perimetral - Firewall	Cant: 1
1.1. Características Generales	
1.1.1. La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.	
1.1.2. Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	
1.1.3. Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	
1.1.4. La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	
1.1.5. Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;	
1.1.6. La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	
1.1.7. Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;	
1.1.8. Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	
1.1.9. Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	
1.1.10. Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	
1.1.11. Los dispositivos de protección de red deben soportar DHCP Relay;	
1.1.12. Los dispositivos de protección de red deben soportar DHCP Server;	
1.1.13. Los dispositivos de protección de red deben soportar sFlow;	
1.1.14. Los dispositivos de protección de red deben soportar Jumbo Frames;	
1.1.15. Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	
1.1.16. Debe ser compatible con NAT dinámica (varios-a-1);	
1.1.17. Debe ser compatible con NAT dinámica (muchos-a-muchos);	
1.1.18. Debe soportar NAT estática (1-a-1);	
1.1.19. Debe admitir NAT estática (muchos-a-muchos);	
1.1.20. Debe ser compatible con NAT estático bidireccional 1-a-1;	
1.1.21. Debe ser compatible con la traducción de puertos (PAT);	
1.1.22. Debe ser compatible con NAT Origen;	
1.1.23. Debe ser compatible con NAT de destino;	
1.1.24. Debe soportar NAT de origen y NAT de destino de forma simultánea;	
1.1.25. Debe soportar NAT de origen y NAT de destino en la misma política	
1.1.26. Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	
1.1.27. Debe ser compatible con NAT64 y NAT46;	
1.1.28. Debe implementar el protocolo ECMP;	
1.1.29. Debe soportar SD-WAN de forma nativa	
1.1.30. Debe soportar el balanceo de enlace hash por IP de origen;	
1.1.31. Debe soportar el balanceo de enlace por hash de IP de origen y destino;	
1.1.32. Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;	
1.1.33. Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	

1.1.34. Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
1.1.35. Enviar logs a sistemas de gestión externos simultáneamente;
1.1.36. Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;
1.1.37. Debe soporta protección contra la suplantación de identidad (anti-spoofing);
1.1.38. Implementar la optimización del tráfico entre dos dispositivos;
1.1.39. Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
1.1.40. Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
1.1.41. Soportar OSPF graceful restart;
1.1.42. Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;
1.1.43. Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
1.1.44. Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
1.1.45. Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
1.1.46. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
1.1.47. Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
1.1.48. Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster;
1.1.49. La configuración de alta disponibilidad debe sincronizar: Sesiones;
1.1.50. La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
1.1.51. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
1.1.52. La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
1.1.53. En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
1.1.54. Debe soportar la creación de sistemas virtuales en el mismo equipo;
1.1.55. Para una alta disponibilidad, el uso de clúster virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
1.1.56. Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;
1.1.57. La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;
1.1.58. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
1.1.59. Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;
1.1.60. El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;
1.1.61. Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;
1.1.62. La consola de administración debe soportar como mínimo, inglés, español y Portugués.

1.1.63. La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad
1.1.64. La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.
1.2. Control por Política de Firewall
1.2.1. Debe soportar controles de zona de seguridad;
1.2.2. Debe contar con políticas de control por puerto y protocolo;
1.2.3. Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;
1.2.4. Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;
1.2.5. Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
1.2.6. Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;
1.2.7. Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
1.2.8. Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);
1.2.9. Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes
1.2.10. Debe soportar el protocolo estándar de la industria VXLAN;
1.2.11. La solución debe permitir la implementación sin asistencia de SD-WAN
1.2.12. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;
1.2.13. La solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web Application firewall.
1.3. Control de Aplicación
1.3.1. Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;
1.3.2. Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;
1.3.3. Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
1.3.4. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;
1.3.5. Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de las aplicaciones conocidas por el fabricante;
1.3.6. Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
1.3.7. Actualización de la base de firmas de la aplicación de forma automática;
1.3.8. Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;
1.3.9. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

1.3.10. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
1.3.11. El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
1.3.12. Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
1.3.13. Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;
1.3.14. Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;
1.3.15. Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;
1.3.16. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);
1.3.17. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;
1.3.18. Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;
1.3.19. Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente
1.4. Prevención de Amenazas
1.4.1. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;
1.4.2. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);
1.4.3. Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;
1.4.4. Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;
1.4.5. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;
1.4.6. Deber permitir el bloqueo de vulnerabilidades y exploits conocidos
1.4.7. Debe incluir la protección contra ataques de denegación de servicio;
1.4.8. Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;
1.4.9. Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;
1.4.10. Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;
1.4.11. Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;
1.4.12. Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);
1.4.13. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;
1.4.14. Detectar y bloquear los escaneos de puertos de origen;
1.4.15. Bloquear ataques realizados por gusanos (worms) conocidos;
1.4.16. Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
1.4.17. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
1.4.18. Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
1.4.19. Identificar y bloquear la comunicación con redes de bots;

