Consejo del Poder Judicial

17 de agosto

2017

Este pliego contiene las condiciones y especificaciones técnicas para presentar propuestas de adquisición de Equipos tecnológicos para el control de riesgo y seguridad, correspondiente a la fase I del proyecto "Modelo de Administración de riesgo de la redes de la Jurisdicción Inmobiliaria".

Pliego de Condiciones Licitación Pública Nacional LPN-CPJ-12-2017.

1. Tabla de contenido

Pliego de Condiciones Licitación Pública Nacional

2. Introducción

El presente documento contiene los requerimientos que establece el Consejo del Poder Judicial a las empresas legalmente registradas en el Registro Nacional de Proveedores, para participar en el proceso de Licitación Pública Nacional a celebrarse **el jueves 17 de agosto de 2017, a las 10:00 a.m.,** horas de la mañana, en el Salón Multiusos, ubicado en el tercer (3er) nivel del Edificio de la Suprema Corte de Justicia, en la Av. Enrique Jiménez Moya, esq. Juan de Dios Ventura Simó, Centro de los Héroes, Santo Domingo, Rep. Dom. Sólo podrá postergarse por causas de fuerza mayor o caso fortuito definidos en el presente Pliego de Condiciones.

Este documento constituye la base para la preparación de las ofertas. Si el oferente omite suministrar alguna información requerida en el presente Pliego de Condiciones 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.

Esta licitación está a cargo del Comité de Compras y Licitaciones del Consejo del Poder Judicial, por lo que siempre que se mencione la palabra Comité se refiere a éste.

3. Información General de Licitación Pública Nacional

3.1 *Objeto*

El presente documento establece 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 físicas o jurídicas, que deseen participar en esta licitación pública para la adquisición, instalación y puesta en funcionamiento de **Equipos Firewalls y Balanceadores de Carga (Application Delivery Controllers (ADCs)** para la Gestión de Seguridad de la Información en la Red Perimetral, para el Modelo de Administración de Riesgos de las Redes de la Jurisdicción Inmobiliaria (JI), fase I. El presente proceso de Licitación Pública Nacional fue aprobado por el Consejo del Poder Judicial mediante Acta núm.15/2017.

3.2 *Responsabilidades del Oferente*

Es responsabilidad de los oferentes que en la presentación de las propuestas deban cumplir con los siguientes requisitos:

a) Descripción de los detalles técnicos de todos los equipos presentados.
b) La propuesta presentada deberá describir el número (#) de parte con que se cumplirá cada requerimiento.
c) Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte.
d) La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF). El formato digital debe permitir realizar búsqueda dentro del documento (OCR).
e) Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.

3.3 *Especificaciones técnicas*

A continuación, presentamos un cuadro conteniendo los lotes, cantidades de artículos y especificaciones técnicas para la adquisición, instalación y puesta en funcionamiento de **Equipos Firewalls y Balanceadores de Carga (Application Delivery Controllers (ADCs)** para la Gestión de Seguridad de la Información en la Red Perimetral, para el Modelo de Administración de Riesgos de las Redes de la JI, fase I, este deberá incluir:

Lote No.1: Equipos Firewalls.

a) Requerimientos de Contratación, Garantía y Soporte

Los requerimientos de contratación, garantía y soporte para la adquisición, instalación y puesta en funcionamiento de los equipos Firewalls son los siguientes:

Req. No.	**Descripción**
Requerimientos de Contratación (RDC).	
Acreditaciones y Experiencia del Oferente.	
RDC01	El Oferente debe contar con una experiencia mínima de tres (3) años y con tres (3) o más clientes, fuera o dentro del territorio dominicano, donde haya ejecutado proyectos de implementación de soluciones de Firewalls de manera satisfactoria y cualquier otro equipo que esté contemplado en la propuesta de implementación. Para esto el Oferente presentará una carta de recomendación por cada uno de los tres (3) o más clientes referenciados, tal como se lista en las especificaciones del Pliego.
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de Firewalls y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Para tal efecto, el Oferente presentará una Carta de Certificación del Fabricante, de que puede vender, dar soporte a los equipos y soluciones de este Fabricante en la República Dominicana.
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones Firewalls y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.
RDC04	Las Soluciones propuestas de Firewalls deben estar dentro del Informe de Gardner, "Magic Quadrant for Enterprise Network Firewalls", dentro del cuadrante de Retadores o Líderes (Challengers o Leaders). Dicho informe de referencia deberá ser actualizado, es decir, debe ser la última publicación valida. Este documento debe ser anexado a la Propuesta.
RDC05	La instalación y migración de los servicios, equipos, configuraciones y demás debe ser contemplada como parte de la propuesta; incluyendo la puesta en funcionamiento de las políticas de seguridad y monitoreo descritos en los requerimientos técnicos y funcionales. El cableado, Switches y demás componentes necesarios para la puesta en instalación y puesta en funcionamiento de las soluciones deben formar parte de la propuesta.
RDC06	Deben dejar en correcto funcionamiento todo lo relacionado a la infraestructura propuesta. La implementación de los equipos y aplicativos citados en este pliego no debe afectar las operaciones diarias de la JI, por lo que el oferente debe tomar las medidas necesarias para este requerimiento.
RDC07	Si el Oferente sub-contrata o integrara todos o parte de los servicios a ofrecer deberá presentar un acuerdo entre las partes donde indique su intención de trabajar en colaboración (Joint-Venture) en el proyecto de implementación de las soluciones. El Sub-contratado deberá contar con la anuencia de la Jurisdicción Inmobiliaria – Poder Judicial, siendo siempre el responsable ante la Institución el contratista (adjudicatario).
RDC08	Las Marcas de los equipos ofertados (Firewalls) para la "Red Perimetral Externa" deben ser diferente a los ofertados para la "Red Perimetral Interna"

Tiempos de Entrega y de Implementación.	
RDC09	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de Firewalls en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.
RDC10	La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.
RDC11	El oferente elaborará un documento informando los productos entregados e instalados; y validando los requerimientos técnicos que han sido cumplidos; así como los riesgos que han sido mitigados. Nota: Este documento debe contener la descripción de todas las políticas implementadas.
Normas de Seguridad Industrial.	
RDC12	El Oferente presentará como parte de su propuesta los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.
Responsabilidades del Oferente.	
RDC13	La presentación de las Propuestas debe cumplir con los siguientes requisitos: • Deben describir claramente la Marca y el Modelo ofertado. • Deben describir los detalles técnicos de todos los equipos presentados. • Las propuestas deberán ser presentadas en idioma español. • La propuesta presentada deberá describir (el **#** de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento. • Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte. • La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF) • El formato digital debe permitir realizar búsqueda dentro del documento (OCR). • Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.
RDC14	El Oferente revisará y leerá detenidamente el contenido de este documento, y hará las preguntas necesarias conforme al protocolo descrito en estos términos de referencia.
Requerimientos de Garantía y Soporte (RGS).	
Garantías y Soporte.	
RGS01	Las Soluciones propuestas de Firewallsy cualquier otro equipo (Ejemplo: Switches, Tokens, Licencias de Equipos, Software, entre otros) que esté contemplado en la propuesta de implementación contarán con una garantía en Piezas y Servicios (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo).**Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.
RGS02	El Software de Administración de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo).**Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación, comenzará a aplicarse a partir de la instalación y puesta en funcionamiento de las mismas. Nota: Para fines de Inicio del Periodo de Garantía, la Puesta en Funcionamiento del Equipo estará aprobada a partir del Documento de Aceptación, el cual será firmado por la JI y el Oferente.

RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación deberá ser posterior al tercer (3er.) año de garantía, tomando como referencia la fecha de esta licitación (Entrega/Apertura de Ofertas). Por lo que se solicita para validar este requerimiento que se presente la constancia escrita del fabricante de la Solución de Firewalls. La propuesta debe incluir equipos de última generación del fabricante.
RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año. Ejemplo: Si el costo del soporte y de Licenciamiento cuando se adquirió el equipo fue de 100 Pesos, este no podrá costar más 115 Pesos, es decir, no podrá ser mayor a un 15%.
RGS06	El Fabricante y el Oferente de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación deben presentar garantías (documentaciones) de que mantienen en la República Dominicana el inventario de todas partes y piezas necesarias para dar soporte a dicho equipo después de su puesta en producción.
Requerimientos de Capacitación.	
RGS07	Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes: ➢ Instalación, Configuración y Administración de los firewalls a instalar en la red perimetral y la red LAN.). Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos: • Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos. • Las capacitaciones serán realizadas de forma Presencial. • El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. • Estas capacitaciones deberán ser impartidas en idioma español. • Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes. • Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente. • El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI. • El oferente cubrirá con todos los costos de la capacitación. • Estas capacitaciones deben impartirse previo a la implementación de los equipos, para que la JI pueda definir las mejores prácticas a ponerse en ejecución durante el proceso de implementación de dichos equipos. Los instructores deberá ser docentes calificados y certificados por el/los fabricante /s de las soluciones a instalar. La empresa suplidora deberá correr con los gastos de alojamiento, viáticos y pasaje aéreo del personal docente, si se necesitaré participación de los instructores Extranjeros.

b) Requerimientos Técnicos para dos (2) Firewalls de la Red Perimetral Externa.

Estos dos (2) Firewalls serán instalados en alta disponibilidad en la red perimetral (externa) de la JI, para realizar las funciones de: primer filtrado de tráfico de información hacia nuestra red LAN, como antivirus hacia la red LAN, y para implementar políticas de seguridad que eviten posible fuga de información crítica de la JI desde la LAN hacia fuera de la institución.

Req. No.	Descripción
Requerimientos Funcionales y Técnicos (RFT).	
RFT01	**Dos (2) Firewalls** de última generación (ambos instalados en la parte externa de la red perimetral de la JI) e instalados en modo HA. Estos equipos deberán ser de una Marca diferente a los que se instalen "Red Perimetral Interna". El propósito de estos firewall serán los de responder preventivamente antes a las amenazas externas de la red (outside), concentrar las conexiones VPN y delimitar el acceso a los servicios externos en la DMZ.
RFT02	Los firewalls deben conectarse a 2 Switches Ethernet en modo Stack en el perímetro externo para soportar la infraestructura de los equipos que están en la DMZ. Características: • 1RU • 24 Puertos 1 Gigabit Ethernet. (Con sus Licencias y Transceiver incluidos) • 2 Puertos SFP+ a 10 Gigabit (Con sus Licencias y Transceiver incluidos) • Tecnología Stac kWise con 480 GB de throughput. • Power Supply Redundante. • Tecnología Stack Power. • Licencia IP Based. • Debe soportar IPv4, IPv6 routing, multicast routing, modular quality of service (QoS), Flexible NetFlow (FNF) y característica de seguridad mejorada (enhanced security features). Estos equipos (Switches) deberá contar con características avanzadas de Quality of Service (QoS) y cumplir con todos los requerimientos de contratación y garantía citados en el pliego.
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Firewall.
RFT04	La solución propuesta debe ser un equipo dedicado solo para estos fines.
RFT05	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.
RFT06	Debe cumplir con las siguientes especificaciones: • 35 Gbps de Stateful inspection firewall throughput. • 15 Gbps de Stateful inspection firewall throughput (multiprotocol). • 12 Gbps de throughput de NGWF (Firewall and Aplication Visibility and Control). • 10 Gbps de throughput de NGIPS. (IPS and Aplication Visibility and Control). • Multiples interface 10g. • High Availability Configurations and clustering. • Redundant Power Supplies. • Secure Boot. • Trust Anchor module. • Image signing.
RFT07	Debe tener capacidad de balanceo de interfaces WAN. Nota: Si el Firewall no realiza de manera nativa esta función, el oferente podrá incluir un equipo adicional al Firewalls de propósito específico para cumplir con esta capacidad.