1.4.20. Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
1.4.21. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
1.4.22. Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
1.4.23. Los eventos deben identificar el país que originó la amenaza;
1.4.24. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
1.4.25. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
1.4.26. Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
1.4.27. En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
1.4.28. Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);
1.5. Filtrado de URL
1.5.1. Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
1.5.2. Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
1.5.3. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
1.5.4. Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;
1.5.5. Tener por lo menos 75 categorías de URL;
1.5.6. Debe tener la funcionalidad de exclusión de URLs por categoría;
1.5.7. Permitir página de bloqueo personalizada;
1.5.8. Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
1.5.9. Además del Explicit Web Proxy, soportar proxy web transparente;
1.6. Identificación de Usuarios
1.6.1. Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
1.6.2. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;
1.6.3. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
1.6.4. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

1.6.5. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios;
1.6.6. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
1.6.7. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
1.6.8. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
1.6.9. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
1.6.10. Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;
1.7. QoS Traffic Shaping
1.7.1. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;
1.7.2. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;
1.7.3. Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;
1.7.4. Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;
1.7.5. Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;
1.7.6. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;
1.7.7. En QoS debe permitir la definición de tráfico con ancho de banda garantizado;
1.7.8. En QoS debe permitir la definición de tráfico con máximo ancho de banda;
1.7.9. En QoS debe permitir la definición de colas de prioridad;
1.7.10. Soportar marcación de paquetes DiffServ, incluso por aplicación;
1.7.11. Soportar la modificación de los valores de DSCP para Diffserv;
1.7.12. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);
1.7.13. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;
1.8. Filtro de Datos
1.8.1. Permite la creación de filtros para archivos y datos predefinidos;
1.8.2. Los archivos deben ser identificados por tamaño y tipo;
1.8.3. Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;
1.8.4. Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;
1.8.5. Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;
1.8.6. Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;
1.9. Geo Localización
1.9.1. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;
1.9.2. Debe permitir la visualización de los países de origen y destino en los registros de acceso;
1.9.3. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de

políticas usando las mismas;
1.10. VPN
1.10.1. Soporte VPN de sitio-a-sitio y cliente-a-sitio;
1.10.2. Soportar VPN IPSec;
1.10.3. Soportar VPN SSL;
1.10.4. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512
1.10.5. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;
1.10.6. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);
1.10.7. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);
1.10.8. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
1.10.9. Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;
1.10.10. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;
1.10.11. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;
1.10.12. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;
1.10.13. Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
1.10.14. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
1.10.15. Deberá mantener una conexión segura con el portal durante la sesión;
1.10.16. El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.
1.11. Wireless Controller
1.11.1. Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);
1.11.2. Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;
1.11.3. Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;
1.11.4. La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;
1.11.5. El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;
1.11.6. La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;
1.11.7. Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;
1.11.8. El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;
1.11.9. Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;
1.11.10. Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;

1.11.11. Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;
1.11.12. La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;
1.11.13. La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;
1.11.14. La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;
1.11.15. La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;
1.11.16. La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;
1.11.17. La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;
1.11.18. La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;
1.11.19. La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;
1.11.20. La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;
1.11.21. La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;
1.11.22. La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;
1.11.23. La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;
1.11.24. La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;
1.11.25. Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;
1.11.26. La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;
1.11.27. La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;

1.11.28. La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;
1.11.29. La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;
1.11.30. La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;
1.11.31. La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;
1.11.32. La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado , Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;
1.11.33. Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;
1.11.34. La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitar para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;
1.11.35. La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;
1.11.36. La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;
1.11.37. La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;
1.11.38. La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;
1.11.39. La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;
1.11.40. La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;
1.11.41. La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;
1.11.42. La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;
1.11.43. La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps o Bps) para las aplicaciones reconocidas a través de la técnica de DPI;
1.11.44. La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;
1.11.45. La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados:
1.11.45.1. Ataques de flood contra el protocolo EAPOL (EAPOL Flooding);
1.11.45.2. Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast

Deauthentication y Spoofed Deauthentication;
1.11.45.3. ASLEAP;
1.11.45.4. Null Probe Response / Null SSID Probe Response;
1.11.45.5. Long Duration;
1.11.45.6. Ataques contra Wireless Bridges;
1.11.45.7. Weak WEP;
1.11.45.8. Invalid MAC OUI.
1.11.46. La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication
1.11.47. La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;
1.11.48. La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos;
1.11.49. Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;
1.11.50. Debe implementar la autenticación administrativa a través del protocolo RADIUS;
1.11.51. En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);
1.11.52. En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;
1.11.53. La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;
1.11.54. Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;
1.11.55. La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;
1.11.56. La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;
1.11.57. La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;
1.11.58. La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;
1.11.59. La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;
1.11.60. La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;
1.11.61. La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;
1.11.62. La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;
1.11.63. La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;
1.11.64. La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6;
1.11.65. La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;

1.11.66. Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;
1.11.67. La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;
1.11.68. La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;
1.11.69. La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;
1.11.70. La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;
1.11.71. La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;
1.11.72. La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;
1.11.73. La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;
1.11.74. La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;
1.11.75. La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;
1.11.76. La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);
1.11.77. La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;
1.11.78. La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;
1.11.79. La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;
1.11.80. La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;
1.11.81. La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;
1.11.82. La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;
1.11.83. La solución debe tener herramientas de diagnóstico y depuración;
1.11.84. La solución debe soportar la comunicación con elementos externos a través de las API;
1.11.85. La solución deberá ser compatible y administrar los puntos de acceso de este proceso;
2. Lista de equipos
2.1. Características Equipo
2.1.1. Throughput de por lo menos 1.40 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6
2.1.2. Soporte a por lo menos 45,000 conexiones simultaneas
2.1.3. Soporte a por lo menos 200 nuevas conexiones por segundo
2.1.4. Throughput de al menos 950 Mbps de VPN IPSec
2.1.5. Estar licenciado para, o soportar sin necesidad de licencia, 2,500 túneles de VPN IPSec site-to-site simultáneos
2.1.6. Estar licenciado para, o soportar sin necesidad de licencia, 200 túneles de clientes VPN IPSec simultáneos
2.1.7. Throughput de al menos 1500.00 Gbps de VPN SSL
2.1.8. Soportar al menos 10 clientes de VPN SSL simultáneos

2.1.9. Soportar al menos 1.80 Gbps de throughput de IPS
2.1.10. Soportar al menos 6.50 Gbps de throughput de Inspección SSL
2.1.11. Soportar al menos 1.00 Gbps de throughput de Application Control
2.1.12. Soportar al menos 900 Mbps de throughput de NGFW
2.1.13. Soportar al menos 715 Mbps de throughput de Threat Protection
2.1.14. Permitir gestionar al menos 16 Access Points
2.1.15. Tener al menos 8 interfaces 1Gbps
2.1.16. Disco de, por lo menos, 16 GB para almacenamiento de información local
2.1.17. Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance

2.9 Suministro

La Convocatoria a procedimiento por comparación de precios se hace sobre la base de un suministro inmediato contado a partir de la notificación de la adjudicación, conforme se establece en el Cronograma.

2.10 Soporte y responsabilidades del oferente proponente

- La solución debe incluir 3 años de soporte 7x24
- Servicios profesionales, migración y actualización de plataforma de siguiente generación.
- Proveedor debe contar con al menos Tres (3) ingenieros que sean empleados a tiempo completo del contratante, no contratistas externos (debe ser avalado con una certificación de la Tesorería de la Seguridad Social) y que estén certificados por el fabricante.

2.11 Presentación de Propuestas Técnicas y Económicas "Sobre A" y "Sobre B"

Las Ofertas se presentarán en un Sobre cerrado y rotulado con las siguientes inscripciones:

COMITÉ DE COMPRAS Y CONTRATACIONES
SENADO DE LA REPÚBLICA DOMINICANA
Referencia: SEN-CCC-CP- 2021-001
Dirección: Av. Enrique Jiménez Moya, esquina Juan de Dios Ventura Simó, Centro de los Héroes de Constanza, Maimón y Estero Hondo, Santo Domingo de Guzmán, Distrito Nacional, Republica Dominicana
Teléfonos: 809-532-5561
Correo electrónico: compra@senado.gob.do

Este Sobre contendrá en su interior el **"Sobre A"** Propuesta Técnica y el **"Sobre B"** Propuesta Económica.

Ninguna oferta presentada en término podrá ser desestimada en el acto de apertura. Las que fueren observadas durante el acto de apertura se agregaran para su análisis por parte de los peritos designados.

2.12 Lugar, Fecha y Hora

La presentación de Propuestas **"Sobre A" y "Sobre B"** se efectuará en acto público, ante el Comité de Compras y Contrataciones y el Notario Público actuante, en el Salón Charles Sunmer, 6to. piso del Senado de la República Dominicana, Avenida Jiménez Moya, Esquina Juan de Dios Ventura Simó, Centro de los Héroes, La Feria, Santo Domingo, D.N, **desde las 9:00am. Hasta las 10:50am.** de los días indicado en el Cronograma y la **apertura del "Sobre A", oferta técnica a las 11:00a.m.** en el mismo salón, sólo podrá postergarse por causas de Fuerza Mayor o Caso Fortuito definidos en el presente Pliego de Condiciones Específicas.

Los **"Sobres B"** quedarán bajo la custodia del Consultor Jurídico de la institución, en su calidad de Asesor Legal del Comité de Compras y Contrataciones hasta la fecha de su apertura, conforme al Cronograma establecido.

La Entidad Contratante no recibirá sobres que no estuviesen debidamente cerrados e identificados según lo dispuesto anteriormente.