RFT08	Debe tener las siguientes capacidades de prevención ataques DDoS: • Maximum mitigation capacity/throughput de 10 Gbps. • Maximum legitímate concurrent sessions de 209,000 Conexiones por Segundo (CPS) • Maximum DDoS flood attack prevention rate de 1,800,000 Paquetes por segundo (PPS).
RFT09	El equipo debe tener al menos 8 Gbps de Throughput de VPN IPSec.
RFT10	Debe tener capacidad de al menos 10 millones de sesiones simultáneas.
RFT11	Debe tener capacidad de al menos 150,000.00 nuevas sesiones por segundo.
RFT12	El equipo debe tener al menos 10,000.00 Túneles (IPsec Client / site-to-site VPN peers)
RFT13	La solución ofertada debe incluir al menos 8 puertos de 10 Gbps. SFP+
RFT14	Debe incluir al menos 10 FIREWALL virtuales.
RFT15	Debe incluir al menos 40 zonas de seguridad distintas.
RFT16	Debe soportar al menos 350 políticas.
RFT17	Estos equipos deben abarcar todas las rutas críticas de los servicios que tenemos instalados en nuestra zona perimetral.
RFT18	La solución propuesta debe ser de tipo Next Gen IPS / Next Gen Firewall con capacidad avanzada contra amenazas. Ejemplo de amenazas: Malware, Ataques día Cero, Denegación de Servicios, entre otros.
RFT19	El equipo debe poder ser configurado en modo Gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá hacer modificaciones en la red en cuanto a enrutamiento o direccionamiento IP.
RFT20	Debe tener Funcionalidades de: • NGIPS • NGFW • VPN – IPSec • DDoS • Anti-Malware
RFT21	Debe poder hacer integración con soluciones de LDAP y tener integrado Sandboxings.
RFT22	Debe tener capacidad para asignar parámetros de traffic shapping sobre reglas de firewall.
RFT23	Debe soportar la creación de políticas de tipo Firewall , VPN, subtipo por dirección IP, tipos de dispositivo y por usuario.
RFT24	Debe poder configurar la autenticación por usuario.
RFT25	Debe ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.(Discriminación de Certificado en Base a Trafico).
RFT26	Debe hacer escaneo de tráfico a profundidad dentro de todos o cierto rango de puertos configurados para este análisis.
RFT27	Debe analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
RFT28	Debe permitir la creación de políticas de tipo VPN (IPSEC/SSL).

RFT29	• Deberá soportar Clúster Firewalls con su sistema de análisis de red y management centralizado (Esta solución debe incluir el Sistema de Gestión y Análisis Centralizado para este Clúster) • El Clúster Firewalls deberá proveer al menos 8 interfaces 10Gbps. SFP+ (Con sus Licencias y Transceiver incluidos) • El Clúster Firewalls deberá proveer la creación de reglas de IPS. • Cluster de firewalls deberá proveer creación de VPN Site-To-Site en las versiones (IKEv1 y IKEv2). • Clúster de firewalls deberá proveer análisis de malware con los siguientes protocolos: Spero Analysis for MSEXE, Dynamic Analysis, Capacity Handling. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.
RFT30	Debe ser capaz de analizar, establecer control de acceso, detener ataques y hacer Antivirus en tiempo real en al menos en los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
RFT31	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP debe estar completamente integrada a la administración del dispositivo.
RFT32	El Antivirus debe incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
RFT33	El antivirus debe poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
RFT34	Debe tener capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
RFT35	El detector y preventor de intrusos debe soportar y captar ataques por variaciones de protocolo, por firmas de ataques conocidos (signature based / misuse detection), reconocimiento de comportamiento de red y ataques día cero.
RFT36	Debe soportar actualización automática de firmas para el detector de intrusos.
RFT37	El Detector de Intrusos debe mitigar los efectos de los ataques de negación de servicios.
RFT38	Debe contar con funcionalidades de Sandboxing para que los archivos bloqueados sean ejecutados en un ambiente seguro para analizar su comportamiento.
RFT39	Debe poder realizar protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats).
RFT40	El Detector y Preventor de intrusos debe poder implementarse tanto en línea como fuera de línea.
RFT41	Debe tener capacidad de detección de más de 4000 ataques.
RFT42	Debe tener capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "Pull" (Consultar los centros de actualización por versiones nuevas).
RFT43	Debe guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos.
RFT44	Debe tener la capacidad de cuarentena, es decir, prohibir el tráfico subsiguiente a la detección de un posible ataque.
RFT45	La alta disponibilidad debe ser transparente, sin pérdida de conexiones en caso de que un nodo falle.
RFT46	Debe tener posibilidad de definir al menos dos interfaces para sincronía y poder gestionar cada equipo de manera independiente.
RFT47	Debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
RFT48	La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
RFT49	El listado de aplicaciones debe actualizarse periódicamente.

RFT50	Debe soportar inspección de Contenido SSL.
RFT51	La solución debe tener la capacidad de inspeccionar tráfico que esté siendo encriptado al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
RFT52	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
RFT53	El equipo debe ser capaz de analizar contenido cifrado.
RFT54	La solución ofertada debe permitir la administración vía web, cli, syslog, snmp2. Administración basada en roles y debe ser centralizada para todos los firewalls propuestos.
RFT55	Debe permitir almacenamiento de eventos de manera interna y/o en un repositorio que pueda consultarse luego con SQL.
RFT56	Debe contar con Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
RFT57	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox, Chrome) instalado sin necesidad de instalación de ningún software adicional.
RFT58	Debe poder virtualizar los servicios de seguridad.
RFT59	Se debe incluir la licencia para al menos 10 (Diez) instancias virtuales dentro de la solución a proveer.
RFT60	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.
RFT61	Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales.
RFT62	Debe de ser capaz de realizar análisis continuo y retrospección de archivo o detección.
RFT63	Debe ser posible obtener una visualización completa del alcance de una amenaza o ataque ya exitoso, como también contener, bloquear o poner en cuarentena.
RFT64	La solución ofertada debe de ser capaz de hacer recomendaciones de políticas o modificaciones de firewall o NGIPS.
RFT65	Debe de mostrar un perfil completo de los usuarios o direcciones IP internas, como sistema operativos, vulnerabilidades, protocolos, etc.
	OTROS REQUERIMIENTOS
RFT66	Todos los equipos de este Lote I serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos (2) UPS independientes para alta disponibilidad.
RFT67	Las Soluciones propuestas de **Firewalls** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad)

c) Requerimientos Técnicos para 2 Firewalls de la Red Perimetral Interna.

Estos 2 Firewalls serán instalados en alta disponibilidad entre parte externa de la DMZ y antes de la Red LAN de la JI, para realizar las funciones de: segundo filtrado de tráfico de información hacia nuestra red LAN, como antivirus hacia la red LAN, y para implementar políticas de seguridad que eviten posible fuga de información crítica de la JI desde la LAN hacia fuera de la institución.

Estos equipos serán implementados con políticas de seguridad diferentes a los 2 Firewalls que serán instalados en la parte externa de la red; a modo cubrir un mayor rango de riesgos de tráfico y liqueo de información, así como malwares, virus, entre otros.

Los requerimientos técnicos y funcionales para los dos (2) firewalls que serán instalados entre la red perimetral y local son los siguientes:

Req. No.	Descripción
Requerimientos Funcionales y Técnicos (RFT).	
RFT01	2 Firewalls de última generación (ambos instalados en la parte interna de la red perimetral de la JI, en la parte frontal de nuestra red LAN) e instalados en modo HA. Estos equipos deberán ser de una Marca diferente a los que se instalen en la "Red Perimetral Externa". El propósito de estos firewalls serán los de detectar y bloquear amenazas desde y hacia el centro de la red (Red Interna). Estos firewall tendrán la característica de Proxy Server para defender y controlar las actividades de los usuarios.
RFT02	Estos Firewalls estarán conectados a los Switches anteriormente citados en el RFT02 de la "Red Perimetral Externa".
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un SO desarrollado por el fabricante específicamente para propósitos de Firewall.
RFT04	La solución propuesta debe ser un equipo dedicado solo para estos fines.
RFT05	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.
RFT06	Debe cumplir con las siguientes especificaciones: • 80 Gbps de Throughput de Firewall (IPV4/IPV6). • 13 Gbps de Throughhput de IPS. • 5 Gbps de Threat Protection Throughput (Protección contra amenazas). • 7 Gbps de Throughput de NGWF. • Múltiple interface 10Gb. SFP+. • High Availability Configurations and clustering. • Redundant Power Supplies.
RFT07	Debe tener Funcionalidades de: • Laboratorio de Investigación. • URL – Filtering. • Application Control. • IPS. • Antivirus.
RFT08	Debe poder hacer integración con soluciones de LDAP y Sandboxings.
RFT09	Debe tener capacidad de balanceo de interfaces WAN.
RFT10	Debe tener capacidad de prevención contra ataques DDoS de 2 Gbps.
RFT11	Debe tener capacidad (Throughput) de al menos 49 Gbps de VPN IPSec
RFT12	Debe tener capacidad de al menos 11 Millones de sesiones simultáneas.

RFT13	Debe tener capacidad de al menos 280,000.00 nuevas sesiones por segundo.
RFT14	El equipo debe soportar al menos 20,000.00 túneles VPN IPSec / túnel.
RFT15	• 16 Interfaces Ethernet 10/100/1000 (Con sus Licencias y Transceiver incluidos). • 8 Interfaces 10GB SFP+ (Con sus Licencias y Transceiver incluidos).
RFT16	Debe tener capacidad de al menos 10,000.00 usuarios SSL VPN.
RFT17	Debe tener capacidad de al menos 10 enrutadores virtuales.
RFT18	Debe tener capacidad de al menos 40 zonas de seguridad distintas.
RFT19	Debe tener capacidad de al menos 350 políticas.
RFT20	Estos equipos deben abarcar todas las rutas críticas de los servicios que tenemos instalados entre nuestra zona perimetral y la red LAN.
RFT21	La solución propuesta debe ser de tipo Next Gen Firewall.
RFT22	El equipo debe poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
RFT23	Debe tener capacidad para asignar parámetros de traffic shapping sobre reglas de firewall.
RFT24	Debe tener capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente.
RFT25	Debe soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de dispositivo y por usuario.
RFT26	Debe poder habilitar funcionalidades de (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas.
RFT27	Deberá contar con soporte para los siguientes servicios: • Soporte de al menos 128 redes virtuales vlans 802.1q, • Traducción de direcciones de red (nat) por fuente y destino, por direcciones ip dinámicas y pool de puertos. • Bgp, ospf y rip2, dhcp server y dhcp relay. • Protocolos de encriptación ike, 3des (con encriptación a 128, 192 y 256 bits), aes, sha1 y md5. • Soporte de pppoe. • Capacidad de firewall con identificación de aplicaciones de al menos 1 Gbps. • Identificación, control (uso de aplicaciones por usuario mediante interacción con ldap, directorio activo o radius y dirección ip)y visibilidad de aplicaciones incluyendo peer-to-peer, redes sociales, mensajería instantánea y web 2.0. • Identificación, control (uso de aplicaciones por usuario mediante interacción con ldap, directorio activo o radius y dirección ip)y visibilidad de aplicaciones incluyendo peer-to-peer, redes sociales, mensajería instantánea y web 2.0.
RFT28	Debe poder configurar la autenticación por usuario.
RFT29	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.
RFT30	Debe ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.
RFT31	Debe hacer escaneo de tráfico a profundidad dentro de todos o cierto rango de puertos configurados para este análisis.
RFT32	Debe analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
RFT33	Debe permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.
RFT34	El filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.
RFT35	El filtro URL debe ser configurable directamente desde la interfaz de administración del equipo.
RFT36	Debe tener capacidad de filtrado de scripts en páginas web.
RFT37	El filtrado de contenido debe estar basado en categorías en tiempo real, integrado a la plataforma de seguridad del equipo, sin necesidad de instalar un servidor de aplicaciones adicionales.