Los documentos contenidos en el **"Sobre A"** deberán ser presentados en original debidamente marcado como "**ORIGINA**L" en la primera página del ejemplar, junto con **TRES (3),** fotocopias simples de los mismos, debidamente marcada, en su primera página, como "**COPIA**". El original y las copias deberán firmarse en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

El "**Sobre A**" deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
SENADO DE LA REPUBLICA DOMINICANA

PRESENTACIÓN: OFERTA TÉCNICA
REFERENCIA : SEN-CCC-CP- 2021-001

2.14 Documentación a Presentar

A. **Documentación Legal:**
   1. Formulario de Presentación de Oferta **(SNCC.F.034)**

2. Formulario de Información sobre el Oferente **(SNCC.F.042)**
3. Registro de Proveedores del Estado (RPE) con documentos legales-administrativos actualizados, emitido por la Dirección General de Contrataciones Públicas.
4. Certificado de MiPymes (si aplica)
5. Copia del Certificado del nombre comercial vigente
6. Certificación de la Dirección General de Impuestos Internos (DGII), en el cual se manifieste que está al día con sus obligaciones fiscales.
7. Certificación de pago de la tesorería de la Seguridad Social (TSS), la cual manifieste que está al día con sus obligaciones de la Seguridad Social.
8. Copia de los estatutos de la empresa
9. Copia del Acta de Asamblea constitutiva (con su nómina de presencia), certificado por la Cámara de Comercio.
10. Copia del Acta de Asamblea General ordinaria correspondiente al año 2020-2021.
11. Copia de identificación del representante legal (cédula nueva o pasaporte)
12. En caso que los estatutos hayan sufrido alguna modificación o adecuación, depositar copia del acta de asamblea extraordinaria que conoce dicha modificación (Certificado Cámara de Comercio).
13. Declaración jurada del solicitante en la que manifieste que no se encuentra dentro de las prohibiciones establecidas en el artículo 14 de la ley 340-06 y donde manifieste si tiene o no juicio con el Estado Dominicano y sus entidades del Gobierno Central, de las instituciones simples de la misma, debidamente marcadas en su primera página como copia. El original y la copia deberán estar firmadas en todas las páginas, por el representante legal, debidamente foliado y sellado y deberán llevar el sello de la compañía.

B. Documentación Financiera:

1. Estados Financieros de los dos (2) últimos ejercicios contables consecutivos.
2. Carta de referencia bancaria.

C. Documentación Técnica:

1. Oferta Técnica (conforme a las especificaciones técnicas suministradas)

Certificación que garantice que el oferente está acreditado por el fabricante para dar soporte en República Dominicana a la plataforma ofertada.

2. Referencia de sus principales clientes, un mínimo de dos (2) en que se han implementados y soportados por el oferente en la República Dominicana con equipos similares y superiores.

3. Certificación de la disponibilidad de garantía de 3 años de soporte 7x24.

Para los consorcios:

En adición a los requisitos anteriormente expuestos, los consorcios deberán presentar:

1. Original del Acto Notarial por el cual se formaliza el consorcio, incluyendo su objeto, las obligaciones de las partes, su duración la capacidad de ejercicio de cada miembro del consorcio, así como sus generales.

2. Poder especial de designación del representante o gerente único del Consorcio autorizado por todas las empresas participantes en el consorcio.

LA PRESENTACIÓN EN OTRO FORMATO INVALIDA LA OFERTA

2.16 Presentación de la Documentación Contenida en el "Sobre B"

A) **Formulario de Presentación de Oferta Económica (SNCC.F.33),** presentado en **Un (1)** original debidamente marcado como "**ORIGINAL**" en la primera página de la Oferta, junto con **TRES (3)** fotocopias simples de la misma, debidamente marcadas, en su primera página, como "**COPIA**". El original y las copias deberán estar firmados en todas las páginas por el Representante Legal, debidamente foliadas y deberán llevar el sello social de la compañía.

B) **Garantía de la Seriedad de la Oferta**. Correspondiente a una póliza de fianza o garantía bancaria]. Correspondiente al **uno por ciento (1%)** del monto total de la Oferta. La vigencia de la garantía deberá ser igual al plazo de validez de la oferta establecido en el numeral 3.8 del presente Pliego de Condiciones.

El **"Sobre B"** deberá contener en su cubierta la siguiente identificación:

NOMBRE DEL OFERENTE/PROPONENTE
(Sello Social)
Firma del Representante Legal
COMITÉ DE COMPRAS Y CONTRATACIONES
SENADO DE LA REPÚBLICA
PRESENTACIÓN: **OFERTA ECONÓMICA**
REFERENCIA: SEN-CCC-CP- 2021-001

Las Ofertas deberán ser presentadas únicas y exclusivamente en el formulario designado al efecto, **(SNCC.F.033)**, **siendo inválida toda oferta bajo otra presentación**.

La Oferta Económica deberá presentarse en Pesos Dominicanos (RD$). Los precios deberán expresarse en **dos decimales (XX.XX)** que tendrán que incluir todas las tasas (divisas), impuestos y gastos que correspondan, transparentados e implícitos según corresponda.

El Oferente será responsable y pagará todos los impuestos, derechos de aduana, o gravámenes que hubiesen sido fijados por autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los bienes y servicios conexos a ser suministrados.
Ninguna institución sujeta a las disposiciones de la Ley que realice contrataciones, podrá contratar o convenir sobre disposiciones o cláusulas que dispongan sobre exenciones o exoneraciones de impuestos y otros atributos, o dejar de pagarlos, sin la debida aprobación del Congreso Nacional.

El Oferente/Proponente que cotice en cualquier moneda distinta al Peso Dominicano (RD$), **se auto-descalifica para ser adjudicatario.**

A fin de cubrir las eventuales variaciones de la tasa de cambio del Dólar de los Estados Unidos de Norteamérica (US$), **EL SENADO DE LA REPÚBLICA** podrá considerar eventuales ajustes, una vez que las variaciones registradas sobrepasen el **cinco por ciento (5%)** con relación al precio adjudicado o de última aplicación. La aplicación del ajuste podrá ser igual o menor que los cambios registrados en la Tasa de Cambio Oficial del Dólar Americano (US$) publicada por el Banco Central de la República Dominicana, a la fecha de la entrega de la Oferta Económica.

En el caso de que el Oferente/Proponente Adjudicatario solicitara un eventual ajuste, **EL SENADO DE LA REPÚBLICA** se compromete a dar respuesta dentro de los siguientes **cinco (5) días hábiles**, contados a partir de la fecha de acuse de recibo de la solicitud realizada.

La solicitud de ajuste no modifica el Cronograma de Entrega de Cantidades Adjudicadas, por lo que, el Proveedor Adjudicatario se compromete a no alterar la fecha de programación de entrega de los Bienes pactados, bajo el alegato de esperar respuesta a su solicitud.

Los precios no deberán presentar alteraciones ni correcciones y **deberán ser dados en la unidad de medida establecida en el Formulario de Oferta Económica.**

En los casos en que la Oferta la constituyan varios bienes, solo se tomará en cuenta la cotización únicamente de lo evaluado CONFORME en el proceso de evaluación técnica.

Será responsabilidad del Oferente/Proponente la adecuación de los precios unitarios a las unidades de medidas solicitadas, considerando a los efectos de adjudicación el precio consignado en la Oferta Económica como el unitario y valorándolo como tal, respecto de otras Ofertas de los mismos productos. El Comité de Compras y Contrataciones, no realizará ninguna conversión de precios unitarios si éstos se consignaren en unidades diferentes a las solicitadas.

Sección III
Apertura y Validación de Ofertas

3.1 Procedimiento de Apertura de Sobres

La apertura de Sobres se realizará en acto público en presencia del Comité de Compras y Contrataciones y del Notario Público actuante, en la fecha, lugar y hora establecidos en el Cronograma de Licitación.

Una vez pasada la hora establecida para la recepción de los Sobres de los Oferentes/Proponentes, no se aceptará la presentación de nuevas propuestas, aunque el acto de apertura no se inicie a la hora señalada.

3.2 Apertura de "Sobre A", contentivo de Propuestas Técnicas

El Notario Público actuante procederá a la apertura de los "**Sobres A**", según el orden de llegada, procediendo a verificar que la documentación contenida en los mismos esté correcta de conformidad con el listado que al efecto le será entregado. El Notario Público actuante, deberá rubricar y sellar cada una de las páginas de los documentos contenidos en los "**Sobres A**", haciendo constar en el mismo la cantidad de páginas existentes.

En caso de que surja alguna discrepancia entre la relación y los documentos efectivamente presentados, el Notario Público autorizado dejará constancia de ello en el acta notarial.

El Notario Público actuante elaborará el acta notarial correspondiente, incluyendo las observaciones realizadas en el desarrollo del acto de apertura de los Sobres A, si las hubiere.
El Notario Público actuante concluido el acto de recepción, dará por cerrado el mismo, indicando la hora de cierre.

Las actas notariales estarán disponibles para los Oferentes/ Proponentes, o sus Representantes Legales, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.3 Validación y Verificación de Documentos

Los Peritos, procederán a la validación y verificación de los documentos contenidos en el referido "**Sobre A**". Ante cualquier duda sobre la información presentada, podrá comprobar, por los medios que considere adecuados, la veracidad de la información recibida.

No se considerarán aclaraciones a una Oferta presentadas por Oferentes cuando no sean en respuesta a una solicitud de la Entidad Contratante. La solicitud de aclaración por la Entidad Contratante y la respuesta deberán ser hechas por escrito.

Antes de proceder a la evaluación detallada del "**Sobre A**", los Peritos determinarán si cada Oferta se ajusta sustancialmente al presente término de referencia y condiciones específicas; o si existen desviaciones, reservas, omisiones o errores de naturaleza o de tipo subsanables de conformidad a lo establecido en el numeral 1.21 del presente documento.