RFT38	Debe poder definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
RFT39	Debe tener capacidad para realizar SSL VPNs.
RFT40	Debe poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
RFT41	RFT66 Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
RFT42	La solución propuesta deberá permitir la creación de un clúster de hasta 23 unidades, tener un puerto dedicado para un failover rápido entre dos unidades de menos de un segundo, soporte de configuración activo-activo / activo-pasivo, todas las direcciones IP virtuales de las aplicaciones deberán ser soportadas por un clúster virtual, la configuración se deberá sincronizar entre las unidades pertenecientes al clúster. Failover automático cuando los servicios reales se encuentren abajo en alguna unidad, el tiempo de failover deberá ser programable.
RFT43	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
RFT44	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP debe estar completamente integrada a la administración del dispositivo.
RFT45	El Antivirus debe incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.
RFT46	El antivirus debe poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
RFT47	Debe tener capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
RFT48	El detector y preventor de intrusos debe soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).
RFT49	Debe soportar actualización automática de firmas para el detector de intrusos.
RFT50	Debe soportar modo sniffer, para inspección vía un puerto espejo del tráfico de datos de la red.
RFT51	Debe soportar modo capa-2 (l2), para inspección de datos en línea y tener visibilidad y control del tráfico.
RFT52	Debe soportar modo capa-3 (l3), para inspección de datos en línea y tener visibilidad y control del tráfico. Generar ruteo virtual para al menos 10 ruteadores virtuales, manejo de tráfico entre diferentes zonas de seguridad, sub-redes, soportando al menos 40 zonas de seguridad.
RFT53	Debe soportar modo de trabajo mezclado sniffer, l2 y l3 en diferentes interfaces físicas.
RFT54	Debe poder realizar protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats).
RFT55	El Detector y preventor de intrusos debe poder implementarse tanto en línea como fuera de línea.
RFT56	Debe tener capacidad de detección de más de 4000 ataques.
RFT57	Debe tener capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
RFT58	Debe guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos.
RFT59	Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque.
RFT60	Debe poder definir el tiempo en que se bloqueará el tráfico.
RFT61	Debe soportar control de tráfico ipv4 e ipv6.
RFT62	Debe permitir observar en una consola las principales aplicaciones y amenazas en proceso.
RFT63	La consola debe permitir la visualización detallada de los usuarios y sistemas más activos en la misma.

RFT64	Deben poder establecerse filtros dinámicos por tipos de aplicaciones, usuarios y equipos que muestren el uso y comportamiento del tráfico.
RFT65	Debe permitir la captura automática de paquetes cuando se detecta una amenaza. Esto debe poder ser activado y desactivado por política / perfil.
RFT66	Debe permitir la administración del ancho de banda mediante políticas, que se apliquen a nivel de aplicación o de usuario.
RFT67	Debe permitir definir clases de tráfico con parámetros de uso de ancho de banda y prioridad.
RFT68	Debe permitir el monitoreo del uso del ancho de banda por las aplicaciones a nivel de cantidad de bytes, sesiones y por usuario.
RFT69	Debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles ssl.
RFT70	Debe contar con software cliente de vpn-ssl para los sistemas operativos Windows.
RFT71	Debe permitir crear políticas para tráfico vpn-ssl.
RFT72	Debe soportar autenticación de vpn-ssl con ldap, secure id y base de datos propia.
RFT73	Debe permitir la creación de políticas basadas en el control por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo, control por usuario, grupos de usuarios o dirección ip.
RFT74	Debe permitir la creación de reportes personalizables y debe incluir al menos reportes de: sesiones por aplicación, utilización de ancho de banda, eventos, ataques, origen y destino del tráfico, usuarios más frecuentes, aplicaciones más frecuentes, amenazas más frecuentes, destinos más frecuentes.
RFT75	Debe permitir el almacenamiento de logs internamente o en ubicaciones externas definidas por el administrador.
RFT76	Debe poder manejar múltiples dominios de firewall.
RFT77	La alta disponibilidad debe ser transparente, sin pérdida de conexiones en caso de que un nodo falle.
RFT78	La alta disponibilidad debe poder configurarse en modo Activo- Activo / Activo-Pasivo.
RFT79	Debe tener posibilidad de definir al menos dos interfaces para sincronía y poder gestionar cada equipo de manera independiente.
RFT80	Debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
RFT81	La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.
RFT82	El listado de aplicaciones debe actualizarse periódicamente.
RFT83	Debe soportar inspección de Contenido SSL.
RFT84	La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
RFT85	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
RFT86	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
RFT87	El equipo debe ser capaz de analizar contenido cifrado para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.
RFT88	La solución ofertada debe permitir la administración vía web, cli, syslog, snmp2. Administración basada en roles y debe ser centralizada para todos los firewalls propuestos.
RFT89	Debe permitir almacenamiento de eventos de manera interna y/o en un repositorio que pueda consultarse luego con SQL.
RFT90	Debe contar con Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.

RFT91	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
RFT92	El oferente debe incluir los siguientes Software, Licencias y Equipos: • Autenticador-VM (Authenticator-VM) con licencia Perpetuas para 100 Usuarios. Este Autenticador debe correr en diferente plataforma de Virtualización, tales como: VMWare y Microsoft Hyper-V. • Debe incluirse software y licencia perpetua para 50 Generadores de contraseñas (Tokens Virtuales) para dispositivos iOS, Android y Windows Phone. (Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic license certificate). • Deben incluirse 50 Tokens Físicos (Generador de contraseña basado en tiempo). Licencia Perpetua. **Nota:** Estas licencias y equipo deben tener las mismas condiciones de los Requerimientos de Garantía y Soporte (RGS) anteriormente citados en este pliego.
	OTROS REQUERIMIENTOS
RFT93	Todos los equipos de este Lote I serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos (2) UPS independientes para alta disponibilidad.
RFT94	Las Soluciones propuestas de **Firewalls** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad).

Lote No. 2 Balanceadores de Carga (Application Delivery Controllers (ADCs)).

a) Requerimientos de Contratación, Garantía y Soporte Balanceadores de Carga (Application Delivery Controllers (ADCs)).

Los requerimientos de contratación, garantía y soporte para la adquisición, instalación y puesta en funcionamiento de los **Balanceadores de Carga (Application Delivery Controller (ADCs))** son los siguientes:

Req. No.	Descripción
Requerimientos de Contratación (RDC).	
Acreditaciones y Experiencia del Oferente.	
RDC01	El Oferente debe contar con una experiencia mínima de tres (3) años y con tres (3) o más clientes, fuera o dentro del territorio dominicano, donde haya ejecutado proyectos de implementación de soluciones **Aplication Deilvery Controllers (ADCs)** de manera satisfactoria y cualquier otro equipo que esté contemplado en la propuesta de implementación. Para esto el Oferente presentará una carta de recomendación por cada uno de los tres (3) o más clientes referenciados, tal como se lista en las especificaciones del Pliego.
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de **Aplication Deilvery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Para tal efecto, el Oferente presentará una Carta de Certificación del Fabricante, de que puede vender, dar soporte a los equipos y soluciones de este Fabricante en la República Dominicana.
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones **Aplication Deilvery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.
RDC04	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** deben estar dentro del Informe de Gardner**, "Magic Quadrant for Application Delivery Controllers",** dentro del cuadrante de **Líderes (Leaders).** Dicho informe de referencia deberá ser actualizado, es decir, debe ser la última publicación valida. Este documento debe ser anexado a la Propuesta.
RDC05	La instalación y migración de los servicios, equipos, configuraciones y demás debe ser contemplada como parte de la propuesta; incluyendo la puesta en funcionamiento de las políticas de seguridad y monitoreo descritos en los requerimientos técnicos y funcionales. El cableado, switches y demás componentes necesarios para la instalación y puesta en funcionamiento de las soluciones deben formar parte de la propuesta.
RDC06	Deben dejar en correcto funcionamiento todo lo relacionado a la infraestructura propuesta. La implementación de los equipos y aplicativos citados en este pliego no debe afectar las operaciones diarias de la JI, por lo que el oferente debe tomar las medidas necesarias para este requerimiento.
RDC07	Si el Oferente subcontrata o integrara todos o parte de los servicios a ofrecer deberá presentar un acuerdo entre las partes donde indique su intención de trabajar en colaboración (Joint-Venture) en el proyecto de implementación de las soluciones. El Subcontrato deberá contar con la anuencia de la Jurisdicción Inmobiliaria – Poder Judicial, siendo siempre el responsable ante la Institución el contratista (adjudicatario).
Tiempos de Entrega y de Implementación.	
RDC08	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de **Aplication Deilvery Controllers (ADCs)** en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.

RDC09	La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.
RDC10	El oferente elaborará un documento informando los productos entregados e instalados; y validando los requerimientos técnicos que han sido cumplidos; así como los riesgos que han sido mitigados. Nota: Este documento debe contener las descripción de todas las políticas implementadas.
Normas de Seguridad Industrial.	
RDC11	El Oferente presentará como parte de su propuesta los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.
Responsabilidades del Oferente.	
RDC12	La presentación de las Propuestas debe cumplir con los siguientes requisitos: • Deben describir claramente la Marca y el Modelo ofertado. • Deben describir los detalles técnicos de todos los equipos presentados. • Las propuestas deberán ser presentadas en idioma español. • La propuesta presentada deberá describir (el **#** de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento. • Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte. • La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF) • El formato digital debe permitir realizar búsqueda dentro del documento (OCR). • Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.
RDC13	El Oferente revisará y leerá detenidamente el contenido de este documento, y hará las preguntas necesarias conforme al protocolo descrito en estos términos de referencia.
Requerimientos de Garantía y Soporte (RGS).	
Garantías y Soporte.	
RGS01	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contarán con una garantía en Piezas y Servicios (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.
RGS02	El Software de Administración de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, comenzará a aplicarse a partir de la instalación y puesta en funcionamiento de las mismas. **Nota:**Para fines de Inicio del Periodo de Garantía y la Puesta en Funcionamiento de los Equipo estará aprobada a partir del Documento de Aceptación, el cual será firmado por la JI y el Oferente.
RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de **Aplication Deilvery Controller (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deberá ser posterior al tercer (3er.) año de garantía, tomando como referencia la fecha de esta licitación (Entrega/Apertura de Ofertas). Por lo que se solicita para validar este requerimiento que se presente la constancia escrita del fabricante de la Solución de **Aplication Deilvery Controller (ADCs)**. La propuesta debe incluir equipos de última generación del fabricante.

RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año. Ejemplo: si el costo del soporte y de Licenciamiento cuando se adquirió el equipo fue de 100 Pesos, este no podrá costar más 115 Pesos, es decir, no podrá ser mayor a un 15%.
RGS06	El Fabricante y el Oferente de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deben presentar garantías (documentaciones) de que mantienen en la República Dominicana el inventario de todas partes y piezas necesarias para dar soporte a dicho equipo después de su puesta en producción.
Requerimientos de Capacitación.	
RGS07	Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes: ➢ Instalación, Configuración y Administración de los **Aplication Deilvery Controllers (ADCs).** Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos: • Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos. • Las capacitaciones serán realizadas de forma Presencial. • El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. • Estas capacitaciones deberán ser impartidas en idioma español. • Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes. • Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente. • El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI. • El oferente cubrirá con todos los costos de la capacitación. • Estas capacitaciones deben impartirse previo a la implementación de los equipos, para que la JI pueda definir las mejores prácticas a ponerse en ejecución durante el proceso de implementación de dichos equipos. Los instructores deberá ser docentes calificados y certificados por el/los fabricante/s de las soluciones a instalar. La empresa suplidora deberá correr con los gastos de alojamiento, viáticos y pasaje aéreo del personal docente, si se necesitaré participación de los instructores Extranjeros.

b) Requerimientos Funcionales y Técnicos para 2 Balanceadores de Carga (Application Delivery Controllers (ADCs)) en la Red Perimetral.

Estos 2 balanceadores de carga **(Application Delivery Controllers (ADCs))** serán instalados en alta disponibilidad en la red perimetral de la JI, para monitorear el desempeño de los servidores y aplicativos que serán instalados para uso externo.
Los requerimientos técnicos y funcionales para los 2 balanceadores de carga son los siguientes:

1	Requerimientos Funcionales y Técnicos (RFT)
	CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO
RFT01	2 **Application Delivery Controller (ADCs),** o solución de balanceo de servidores y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un esquema de alta disponibilidad; ambos instalados en modo HA.
RFT02	El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado **"Appliance".**
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.
RFT04	Los valores de desempeño solicitados deberán ser logrados por el equipo **"Appliance"** como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios **"Appliance"** que logren sumar el valor solicitado.
RFT05	Se debe ofrecer dos (2) equipos en Alta disponibilidad (HA) funcionando en configuración Activo-Activo / Activo-Pasivo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.
RFT06	Cada equipo debe cumplir con las siguientes características: • La solución debe soportar un Throughput en L4 de al menos 10 Gbps. • La solución debe soportar un Throughput en L7 de al menos 10 Gbps. • La solución debe soportar un Throughput en SSL de al menos 10 Gbps. • La solución debe soportar una Compresión de Throughput de al menos 3.5 Gbps. • La solución deberá tener al menos 32 GB de Memoria. • La solución debe soportar al menos 1,400,000.00 Millones de peticiones en L7 HTTP requests/sec. • La solución de soportar al menos 13,000.00 Transacciones en SSL (SSL transactions/sec (2K key certificates) • La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • La solución de soportar al menos 6,000.00 Transacciones en ECDHE (ECDHE transactions/sec)
RFT07	Cada equipo debe tener al menos las siguientes Interfaces de red: • 4x10GE SFP+ (4 puertos SFP+ de 10 Gbps (Transceivers Incluidos)) • 6x10/100/1000 CU (con opción de conectividad de 1 Gbps cobre o fibra (Transceivers Incluidos)). • 2x1G For Management. **Nota:** Además de lo anteriormente mencionado, estos equipos deben tener Soporte de Transceivers 10G SFP+: SR, LR;XFP
RFT08	Las interfaces de 10G deben soportar velocidades de 1G o 10G dependiendo el transceiver usado.
RFT09	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 100 a 240 VAC.
RFT10	Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.
RFT11	Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.
RFT12	Cada equipo debe incluir 32 GB de Memoria RAM mínimo
RFT13	Cada equipo debe incluir mínimo un Disco duro de 240 GB SSD.

RFT14	El oferente deberá especificar detalladamente las especificaciones técnicas de los equipos ofertados, a nivel de Hardware y Software. Ejemplo: • Tipo de Memoria. • Cantidad de Memoria en GB. • Cantidad Slot de Memoria. • Capacidad máxima de Memoria Soportada. • Procesador. • Capacidad y Velocidad del procesador. • Marca del Procesador. • Cantidad de Núcleos del Procesador • Generación del Procesador. • Tipo de disco Duro (Sata, Sata III o Hibrido, SSD Etc.)
RFT15	Debe soportar Clúster Activo/Activo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).
RFT16	La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda.
RFT17	Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.
RFT18	Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.
RFT19	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.
2	**FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO**
RFT20	La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.
RFT21	La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
RFT22	La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.
RFT23	La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.
RFT24	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones.
RFT25	La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting: • Round Robín. • Proporcional (Ratio). • Proporcional dinámico. • Respuesta más rápida. • Conexiones mínimas. • Menor número de sesiones. • Tendencia de menor cantidad de conexiones (observed). • Tendencia de desempeño (predictive).
RFT26	Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM

RFT27	El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)
RFT28	El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.
RFT29	La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica.
RFT30	La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de: • Ping. • Chequeo a nivel de TCP y UDP a puertos específicos. • Monitoreo http y https. • Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft. • Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. • Ejecución de scripts para determinar la respuesta emulando un cliente. • Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. • Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma. • Monitoreo de aplicaciones de mercado: o LDAP o FTP o SMTP o IMAP/POP3 o Oracle o MSSQL o MySQL o RADIUS o SIP o Protocolo SASP o SOAP o WMI o SNMP
RFT31	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes: • Dirección IP origen. • Dirección IP destino. • Cookies. • Hash. • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia. • Sesiones SSL. • Microsoft Remote Desktop. • Entre otros.
RFT32	Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.
RFT33	Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.
RFT34	El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.
RFT35	Soporte de Scripts de Programación que permita crear funcionalidades que por defecto no se encuentran en el menú de configuración u opciones a través de un lenguaje gráfico.
RFT36	Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: • Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.

RFT37	Debe permitir la integración con plataformas de automatización a través del protocolo REST
RFT38	Soporte de RESTful API
RFT39	La solución debe tener la capacidad de ampliarse para soportar la creación de alta disponibilidad entre Datacenters a través de GSLB.
RFT40	La solución debe soportar la configuración de un portal de acceso unificado con capacidad de ofrecer n-factores de autenticación.
RFT41	Debe permitir la optimización de la interfaz y el tráfico presentado a los clientes que consumen las aplicaciones a través de la plataforma ADC (Front End Optimization).
RFT42	Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.
RFT43	Debe soportar el protocolo TDS para balanceo de MSSQL y SQL SERVER.
RFT44	Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT.
RFT45	El sistema deberá soportar scripts de programación basados en un lenguaje estructurado que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.
RFT46	El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC.
RFT47	Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP. La Base de datos de Geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).
3	**FUNCIONES DE SEGURIDAD GENERALES**
RFT48	Cada equipo debe soportar seguridad SSL con las siguientes características: • Incluir el soporte de Aceleración SSL usando Hardware Dedicado • Incluir mínimo 13,000.00 Transacciones por segundo SSL (2K Keys) • Incluir mínimo 6,000.00 Transacciones concurrente de Curva elíptica (ECDHE) • Soportar al menos 10 Gbps SSL (Throughput SSL) • La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • Soporte de llaves SSL de 1024, 2048 y 4096 bits
RFT49	La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL.
RFT50	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características • Session ID. • Session Ticket. • OCSP Stapling (on line certificate status protocol). • Dynamic Record Sizing. • ALPN (Application Layer Protocol Negotiation). • Forward Secrecy.
RFT51	La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital SignatureAlgorithm (DSA) y Elliptic Curve Cryptography (ECDHE).
RFT52	El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall). Nota: Debe Agregar certificación.
RFT53	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.
RFT54	Cada equipo debe incluir protección contra ataques de DDoS de mínimo 2,500,000.00 SYN/sec
RFT55	Firmado criptográfico de cookies para verificar su integridad.
RFT56	Capacidad de integración con dispositivos HSM "Hardware Security Module" (Módulo de Seguridad Hardware) externos. Deberá soportar al menos ThalesnShield YSafenet (Gemalto) Luna.
RFT57	La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.
RFT58	Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.

RFT59	Debe soportar HSTS (HTTP Strict Transport Security).
RFT60	Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías. • Scanners • Exploits Windows • Denial of Service • Proxies de Phishing • Botnets • Proxies anónimos
4	**FUNCIONES DE ACELERACIÓN DE TRÁFICO**
RFT61	La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: • Memoria cache. • Compresión tráfico HTTP • Optimización de conexiones a la aplicación a nivel TCP • Multiplexación de conexiones hacia los servidores
RFT62	El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Edge, Google Chrome, Mozilla Firefox, Safari, etc.
RFT63	Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 3.5 Gbps o superior
RFT64	Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.
RFT65	Debe soportar el protocolo HTTP y funcionar como Gateway para este protocolo.
RFT66	Permitir la modificación de los Tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los Tags generados por el Web server o modificarlos.
5	**FIREWALL DE APLICACIONES WEB (WAF)**
RFT67	La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un Appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).
RFT68	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.
RFT69	La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs, parámetros, métodos, de manera específica.
RFT70	Debe trabajar en un esquema proxy TCP Reverso y/o Transparente.
RFT71	Debe soportar la creación automática de políticas
RFT72	Debe trabajar con políticas de seguridad por capas, donde se configura una política de seguridad base y las políticas de seguridad hijas heredan sus configuraciones y permita que solo cambios específicos se apliquen a las políticas hijas.
RFT73	La creación automática de políticas deberá unificar múltiples URLs explicitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.
RFT74	Debe trabajar en modo de bloqueo o en modo informativo
RFT75	Debe permitir diferentes políticas de seguridad para diferentes aplicaciones
RFT76	Debe permitir la creación de firmas personalizadas
RFT77	Debe trabajar con modelos de seguridad positiva y negativa
RFT78	Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana.
RFT79	Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.
RFT80	El WAF debe permitir personalizar las páginas de bloqueo
RFT81	Debe prevenir exponer el "OS fingerprinting"
RFT82	Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.

RFT83	El WAF Debe soportar: • Restringir protocolo y versión utilizada. • Multi-byte language encoding. • Validar URL-encoded characters. • Restringir la longitud del método de request. • Restringir la longitud del URI solicitado. • Restringir el número de Encabezados (headers). • Restringir la longitud del nombre de los encabezados. • Restringir la longitud del valor de los encabezados. • Restringir la longitud del cuerpo (body) de la solicitud. • Restringir la longitud del nombre y el valor de las cookies. • Restringir el número de cookies. • Restringir la longitud del nombre y valor de los parámetros. • Restringir el número de parámetros.
RFT84	El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)
RFT85	El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP.
RFT86	El WAF debe incluir protección contra Web Scraping.
RFT87	Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario.
RFT88	Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento Cross-Domain, permitiendo evitar un CORS (Cross-Origin Resource Sharing).
RFT89	Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario
RFT90	Debe permitir el enmascaramiento de información sensible filtrada por el servidor
RFT91	Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de Geolocalización.
RFT92	Debe permitir la integración con servidores Antivirus.
RFT93	Debe brindar reportes respecto a la normativa PCI DSS 3.1 MINIMO.
RFT94	Debe proteger contra ataque DoS /DDoS de Capa 4 Y 7.
RFT95	Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa.
RFT96	En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico para poseer información forense.
RFT97	Debe soportar tecnologías AJAX y JSON .
RFT98	Debe proteger como mínimo: • Ataques de Fuerza Bruta. • Cross-site scripting (XSS). • Cross Site Request Forgery. • SQL injection. • Parameter and HPP tampering. • Sensitive information leakage. • Session high jacking. • Buffer overflows. • Cookie manipulation. • Various encoding attacks. • Broken access control. • Forceful browsing. • Hidden fields manipulation. • Requests muggling.