En los casos en que se presenten desviaciones, reservas, omisiones o errores de naturaleza o tipo subsanables, los Peritos Especialistas procederán de conformidad con los procedimientos establecidos en el presente Pliego de Condiciones Específicas.

3.4 Criterios de Evaluación

Las Propuestas deberán contener la documentación necesaria, suficiente y fehaciente para demostrar los siguientes aspectos que serán verificados bajo la modalidad **"CUMPLE/ NO CUMPLE":**

Elegibilidad: Que el Proponente está legalmente autorizado para realizar sus actividades comerciales en el país.

Capacidad Técnica: Que los Bienes cumplan con las todas características especificadas en las Fichas Técnicas.

3.6 Apertura de los "Sobres B", Contentivos de Propuestas Económicas

El Comité de Compras y Contrataciones, dará inicio al Acto de Apertura y lectura de las Ofertas Económicas, **"Sobre B",** conforme a la hora y en el lugar indicado.

Sólo se abrirán las Ofertas Económicas de los Oferentes/Proponentes que hayan resultado habilitados en la primera etapa del proceso. Son éstos aquellos que una vez finalizada la evaluación de las Ofertas Técnicas, cumplan con los criterios señalados en la sección Criterios de evaluación. Las demás serán devueltas sin abrir. De igual modo, solo se dará lectura a los renglones que hayan resultado CONFORME en el proceso de evaluación de las Ofertas Técnicas.

A la hora fijada en el Cronograma, el Consultor Jurídico de la institución, en su calidad de Asesor Legal del Comité de Compras y Contrataciones, hará entrega formal al Notario Público actuante, en presencia de los Oferentes, de las Propuestas Económicas, **"Sobre B",** que se mantenían bajo su custodia, para dar inicio al procedimiento de apertura y lectura de las mismas.

En acto público y en presencia de todos los interesados el Notario actuante procederá a la apertura y lectura de las Ofertas Económicas, certificando su contenido, rubricando y sellando cada página contenida en el **"Sobre B".**

Las observaciones referentes a la Oferta que se esté leyendo, deberán realizarse en ese mismo instante, levantando la mano para tomar la palabra. El o los Notarios actuantes procederán a hacer constar todas las incidencias que se vayan presentando durante la lectura.

Finalizada la lectura de las Ofertas, el o los Notarios actuantes procederán a invitar a los Representantes Legales de los Oferentes/Proponentes a hacer conocer sus observaciones; en caso de conformidad, se procederá a la clausura del acto.

No se permitirá a ninguno de los presentes exteriorizar opiniones de tipo personal o calificativos peyorativos en contra de cualquiera de los Oferentes participantes.

El Oferente/Proponente o su representante que durante el proceso de la Licitación tome la palabra sin ser autorizado o exteriorice opiniones despectivas sobre algún producto o compañía, será sancionado con el retiro de su presencia del salón, con la finalidad de mantener el orden.

En caso de discrepancia entre la Oferta presentada en el formulario correspondiente, **(SNCC.F.033)**, debidamente recibido por el Notario Público actuante y la lectura de la misma, prevalecerá el documento escrito.

El o los Notarios Públicos actuantes elaborarán el acta notarial correspondiente, incluyendo las observaciones realizadas al desarrollo del acto de apertura, si las hubiera, por parte de los Representantes Legales de los Oferentes/ Proponentes. El acta notarial deberá estar acompañada

de una fotocopia de todas las Ofertas presentadas. Dichas actas notariales estarán disponibles para los Representantes Legales de los Oferentes/Proponentes, quienes para obtenerlas deberán hacer llegar su solicitud a través de la Oficina de Acceso a la Información (OAI).

3.7 Confidencialidad del Proceso

Las informaciones relativas al análisis, aclaración, evaluación y comparación de las Ofertas y las recomendaciones para la Adjudicación del Contrato no podrán ser reveladas a los Licitantes ni a otra persona que no participe oficialmente en dicho proceso hasta que se haya anunciado el nombre del Adjudicatario, a excepción de que se trate del informe de evaluación del propio Licitante. Todo intento de un Oferente para influir en el procesamiento de las Ofertas o decisión de la Adjudicación por parte del Contratante podrá dar lugar al rechazo de la Oferta de ese Oferente.

3.8 Plazo de Mantenimiento de Oferta

Los Oferentes/Proponentes deberán mantener las Ofertas por el término de TREINTA DIAS (30) días hábiles contados a partir de la fecha del acto de apertura.

.

3.9 Evaluación Oferta Económica

El Comité de Compras y Contrataciones evaluará y comparará únicamente las Ofertas que se ajustan sustancialmente al presente Pliego de Condiciones Específicas y que hayan sido evaluadas técnicamente como **CONFORME**, bajo el criterio del menor precio ofertado.

Sección IV
Adjudicación

4.1 Criterios de Adjudicación

El Comité de Compras y Contrataciones evaluará las Ofertas dando cumplimiento a los principios de transparencia, objetividad, economía, celeridad y demás, que regulan la actividad contractual, y comunicará por escrito al Oferente/Proponente que resulte favorecido. Al efecto, se tendrán en cuenta los factores económicos y técnicos más favorables.