	• XML bombs/DoS. • Open Redirect.
RFT99	Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.
RFT100	Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP
RFT101	Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas
RFT102	Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.
RFT103	Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.
RFT104	Debe ofrecer protección sobre tráfico basado en Web Sockets.
RFT105	El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.
RFT106	Debe proteger las aplicaciones contra ataques de denegación de servicio a nivel de L4 y L7
6	**ESTÁNDARES DE RED**
RFT107	Soporte VLAN 802.1q, Vlantagging.
RFT108	Soporte de 802.3ad para definición de múltiples troncales
RFT109	Soporte de NAT, SNAT
RFT110	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.
RFT111	Soporte de Rate Shapping.
RFT112	Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.
RFT113	Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.
RFT114	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS,
7	**ADMINISTRACIÓN DEL SISTEMA**
RFT115	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS)
RFT116	La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.
RFT117	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.
RFT118	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.
RFT119	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales
RFT120	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: • Protocolo SysLog • Notificación vía SMTP • SNMP versión.2.0 o superior.
RFT121	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.
RFT122	El equipo debe contar con un módulo de administración tipo lightsout que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.
RFT123	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real
RFT124	Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.
RFT125	Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (Ejemplo: Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.

RFT126	Se debe un incluir una Herramienta de Análisis con su respectivo Licenciamiento, la cual permitirá una mejor gestión las solución ADCs Propuesta.
8	**OTROS REQUERIMIENTOS**
RFT127	Todos los equipos de este Lote serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos UPS independientes para alta disponibilidad.
RFT128	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad).

3.4 Modalidad de la Compra

La presente contratación se ejecutará por Licitación Pública Nacional, conforme a las disposiciones establecidas en el Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Consejo del Poder Judicial.

3.5 Fuente de Recursos

Los fondos para financiar el costo de la compra objeto de la presente Licitación Pública Nacional provienen de los fondos de Tasa por Servicio de la Jurisdicción Inmobiliaria, tomándose las previsiones correspondientes.

3.6 Órgano de contratación

El órgano administrativo competente para la adjudicación de que se trata es el Comité de Compras y Licitaciones del Consejo del Poder Judicial y para la contratación el Consejo del Poder Judicial.

3.7 Competencia Judicial

Todo litigio, controversia o reclamación resultante de este documento y/o el o los contratos a intervenir, sus incumplimientos, interpretaciones, resoluciones o nulidades serán sometidos al Tribunal Superior Administrativo conforme al procedimiento establecido en la Ley 13-07, de fecha cinco (05) de febrero del 2007.

3.8 Idioma

El idioma oficial de la presente Licitación Pública Nacional es el español, por tanto, toda la correspondencia y documentos generados durante el procedimiento que intercambien el oferente y el Comité de Compras y Licitaciones deberán ser presentados en este idioma; de encontrarse en idioma distinto, deberán contar con la traducción al español realizada por un intérprete judicial debidamente autorizado.

3.9 Moneda de la Oferta

La moneda de cotización debe ser expresada 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.

3.10 Visita Informativa al lugar del proyecto.

Los oferentes deberán realizar una visita de inspección al lugar del proyecto y obtener por sí mismos y bajo su responsabilidad y riesgo, toda la información que pueda ser necesaria para preparar sus propuestas. De no hacerlo, quedaran excluidos de participar en el presente proceso, por lo que no podrán alegar desconocimiento de las características de dicho emplazamiento y serán a su cargo las consecuencias económicas o de otro tipo que de ello pudieran derivarse. El costo económico de esta visita será por exclusiva cuenta de los oferentes.

Los oferentes deberán examinar el sitio y los alrededores del proyecto e informarse por su cuenta acerca de la forma y características de proyecto, las cantidades, localización y naturaleza del proyecto y los materiales necesarios para su ejecución, transporte, mano de obra, las instalaciones que se puedan requerir, complejidad, las condiciones del ambiente y, en general, sobre todas las circunstancias que puedan afectar o influir en el cálculo del valor de su propuesta.

Estas visitas podrán llevarse a cabo durante los días del 10 al 14 de julio de 2017, los representantes designados por la Gerencia de Tecnología de la Jurisdicción Inmobiliaria, tendrá la responsabilidad de trasladarse conjuntamente con los oferentes, al lugar donde se llevará a cabo el proyecto objeto de esta Licitación Pública Nacional, para mostrar in situ a los mismos donde se ejecutará.

Para la visita y reunión informativa coordinar al número (809)533-1555 Exts. 4185 y 4150 o a través del correo electrónico **tecnologiaji@ji.gob.do.**

Producto de la visita informativa los representantes Gerencia de Tecnología de la Jurisdicción Inmobiliaria, emitirán una copia de la constancia de visita a cada oferente, mientras que la original será entregada al Comité de Compras y Licitaciones. Los oferentes además firmarán un documento de confidencialidad el cual será enviado por la Gerencia de Tecnología de la Jurisdicción Inmobiliaria al Comité de Compras y Licitaciones.

La visita informativa de los Oferentes al lugar donde se llevará a cabo el proyecto es de carácter obligatorio y su inasistencia acarreará la eliminación automática de la propuesta.

3.11 Precio de la Oferta

Los precios cotizados por el oferente en el Formulario de Presentación de Oferta Económica (Anexo 1), deberán ajustarse a los requerimientos que se indican a continuación:

a) La oferta debe de incluir el número de parte con que se cumplirá cada requerimiento.

b) La oferta debe presentar los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.

c) Todas las partidas deberán enumerarse y cotizarse por separado en el Formulario de Presentación de Oferta Económica. Si un formulario de oferta económica detalla partidas pero no las cotiza, se asumirá que están incluidas en el precio total de la oferta.

d) Los precios cotizados por el oferente serán fijos durante la ejecución del contrato y no estarán sujetos a ninguna variación por ningún motivo. Los precios cotizados incluirán los impuestos, los gastos de servicios profesionales, transportación y acarreo hasta la entrega final en la División de Almacén de la Jurisdicción Inmobiliaria y la Gerencia de Tecnología de la JI, así como cualquier otro tipo de gasto.

e) Una vez adjudicado el oferente deberá asumir la totalidad de los costos, en relación a lo ofertado en su propuesta. El Consejo del Poder Judicial, no reconocerá ninguna exigencia por concepto de gastos adicional en materiales, equipos, personal u otros para la entrega e implementación de la misma durante el tiempo contratado; así como daños ocasionados en la infraestructura de la JI por parte del personal asignado del oferente.

3.12 De la Publicidad

A fin de cumplir con la transparencia y publicidad adecuada, la convocatoria o invitación a participar en el procedimiento por Licitación Pública Nacional objeto de este pliego, se efectuara mediante convocatoria en un mínimo de dos (2) diarios de circulación nacional por el término de dos (2) días consecutivos, y en la página web del Poder Judicial, **www.poderjudicial.gob.do**,con un plazo que no será inferior a treinta (30) días hábiles de antelación entre el momento de efectuarse la invitación y la fecha fijada para la apertura de las ofertas.

3.13 Consultas

Los oferentes podrán efectuar sus preguntas al Comité de Compras y Licitaciones para aclaraciones con respecto al Pliego de Condiciones, las cuales serán aceptadas hasta el día 25 de julio de 2017.

Las consultas las formularán los oferentes, sus representantes legales, o agentes autorizados, por escrito, dirigido al Comité de Compras y Licitaciones, dentro del plazo previsto; quien se encargará de obtener las respuestas conforme a la naturaleza de las mismas.

El Comité de Compras y Licitaciones dará respuestas a tales consultas, mediante notas aclaratorias, sin identificar quien consultó, en un plazo no más allá del día 04 de agosto de 2017, mediante publicación en el portal del Poder Judicial **(www.poderjudicial.gob.do).**

Las Consultas se remitirán al Comité de Compras y Contrataciones del Consejo del Poder Judicial, ubicado en la Avenida Enrique Jiménez Moya Esq. Juan de Dios Ventura Simó, Centro de los Héroes de Constanza, Maimón y Estero Hondo incluyendo la referencia de la Licitación o a través del correo electrónico **licitaciones-cpj@poderjudicial.gob.do.**

De considerarlo necesario, por iniciativa propia, o cuando como consecuencia de una pregunta, se requiera realizar una modificación al Pliego de Condiciones, mediante adenda o enmienda, la misma será aprobada por el Comité de Compras y Licitaciones, si procediere.

Las comunicaciones emitidas por el Comité pasarán a constituir parte integral del Pliego de Condiciones y en consecuencia, serán de cumplimiento obligatorio para todos los oferentes.

3.14 Subsanaciones

A los fines de la presente licitación, se considera que una oferta se ajusta sustancialmente a los pliegos de condiciones cuando concuerda con todos los términos y especificaciones de dichos documentos, sin desviaciones, reservas, omisiones o errores significativos. La ausencia de requisitos relativos a las credenciales de los oferentes es siempre subsanable.

La determinación del Comité de Compras y Licitaciones de que una oferta se ajusta sustancialmente a los documentos de la licitación se basará en el contenido de la propia oferta, sin que tenga que recurrir a pruebas externas.

Siempre que se trate de errores u omisiones de naturaleza subsanable entendiendo por éstos, generalmente, aquellas cuestiones que no afecten el principio de que las ofertas deben ajustarse sustancialmente a los Pliegos de Condiciones; pudiendo el Comité, siempre que se trate de errores u omisiones de naturaleza subsanable, requerir en un plazo breve contados a partir del requerimiento, que el oferente rectifique la información y/o suministre la documentación faltante;
Cuando proceda la posibilidad de subsanar errores u omisiones se interpretará en todos los casos bajo el entendido de que el Comité de Compras y Licitaciones tenga la posibilidad de contar con la mayor cantidad de ofertas validas posibles y de evitar que, por cuestiones formales

intrascendentes, se vea privada de optar por ofertas serias y convenientes desde el punto de vista del precio y la calidad.

No se podrá considerar error u omisión subsanable, cualquier corrección que altere la sustancia de una oferta para que se la mejore.

El Comité de Compras y Licitaciones rechazará toda oferta que no se ajuste sustancialmente al Pliego de Condiciones. No se admitirán correcciones posteriores que permitan que cualquier oferta, que inicialmente no se ajustaba a dicho pliego, posteriormente se ajuste al mismo.

3.15 Rectificaciones Aritméticas

Para fines de subsanaciones, los errores aritméticos serán corregidos de la siguiente manera:

a) Si existiere una discrepancia entre una cantidad parcial y la cantidad total obtenida multiplicando las cantidades parciales, prevalecerá la cantidad parcial y el total será corregido.

b) Si la discrepancia resulta de un error de suma o resta, se procederá de igual manera; esto es, prevaleciendo las cantidades parciales y corrigiendo los totales.

c) Si existiere una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras.

PÁRRAFO: Si el oferente no acepta la corrección de los errores, su oferta será rechazada.

3.16 Prohibición de Contratar

No podrán participar como Oferentes/Proponentes, en forma directa o indirecta, las personas físicas o sociedades comerciales que se relacionan a continuación:

a) El Presidente y Vicepresidente de la República; los Ministros y Viceministros de Estado; los Senadores y Diputados; los Magistrados de la Suprema Corte de Justicia y de los demás tribunales del orden judicial, los Magistrados del Tribunal Constitucional; los Magistrados del Tribunal Superior Electoral; los miembros de la Junta Central Electoral; los Alcaldes y Regidores de los Ayuntamientos de los Municipios y del Distrito Nacional; el Contralor General de la República y el Sub-contralor; el Director de Presupuesto y Subdirector; el Director Nacional de Planificación y el Subdirector; el Procurador General de la República y los demás miembros del Ministerio Público; el Tesorero Nacional y el Subtesorero y demás funcionarios de primer y segundo nivel de jerarquía de las instituciones incluidas bajo el ámbito de aplicación de la Ley 340-06;

b) Los jefes y subjefes del Ministerio de Defensa de la República Dominicana, así como el jefe y subjefes de la Policía Nacional;

c) Los funcionarios públicos con injerencia o poder de decisión en cualquier etapa del procedimiento de contratación administrativa;

d) Todo personal del Poder Judicial;

e) Los parientes por consanguinidad hasta al tercer grado o por afinidad hasta al segundo grado, inclusive, de los funcionarios relacionados con la contratación cubiertos por la prohibición, así como los cónyuges, las parejas en unión libre, las personas vinculadas con análoga relación de convivencia afectiva o con las que hayan procreado hijos y descendientes de estas personas;

f) Las personas jurídicas en las cuales las personas naturales a las que se refieren los Numerales 1 al 4 tengan una participación superior al diez por ciento (10%) del capital social, dentro de los seis meses anteriores a la fecha de la convocatoria;

g) Las personas físicas o jurídicas que hayan intervenido como asesoras en cualquier etapa del procedimiento de contratación o hayan participado en la elaboración de las especificaciones técnicas o los diseños respectivos, salvo en el caso de los contratos de supervisión;

h) Las personas físicas o jurídicas que hayan sido condenadas mediante sentencia que haya adquirido la autoridad de la cosa irrevocablemente juzgada, por delitos de falsedad o contra la propiedad, o por delitos de cohecho, malversación de fondos públicos, tráfico de influencia, prevaricación, revelación de secretos, uso de información privilegiada o delitos contra las finanzas públicas, hasta que haya transcurrido un lapso igual al doble de la condena. Si la condena fuera por delito contra la administración pública, la prohibición para contratar con el Estado será perpetua;

i) Las empresas cuyos directivos hayan sido condenados por delitos contra la administración pública, delitos contra la fe pública o delitos comprendidos en las convenciones internacionales de las que el país sea signatario;

j) Las personas físicas o jurídicas que se encontraren inhabilitadas en virtud de cualquier ordenamiento jurídico;

k) Las personas que suministraren informaciones falsas o que participen en actividades ilegales o fraudulentas relacionadas con la contratación;

l) Las personas naturales o jurídicas que se encuentren sancionadas administrativamente con inhabilitación temporal o permanente para contratar;

m) Las personas naturales o jurídicas que no estén al día en el cumplimiento de sus obligaciones tributarias o de la seguridad social, de acuerdo con lo que establezcan las normativas vigentes.

PÁRRAFO: Para los funcionarios contemplados en los acápites a) y b), la prohibición se extenderá hasta seis (6) meses después de la salida del cargo.

3.17 Demostración de Capacidad para Contratar

Los oferentes deben demostrar que:

a) No están embargados, en estado de quiebra o en proceso de liquidación; sus negocios no han sido puestos bajo administración judicial, y sus actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en su contra por cualquiera de los motivos precedentes;

b) Han cumplido con sus obligaciones tributarias y de seguridad social;

c) Han cumplido con las demás condiciones de participación, establecidas de antemano en los avisos y los presentes Pliegos de Condiciones;

d) Se encuentran legalmente domiciliados y establecidos en el país;

e) Que los fines sociales sean compatibles con el objeto contractual;

f) Que ni ellos ni su personal directivo hayan sido condenados por un delito relativo a su conducta profesional o por declaración falsa o fraudulenta acerca de su idoneidad para firmar un contrato adjudicado.

3.18 Disponibilidad del Pliego de Condiciones.

El Pliego de Condiciones estará disponible para quien lo solicite, en el edificio que aloja a la Suprema Corte de Justicia y el Consejo del Poder Judicial, en la División de Cotizaciones y Seguimiento de Compras, ubicada en el tercer piso de la Avenida Enrique Jiménez Moya esquina Juan de Dios Ventura Simó, Centro de los Héroes, Constanza, Maimón y Estero Hondo (La Feria), en el horario de ocho de la mañana (8:00 a.m.) a cuatro quince de la tarde (4:15 P.m); y en la página Web de la institución: www.poderjudicial.gob.do para todos los interesados.

3.19 Conocimiento y Aceptación del Pliego de Condiciones.

El sólo hecho de un oferente participar en la Licitación Pública Nacional implica pleno conocimiento, aceptación y sometimiento a él, por sus miembros, ejecutivos, representante legal y agentes autorizados, de los procedimientos, condiciones, estipulaciones y normativas, sin excepción alguna, establecidos en el presente Pliego de Condiciones, el cual tiene carácter jurídicamente obligatorio y vinculante.

4. Datos de la Licitación Pública Nacional.

4.1 Lugar, Fecha y Hora.

La presentación de Propuestas "Sobre A" y "Sobre B" se efectuará ante el Comité de Compras y Licitaciones y el Notario Público actuante, en fecha **17 de agosto de 2017, a las 10:00 a.m,** horas de la tarde, en el Salón Multiusos, ubicado en el tercer (3er) nivel del Edificio de la Suprema Corte de Justicia, en la Av. Enrique Jiménez Moya, esq. Juan de Dios Ventura Simó, Centro de los Héroes, Santo Domingo, Rep. Dom. Sólo podrá postergarse por causas de fuerza mayor o caso fortuito definidos en el presente Pliego de Condiciones.

4.2 Tiempo de Entrega.

El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de **Firewalls y las soluciones de Aplication Deilvery Controllers (ADCs)** en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.
La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.

4.3 Condiciones/Forma de Pago.

Se procederá a realizar un primer pago correspondiente al avance, el cual será igual o menor a un veinte por ciento (20%) del monto total adjudicado. Este pago se hará a más tardar a los diez (10) días de la firma del contrato y posterior a la entrega de la fianza de anticipo.

La suma restante será pagada de la siguiente manera:

- Un segundo pago equivalente a un cuarenta (40%) del monto total de la propuesta presentada luego de recibido los equipos.
- Un pago final equivalente al cuarenta por ciento (40%) del monto total de la propuesta presentada, el cual se hará posterior a la culminación de los servicios, mediante Certificación de Conformidad emitida por la Gerencia de Tecnología de la Jurisdicción Inmobiliaria, y luego de presentar el contratista los documentos que avalen el pago de los compromisos fiscales, liquidaciones y prestaciones laborales.

4.4 Presentación de Propuestas Técnicas y Económicas "Sobre A" y "Sobre B".

Las ofertas se presentarán en digital (PDF) y en físico.
Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus y debe permitir realizar búsqueda dentro del documento (OCR).
El formato físico debe estar en dos sobres (original y copia), cerrados y firmados, con las siguientes inscripciones:

SOBRE (dependiendo de qué propuesta se trate) A/B
NOMBRE DEL OFERENTE
(Sello social)
Firma del Representante Legal
Comité de Compras y Licitaciones
Consejo del Poder Judicial Dominicano
Referencia: LPN-CPJ-12-2017
Dirección: Av. Enrique Jiménez Moya, esq. Juan de Dios Ventura Simó, Centro de los Héroes, de Constanza, Maimón y Estero Hondo, Sto. Dgo., R.D.
Fax: 809-532-2906
Teléfono: 809-533-3191 Ext. 2052/2009/2079

Estos sobres contendrán en su interior el "Sobre A" (Propuesta Técnica) y el "Sobre B" (Propuesta Económica).

4.5 Forma para la presentación de los documentos contenidos en Sobre A y Sobre B

Los documentos contenidos, tanto en el Sobre A como en el Sobre B, deberán ser presentados en original debidamente marcados como "ORIGINAL" en la primera página del ejemplar, junto con una (1) fotocopia simple de los mismos, debidamente marcados en su primera página como "COPIA". Los documentos contenidos en el Sobre A como en el Sobre B, tanto el original como la copia, deberán contener en todas sus páginas la firma del Representante Legal, todas las páginas deben estar numeradas y llevar el sello social de la empresa o sociedad.

4.6 Documentaciones Necesarias a Presentar: Sobre A

I. Documentaciones legales:

La documentación legal debe presentarse encuadernada y con un índice en el siguiente orden:

a) Formulario de Presentación de la oferta. **(Usar el modelo denominado Anexo 2, que se encuentra al final del Pliego)**

b) Formulario de Información sobre el oferente.**(Usar el modelo denominado Anexo 3, que se encuentra al final del Pliego)**

c) Carta manifestando su interés de participar en esta Licitación Pública Nacional, debidamente firmada.

d) Copia de los estatutos sociales, última asamblea general ordinaria anual y lista de suscriptores, debidamente registrados por la Cámara de Comercio correspondiente.

e) Copia de la certificación actualizada del Registro Mercantil.

f)Poder debidamente notariado o Asamblea General registrada en la Cámara de Comercio correspondiente, designando al Representante Legal con sus generales y en calidad de qué puede asumir compromisos, firmar contratos, entregar y recibir, cheques y otorgar descargos.

g) Copia de la cédula de identidad y electoral del representante y de cada miembro de la Junta Directiva.

h) Copia certificación de no antecedentes penales del representante legal y de cada miembro de la junta Directiva de la Sociedad.

i) Copia actualizada del Registro Nacional de Proveedores del Estado emitido por la Dirección General de Contrataciones Públicas.

j) Declaración jurada debidamente notariada. **(Usar el modelo denominado Anexo 4, que se encuentra al final del Pliego)**

k) Copia de la certificación emitida por la Dirección General de Impuestos Internos (DGII), donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones fiscales.

l) Copia de la certificación emitida por la Tesorería de la Seguridad Social, donde se manifieste que el oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social.

m) Copia del último Estado Financiero de la empresa o persona física, firmado por un contador público autorizado.

II. Documentación Técnica:

n) Oferta Técnica:

- Presentar las fichas técnicas completas e individualizadas de los bienes ofertados por el licitante en razón de los lotes, descritos en el numeral 3.3 del presente Pliego de Condiciones, donde deseen participar, dentro de los cuales están requerimientos de contratación, de garantía y soporte y funcionales y técnicos.

o) Plan de implementación, debe contener la descripción de todas las políticas a implementar, un cronograma que describa todas las fases y alcance del proyecto.

p) Un mínimo de (3) certificaciones, emitidas por clientes del oferente que hayan adquirido los bienes y servicios tal como se listan en las especificaciones del pliego.

q) Certificación emitida por el Oferente estableciendo de manera individualizada y detallada las condiciones de garantía de cada tipo de producto o bien ofertado.

r) Certificación del o los fabricantes, de cada uno de los bienes ofertados, indicando que el oferente está autorizado a ofertar las soluciones propuestas. Esta certificación debe indicar que tipo de Partner es el oferente y desde que fecha está habilitado para vender dichos equipos.

s) Documentación, certificaciones de capacitaciones, que demuestren que su personal está altamente capacitado para ofrecer soporte y soluciones en los equipos y servicios a ofertar que se listan en las especificaciones del presente pliego. **anexar certificaciones de referencias**

t) Última versión publicada válida, del informe de Gardner de las Soluciones propuestas para Firewells y ADCs, de los cuales:
   - LOTE I, debe estar dentro del Informe de Gardner, ¨Magic Quadrant for Enterprise Network Firewalls", dentro del cuadrante de Retadores o Líderes (Challengers o Leaders).
   - LOTE II, deben estar dentro del Informe de Gardner, "Magic Quadrant for Application Delivery Controllers", dentro del cuadrante de Líderes (Leaders).

u) Certificación de fabricante y del oferente donde indique que cuentan con un inventario de todas las partes y piezas necesarias para dar soporte a todos los equipos después de su puesta en producción.