La Adjudicación será decidida a favor del Oferente/Proponente cuya propuesta cumpla con los requisitos exigidos y sea calificada como la más conveniente para los intereses institucionales, teniendo en cuenta el precio, la calidad, y las demás condiciones que se establecen en el presente Términos de Referencias y Condiciones Específicas.

Si se presentase una sola Oferta, ella deberá ser considerada y se procederá a la Adjudicación, si habiendo cumplido con lo exigido en el Pliego de Condiciones Específicas, se le considera conveniente a los intereses de la Institución.

4.2 Empate entre Oferentes

En caso de empate entre dos o más Oferentes/Proponentes, se procederá de acuerdo al siguiente procedimiento:

El Comité de Compras y Contrataciones procederá por una elección al azar, en presencia de Notario Público y de los interesados, utilizando para tales fines el procedimiento de sorteo.

4.3 Declaración de Desierto

El Comité de Compras y Contrataciones podrá declarar desierto el procedimiento, total o parcialmente, en los siguientes casos:

- Por no haberse presentado Ofertas.
- Por haberse rechazado, descalificado, o porque son inconvenientes para los intereses nacionales o institucionales todas las Ofertas o la única presentada.

En la Declaratoria de Desierto, la Entidad Contratante podrá reabrirlo dando un plazo para la presentación de Propuestas de hasta un **cincuenta por ciento (50%)** del plazo del proceso fallido.

4.5 Adjudicaciones Posteriores

En caso de incumplimiento del Oferente Adjudicatario, la Entidad Contratante procederá a solicitar, mediante ***"Carta de Solicitud de Disponibilidad"***, al siguiente Oferente/Proponente que certifique si está en capacidad de suplir los renglones que le fueren indicados, en un plazo no mayor de treinta (30) días. Dicho Oferente/Proponente contará con un plazo de **Cuarenta y Ocho (48) horas** para responder la referida solicitud. En caso de respuesta afirmativa, El Oferente/Proponente deberá presentar la Garantía de Fiel cumplimiento de Contrato, conforme se establece.

PARTE 2
CONTRATO

Sección V
Disposiciones Sobre los Contratos

5.1 Condiciones Generales del Contrato

5.1.1 Validez del Contrato

El Contrato será válido cuando se realice conforme al ordenamiento jurídico y cuando el acto definitivo de Adjudicación y la constitución de la Garantía de Fiel Cumplimiento de Contrato sean cumplidos.

5.1.2 Garantía de Fiel Cumplimiento de Contrato

La Garantía de Fiel Cumplimiento de Contrato corresponderá a una Póliza de Fianza o Garantía Bancaria. La vigencia de la garantía será conforme al período de vigencia del contrato, contados a partir de la Notificación de la Adjudicación, por el importe del **CUATRO POR CIENTO (4%)** del monto total del Contrato a intervenir, a disposición de la Entidad Contratante, cualquiera que haya sido el procedimiento y la forma de Adjudicación del Contrato. En el caso de que el adjudicatario sea una Micro, Pequeña y Mediana empresa (MIPYME) el importe de la garantía será de un **UNO POR CIENTO (1%).**

5.1.3 Perfeccionamiento del Contrato

Para su perfeccionamiento deberán seguirse los procedimientos de contrataciones vigentes, cumpliendo con todas y cada una de sus disposiciones y el mismo deberá ajustarse al modelo que se adjunte al presente Pliego de Condiciones Específicas, conforme al modelo estándar el Sistema Nacional de Compras y Contrataciones Públicas.

5.1.4 Plazo para la Suscripción del Contrato

Los Contratos deberán celebrarse en el plazo que se indique en el presente Pliego de Condiciones Específicas; no obstante a ello, deberán suscribirse en un plazo no mayor de **veinte (20) días hábiles**, contados a partir de la fecha de Notificación de la Adjudicación.

5.1.5 Incumplimiento del Contrato

Se considerará incumplimiento del Contrato:

a. La mora del Proveedor en la entrega de los Bienes.

b. La falta de calidad de los Bienes suministrados.

c. El Suministro de menos unidades de las solicitadas, no aceptándose partidas incompletas para los adjudicatarios en primer lugar.

5.1.6 Efectos del Incumplimiento

El incumplimiento del Contrato por parte del Proveedor determinará su finalización y supondrá para el mismo la ejecución de la Garantía Bancaria de Fiel Cumplimiento del Contrato, procediéndose a contratar al Adjudicatario que haya quedado en el segundo lugar.

En los casos en que el incumplimiento del Proveedor constituya falta de calidad de los bienes entregados o causare un daño o perjuicio a la institución, o a terceros, la Entidad Contratante podrá solicitar a la Dirección General de Contrataciones Pública, en su calidad de Órgano Rector del Sistema, su inhabilitación temporal o definitiva, dependiendo de la gravedad de la falta.