4.7 Documentaciones Necesarias a Presentar: Sobre B

La presente documentación debe presentarse encuadernada en el siguiente orden:

a. Formulario de Oferta Económica **(Usar el modelo denominado Anexo 1, que se encuentra al final del Pliego)**

b. Garantía de Mantenimiento de la Oferta favor del Consejo del Poder Judicial. La cual deberá ser equivalente al tres por ciento (3%) del monto total de la propuesta, impuestos incluidos y tener una vigencia de ciento veinte (120) días calendarios. Esta deberá ser presentada mediante póliza expedida por una compañía de seguros de reconocida solvencia en el país o mediante una garantía bancaria.

La no presentación de la Garantía de Mantenimiento de la Oferta o cuando ésta resulte insuficiente conllevará la descalificación automática de la oferta.

4.8 Costos de la Presentación de las Propuestas.

El licitante deberá asumir la totalidad de los costos, relacionados a la preparación y presentación de su propuesta. El Consejo del Poder Judicial, no reconocerá ninguna exigencia por concepto de gastos de elaboración de la misma.

4.9 Calidad de Presentación

Las propuestas presentadas deberán cumplir con los requisitos previamente establecidos en este documento.

4.10 Otras condiciones para la presentación de ofertas

a. Cada oferente tendrá que suplir toda información requerida. En caso de requerírseles, suplirán certificaciones, documentos especiales, muestras o demostraciones como parte de su oferta.

b. Toda corrección y/o borradura en la oferta tiene que estar inicialada y explicada por el licitador, incluyendo la fecha, de lo contrario quedará invalidada la oferta.

c. Los precios no deberán presentar alteraciones ni correcciones y deberán ser dados por la unidad de medida establecida en los listados.

d. Los oferentes son responsables de los errores presentados en las propuestas; el precio unitario cotizado prevalecerá para consideraciones en la adjudicación final. Todas las cantidades y cifras totales estarán impresas en números y letras, en caso de diferencia prevalecerá la indicada en letra.

e. Las ofertas serán recibidas por el Comité de Compras y Licitaciones, el día en que se realice la Licitación Pública Nacional, bajo acta notarial y en presencia de los participantes y el público asistente.

f. Las propuestas después de recibida por el Comité de Compras y Licitaciones, no podrán ser modificadas.

g. Las ofertas luego de ser sometidas no podrán ser retiradas, excepto cuando así se solicite al Comité de Compras y Licitaciones ante el público presente en la licitación.

h. Una vez retirada la oferta por el licitador, éste no podrá depositar una oferta sustituta.

i. El Contratista no podrá, bajo pretexto de error u omisión de su parte, reclamar aumento de los precios fijados en el contrato.

j. El Oferente que resulte favorecido con la adjudicación de la presente Licitación Pública Nacional, debe mantener durante todo el plazo de ejecución del contrato el precio que proponga en el momento de presentación de la Oferta.

k. El Oferente será responsable y pagará todos los impuestos que hubiesen sido fijados por autoridades municipales, estatales o gubernamentales, dentro y fuera de la República Dominicana, relacionados con los productos y servicios a ofrecer.

5. Apertura y Validación de Ofertas

5.1 Procedimiento de Apertura de Sobres

La apertura de sobres se realizará en presencia del Comité de Compras y Licitaciones, el Notario Público y los oferentes en la fecha, lugar y hora establecidos.

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

El Consejo del Poder Judicial no recibirá sobres que no estuviesen debidamente cerrados e identificados, según lo dispuesto anteriormente.

5.2 Apertura de Sobres

El Notario Público preparará un registro de los participantes según el orden de llegada de los oferentes.

Luego que el Presidente del Comité de Compras y Licitaciones da apertura a la licitación, de inmediato se procederá a la apertura de las ofertas presentadas según el orden de llegada, procediendo a verificar que la documentación contenida en la propuesta esté completa de conformidad con el listado especificado en el presente pliego de condiciones.

La revisión a detalle de los documentos contentivos de la propuesta técnica (SOBRE A) será realizada durante el proceso de evaluación de la propuesta; pudiendo el Comité, siempre que se trate de errores u omisiones de naturaleza subsanable, requerir en un plazo breve que no excederá de tres días hábiles, contados a partir del requerimiento, que el oferente rectifique la información y/o suministre la misma faltante;

Solo se procederá a la apertura de la oferta económica (SOBRE B) de aquellos oferentes que hayan quedado habilitados en el proceso de verificación de la documentación contenida en el (SOBRE A).

El Notario Público actuante levantará acta notarial de todas las incidencias de la licitación.

5.3 Validación, Verificación y Evaluación Técnica

Culminado el proceso de apertura de licitación, el Comité remite a los peritos correspondientes las propuestas presentadas, para su evaluación, quienes verificarán que las mismas cumplan con los requisitos técnicos requeridos en el pliego de condiciones.

El Comité de Compras y Licitaciones, si lo estima necesario y mientras dure el proceso de evaluación, podrá solicitar informes o requerimientos adicionales, probar equipos, exigir muestras, y cualquier otro requerimiento adicional a los oferentes, para el análisis de su propuesta, siempre que no afecte materialmente la oferta.

5.4 Exención de Obligación

El Comité de Compras y Licitaciones no estará obligado a declarar habilitado o adjudicatario a ningún oferente que haya presentado sus credenciales u ofertas, si las mismas no demuestran que cumplen con los requisitos establecidos en el presente Pliego de Condiciones.

5.5 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" con los estándares de calidad de la Institución:

5.5.1 Elegibilidad

a. Que el Proponente está legalmente autorizado para realizar sus actividades comerciales en el país.
b. Que el oferente demuestre que tiene la capacidad y la experiencia para la entrega en las condiciones establecidas.
c. Que el oferente cumpla con todos los requerimientos exigidos.

5.5.2 Capacidad Técnica

Que los bienes y servicios cumplan con las todos los requisitos y características establecidas en las especificaciones técnicas del presente pliego de condiciones.

5.5.3 Situación financiera

El oferente debe contar con la estabilidad financiera suficiente para ejecutar satisfactoriamente el eventual contrato. El Comité podrá evaluar la estabilidad financiera del oferente en base a la documentación presentada por el mismo en el SOBRE A, sin que esto impida que pueda requerir información adicional para tales fines.

5.5.4 Experiencia de la empresa

El Comité podrá evaluar la experiencia del oferente en base a la documentación presentada por éste en el SOBRE A, sin que esto impida que pueda requerir información adicional para tales fines.

5.6 Adjudicación

El Comité de Compras y Litaciones tomará en cuenta para la adjudicación al oferente cuya propuesta cumpla con los requisitos y sea calificada como la más conveniente para los intereses del

Poder Judicial, teniendo en cuenta el precio, la calidad, la idoneidad del oferente y demás condiciones que se establezcan en el pliego de condiciones.

Luego de recibir el informe de los peritos y hacer el análisis correspondiente, el Comité de Compras y Licitaciones levantará Acta de Adjudicación con la decisión adoptada.

El Comité podrá declarar adjudicatario a uno o varios oferentes, podrá adjudicar por lotes de artículos.

En caso de resultar adjudicatarios más de un oferente, ambos deberán trabajar en coordinación bajo la supervisión de la Gerencia de Tecnología de la Jurisdicción Inmobiliaria.

El Comité de Compras y Licitaciones procederá a informar a todos los participantes el resultado de la Licitación dentro de un plazo de cinco (5) días hábiles, contados a partir de la expedición del acta de decisión. La notificación de adjudicación podrá entregarse de manera física o vía correo electrónico.

5.7 Rechazos

Serán excluidas las ofertas que procuren la adjudicación por cualquier vía no prevista en este Pliego de Condiciones.

5.8 Impugnación de Adjudicación

Para la impugnación de la adjudicación se seguirá el procedimiento siguiente:

a) A pena de inadmisibilidad, la impugnación de la adjudicación de una licitación por los ofertantes participantes deberá someterse mediante escrito motivado, en hecho y en derecho, y depositado en el Comité de Compras y Licitaciones, dentro de los diez (10) días hábiles, a partir de la notificación de la adjudicación. El depósito del escrito contentivo de la Impugnación suspenderá la ejecución de la adjudicación, hasta que el Comité decida.
b) El Comité de Compras y Licitaciones y el impugnante notificarán la impugnación al beneficiario de la adjudicación y a los demás participantes, dentro de un plazo de dos (2) días hábiles, a partir de su depósito.
c) Los oferentes notificados tendrán un plazo de dos (2) días hábiles para emitir su opinión sobre la impugnación.
d) El Comité de Compras y Licitaciones conocerá de la impugnación dentro de los diez (10) días hábiles que siguieren al cumplimiento de las disposiciones que anteceden, y decidirá sobre ella dentro de los cinco (5) días que siguieren al vencimiento del plazo precedente.
e) El Comité de Compras y Licitaciones, después de vencido el plazo, dicta la resolución relativa a la impugnación y la notifica a los participantes.
f) La decisión que rechazare la impugnación no será recurrible, por lo que, a continuación, se ejecutará el procedimiento final de la licitación.
g) La decisión que acogiere la impugnación hará consignar los procedimientos que serán seguidos para la solución definitiva del proceso.
h) No será ponderada ninguna impugnación que incumpliere con el procedimiento previsto en esta disposición.

5.9 Adjudicaciones Posteriores

En caso de incumplimiento del oferente adjudicatario, así como por situaciones o errores detectados en este proceso, este pierde la adjudicación y el Comité de Compras y Licitaciones procederá a revisar la siguiente mejor oferta y así sucesivamente, y decidirá el respecto.

5.10 Declaración de Desierto

El Comité de Compras y Licitaciones 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 institucionales todas las ofertas o la única presentada.
- Por violación sustancial del procedimiento de Licitación Pública Nacional.

Si el proceso es declarado desierto, el Comité de Compras y Licitaciones podrá reabrirlo dando un plazo para la presentación de propuestas de hasta un cincuenta por ciento (50%) del plazo del proceso fallido.

5.11 Cancelación de Licitación Pública Nacional

El Comité de Compras y Licitaciones se reserva al derecho de cancelar de manera justificada a cualquier oferente o la Licitación Pública Nacional, ya sea antes o después de la apertura, no incurriendo en ningún compromiso o responsabilidad al respecto.

5.12 Garantía de Fiel Cumplimiento de Contrato.

El Adjudicatario deberá constituir una garantía Bancaria o Póliza de compañía aseguradora de reconocida solvencia en la República Dominicana, en un 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 del Consejo del Poder Judicial. Esta garantía será devuelta una vez que el Adjudicatario cumpla con sus obligaciones a satisfacción del Consejo del Poder Judicial, y no quede pendiente la aplicación de multa o penalidad alguna.

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 con la ejecución de la Garantía de Mantenimiento de Oferta.

Si el Oferente Adjudicatario incumple con el plazo precitado pierde la adjudicación y el Comité de Compras y Licitaciones procederá a la adjudicación a quien haya quedado en el segundo lugar, conforme al reporte de lugares ocupados y al procedimiento de re-adjudicación posterior.