5.1.7 Ampliación o Reducción de la Contratación

La Entidad Contratante no podrá producir modificación alguna de las cantidades previstas en el Pliego de Condiciones Específicas.

5.1.8 Finalización del Contrato

El Contrato finalizará por vencimiento de su plazo, o por la concurrencia de alguna de las siguientes causas de resolución:

- Incumplimiento del Proveedor.
- Incursión sobrevenida del Proveedor en alguna de las causas de prohibición de contratar con la Administración Pública que establezcan las normas vigentes, en especial el Artículo 14 de la Ley No. 340-06, sobre Compras y Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones.

5.1.9 Subcontratos

En ningún caso el Proveedor podrá ceder los derechos y obligaciones del Contrato a favor de un tercero, ni tampoco estará facultado para subcontratarlos sin la autorización previa y por escrito de la Entidad Contratante.

5.2 Condiciones Específicas del Contrato

5.2.1 Vigencia del Contrato

La vigencia del Contrato será a partir de la fecha de la suscripción del mismo y hasta su fiel cumplimiento, de conformidad con el Cronograma de Entrega de Cantidades Adjudicadas, el cual formará parte integral y vinculante del mismo.

5.2.2 Inicio del Suministro

Una vez notificada la adjudicación de Suministro entre la Entidad Contratante y el Proveedor, éste último iniciará el Suministro de los Bienes y servicios que se requieran mediante y forma parte constitutiva, obligatoria y vinculante del presente término de referencia y condiciones específica.

5.2.3 Modificación del Cronograma de Entrega

La Entidad Contratante, como órgano de ejecución del Contrato se reserva el derecho de modificar de manera unilateral el Cronograma de Entrega de los Bienes y servicios Adjudicados, conforme entienda oportuno a los intereses de la institución.

Si el Proveedor no suple los Bienes en el plazo requerido, se entenderá que la misma renuncia a su Adjudicación y se procederá a declarar como Adjudicatario al que hubiese obtenido el segundo

(2do.) lugar y así sucesivamente, en el orden de Adjudicación y de conformidad con el Reporte de Lugares Ocupados. De presentarse esta situación, la Entidad Contratante procederá a ejecutar la Garantía Bancaria de Fiel Cumplimiento del Contrato, como justa indemnización por los daños ocasionados.

PARTE 3
ENTREGA Y RECEPCIÓN

Sección VI
Recepción de los Productos

6.1 Requisitos de Entrega

Todos los bienes y servicios adjudicados deben ser entregados conforme a las especificaciones técnicas solicitadas, así como en el lugar de entrega convenido con **EL SENADO DE LA REPÚBLICA,** siempre con previa coordinación con el Director de Informática del Senado y técnicos asignados.

6.2 Recepción Provisional

El Encargado de Compras y Suministro en coordinación con la Dirección de Informática debe recibir los bienes de manera provisional hasta tanto verifique que los mismos corresponden con las características técnicas de los bienes adjudicados.

6.3 Recepción Definitiva

Si los Bienes son recibidos CONFORME y de acuerdo a lo establecido en el presente Término de referencia y Condiciones Específicas, en el Contrato se procede a la recepción definitiva.

No se entenderán suministrados, ni entregados los Bienes que no hayan sido objeto de recepción definitiva.

6.4 Obligaciones del Proveedor

El Proveedor está obligado a reponer Bienes deteriorados durante su transporte o en cualquier otro momento, por cualquier causa que no sea imputable a la Entidad Contratante.

Si se estimase que los citados Bienes no son aptos para la finalidad para la cual se adquirieron, se rechazarán los mismos y se dejarán a cuenta del Proveedor, quedando la Entidad Contratante exenta de la obligación de pago y de cualquier otra obligación.

El Proveedor es el único responsable ante Entidad Contratante de cumplir con el Suministro de los renglones que les sean adjudicados, en las condiciones establecidas en los presente Términos de

referencia y Condiciones Específicas. El Proveedor responderá de todos los daños y perjuicios causados a la Entidad Contratante y/o entidades destinatarias y/o frente a terceros derivados del proceso contractual.

Sección VII
Formularios

7.1 Formularios Tipo

El Oferente/Proponente deberá presentar sus Ofertas de conformidad con los Formularios determinados en el presente Término de referencia y Condiciones Específicas, **los cuales se anexan como parte integral del mismo.**

7.2 Anexos (descargar página web de Compras y Contrataciones, sección: Documento Estándar).

1. Formulario de Oferta Económica **(SNCC.F.033)**
2. Presentación de Oferta **(SNCC.F.034)**
3. Garantía bancaria de Fiel Cumplimiento de Contrato **(SNCC.D.038)**,
4. Formulario de Información sobre el Oferente **(SNCC.F.042)**
5. Formulario de Autorización del Fabricante **(SNCC.F.047)**,