5.13 Fianza de Avance

Esta fianza la debe presentar el oferente al cual se le adjudique el proyecto al momento de recibir la orden de compra o la firma del contrato, equivalente al monto total del avance entregado. Dicha fianza será condición indispensable para la entrega del avance.

6. El Contrato

El adjudicatario y el Consejo del Poder Judicial no contraen obligación alguna hasta tanto sea firmado el contrato correspondiente.

Posterior a la entrega de la garantía de fiel cumplimiento, se redactará el contrato conforme con todas las normas y procedimientos de contrataciones vigentes. Deberá ajustarse a lo establecido en este Pliego de Condiciones.

6.1 Vigencia del Contrato

La vigencia del Contrato será a partir de la fecha de la suscripción del mismo, hasta su fiel cumplimiento o cuando una de las partes decida rescindirlo, de conformidad con lo establecido en este Pliego de Condiciones y en el mismo.

6.2 Subcontratos

En ningún caso el contratista 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 El Consejo del Poder Judicial.

6.3 Incumplimiento del contrato

Se considerará incumplimiento del contrato, siendo enunciativas y no limitativas:

- La mora del proveedor en la entrega de los bienes.
- La falta de calidad de los bienes suministrados.
- El suministro de menos unidades de las solicitadas.
- Si no se cumplen con las condiciones establecidas en el pliego de condiciones.
- Que incumpla con cualquiera de las cláusulas contratadas.

6.4 Efectos del Incumplimiento

El incumplimiento del Contrato por parte del proveedor determinará su finalización y supondrá para el mismo la ejecución de la Garantía 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, el Consejo del Poder Judicial podrá determinar su inhabilitación temporal o definitiva, dependiendo de la gravedad de la falta, así como realizar cualquier reclamo ante los tribunales correspondientes.

6.5 Finalización del Contrato

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

- Incumplimiento del contratista.
- Incursión sobrevenida del proveedor en alguna de las causas de prohibición de contratar que establezcan las normas vigentes.

6.6 Tipos de Incumplimientos

A los efectos de este Pliego de Condiciones, los incumplimientos se clasifican en leves, graves y muy graves, conforme se indica a continuación:

a) Incumplimientos leves

Se considerará falta leve, y el proveedor podrá ser inhabilitado por un período de un (1) año, cuando incurra en alguna de las siguientes faltas:

- Presentar recurso de revisión o impugnación fundamentado en hechos falsos, con el solo objetivo de perjudicar a un determinado adjudicatario;
- Incumplir sus obligaciones contractuales derivadas de una adjudicación por licitación;
- Renunciar, sin causa justificada, a la adjudicación de un contrato;
- Cometer, por comisión o por omisión, cualquier otro hecho de la misma gravedad o consecuencias.

b) Incumplimientos graves

Se considerará falta grave, y el proveedor podrá ser inhabilitado por un período de dos (2) a tres (3) años, cuando incurriera por segunda vez en una cualquiera de las causas previstas en el párrafo precedente.

c) Incumplimientos muy graves

Se considerará falta muy grave, y el proveedor podrá ser inhabilitado por un período de cuatro (4) a cinco (5) años, cuando incurra por tercera vez en las mismas faltas.

Sin perjuicio de las demás sanciones que correspondieren, el Comité de Compras y Licitaciones inhabilitará de forma permanente los proveedores inscritos en el Registro de Proveedores, por la comisión de las acciones siguientes:

- Cambiar, sin notificación y aceptación de la Institución, la composición, calidad, marca y especialización del personal que se comprometieron a asignar a la obra, servicios o bien;
- Presentar documentación falsa o alterada, o utilizar procedimientos coercitivos o de chantaje;
- Incurrir en acto de colusión, debidamente comprobado, en la presentación de su oferta;
- Ofrecer dádivas, comisiones o regalías a servidores judiciales vinculados al procedimiento de compras o licitación y relacionados, o utilizar personal de la Institución para elaborar sus propuestas;
- Obtener la precalificación o calificación, mediante el ofrecimiento de ventajas de cualquier tipo;
- Contratar con dispensa del procedimiento de licitación previsto por este Reglamento, en complicidad con servidores administrativos judiciales;
- Obtener informaciones que les coloquen en una situación de ventaja respecto de otros competidores, en violación a los trámites establecidos por el Comité de Compras y Licitaciones;
- Participar directa o indirectamente en un proceso de contratación, pese a encontrarse dentro del régimen de prohibiciones.

6.7 Sanciones

En caso de retraso en el cumplimiento de la entrega, El Consejo del Poder Judicial, podrá exigir que el contratista page el 1% del total del contrato por cada día hábil de retraso hasta un máximo de treinta (30) días, a partir de la notificación del mismo; si llegados los treinta (30) días el contratista aún no cumple con la entrega, se ejecutará la fianza de fiel cumplimiento y se rescindirá el contrato.

La ocurrencia de los incumplimientos leves y graves detallados, hace pasible al Contratista de la aplicación de las sanciones previstas en el Reglamento de Compras de Bienes y Contrataciones de Obras y Servicios del Consejo del Poder Judicial.

En caso de infracciones graves el Consejo del Poder Judicial podrá rescindir el contrato, sin perjuicio de las demás acciones que la Ley pone a su alcance en reparación del perjuicio causado.

6.8 Retraso en la Entrega

Se entiende que ha habido un retraso en la entrega cuando el contratista no cumpla con la fecha convenida en el contrato.

Párrafo I: El cumplimiento al tiempo de entrega tendrá las siguientes excepciones:

- Por causa justificada sometida al Comité de Compras y Licitaciones dentro de tres (3) días antes de la fecha límite de entrega.

- Por causa de fuerza mayor o caso fortuito. Un evento de fuerza mayor se define como un hecho que no ha podido ser previsto ni impedido, lo cual libera a una parte por su imposibilidad de cumplir su obligación frente a la otra; tales como, sin que dicha enumeración resulte limitativa: huelga, guerra, bloqueo, huracán, fuego, terremoto e inundaciones.[1]

6.9 Penalidades Aplicadas por Incumplimiento en la entrega

Las penalidades por incumplimiento del contrato por parte de la Empresa o persona física a quién se le adjudique la licitación, son las siguientes:

- Eliminar de las listas del Banco de Proveedores del Poder Judicial, el nombre de cualquier firma que no cumpliere un contrato, o que en otra forma incurriere en defecto.

- Demandar en daños y perjuicios ante los tribunales nacionales.

7. Generalidades

Los casos no contemplados quedarán sujetos a decisiones del Comité de Compras y Licitaciones, quien es la autoridad máxima dentro de esta Licitación Pública Nacional.

[1] Ocurrida la causa de fuerza mayor, se debe notificar la naturaleza y el evento de fuerza mayor que se invoca.

8. Formulario de Cumplimiento

Req. No.	Cumplimiento		Observaciones
	Cumple	No Cumple	
Requerimientos de Contratación (RDC).			
Acreditaciones y Experiencia del Oferente: _____			
Formulario de Presentación de Oferta (Anexo 2)			
Formulario de Información sobre Oferente (Anexo 3)			
Carta de interés en participar de la Licitación			
Copia de los estatutos sociales, última asamblea general ordinaria anual y lista de suscriptores, debidamente registrados por la Cámara de Comercio correspondiente.			
Copia actualizada Registro Mercantil			
Poder notariado o Asamblea General registrada en Cámara de Comercio designando al representante legal.			
Copia de la Cédula de Identidad del Representante legal y miembros de la Junta Directiva			
Copia certificación de No Antecedentes Penales representante legal y miembros de la Junta Directiva			
Declaración Jurada Notariada (Anexo 4)			
Copia actualizada Registro Nacional de Proveedores del Estado			
Copia certificación de la DGII donde se manifieste que el Oferente se encuentra al día en el pago de sus obligaciones fiscales.			
Certificación emitida por el Oferente estableciendo de manera individualizada y detallada las condiciones de garantía de cada tipo de producto o bien ofertado.			
Copia certificación TSS donde se manifieste que el oferente se encuentra al día en el pago de sus obligaciones de la Seguridad Social.			
Referencias comerciales.			
Formulario Oferta Económica (Anexo 1)			Valor:
Copia último Estado Financiero de la empresa o persona física, firmado por un contador público autorizado.			

Req. No.	Cumplimiento		Observaciones
	Cumple	No Cumple	
Oferta Técnica			
Presentar las fichas técnicas completas e individualizadas de los bienes ofertados por el licitante en razón de los lotes, descritos en el numeral 3.3 del presente Pliego de Condiciones, donde deseen participar, dentro de los cuales están requerimientos de contratación, de garantía y soporte y funcionales y técnicos.			Valor:
Un mínimo de (3) certificaciones, emitidas por clientes del oferente que hayan adquirido los bienes y servicios tal como se listan en las especificaciones del pliego.			
Plan de implementación, debe contener la descripción de todas las políticas a implementar, un cronograma que describa todas las fases y alcance del proyecto.			
Certificación emitida por el Oferente estableciendo de manera individualizada y detallada las condiciones de garantía de cada tipo de producto o bien ofertado.			
Certificación del o los fabricantes, de cada uno de los bienes ofertados, indicando que el oferente está autorizado a ofertar las soluciones propuestas. Esta certificación debe indicar que tipo de Partner es el oferente y desde que fecha está habilitado para vender dichos equipos.			
Documentación, certificaciones de capacitaciones, que demuestren que su personal está altamente capacitado para ofrecer soporte y soluciones en los equipos y servicios a ofertar que se listan en las especificaciones del presente pliego. **anexar certificaciones de referencias**			
Última versión publicada válida, del informe de Gardner de las Soluciones propuestas para Firewells y ADCs, de los cuales: • LOTE I, debe estar dentro del Informe de Gardner, ¨Magic Quadrant for Enterprise Network Firewalls", dentro del cuadrante de Retadores o Líderes (Challengers o Leaders). • LOTE II, deben estar dentro del Informe de Gardner, "Magic Quadrant for Application Delivery Controllers", dentro del cuadrante de			

Req. No.	Cumplimiento		Observaciones
	Cumple	No Cumple	
Líderes (Leaders).			
Certificación de fabricante y del oferente donde indique que cuentan con un inventario de todas las partes y piezas necesarias para dar soporte a todos los equipos después de su puesta en producción.			
Garantía de Mantenimiento de Oferta			

Esta sección se presenta para ayudar a los oferentes a constatar que presentan toda la documentación requerida.

9. Anexos: Ver páginas siguientes.

Formulario de Presentación de Propuestas

En esta sección se presenta el formulario de presentación de las propuestas

Lote No.1: Equipos Firewalls.

a) Requerimientos de Contratación, Garantía y Soporte

Req. Núm. Requerimientos de Contratación (RDC).	Descripción	Solución Propuesta	Número de Partes
Acreditaciones y Experiencia del Oferente.			
RDC01	El Oferente debe contar con una experiencia mínima de tres (3) años y con tres (3) o más clientes, fuera o dentro del territorio dominicano, donde haya ejecutado proyectos de implementación de soluciones de Firewalls de manera satisfactoria y cualquier otro equipo que esté contemplado en la propuesta de implementación. Para esto el Oferente presentará una carta de recomendación por cada uno de los tres (3) o más clientes referenciados, tal como se lista en las especificaciones del Pliego.		
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de Firewalls y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Para tal efecto, el Oferente presentará una Carta de Certificación del Fabricante, de que puede vender, dar soporte a los equipos y soluciones de este Fabricante en la República Dominicana.		
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones Firewalls y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.		
RDC04	Las Soluciones propuestas de Firewalls deben estar dentro del Informe de Gardner, "Magic Quadrant for Enterprise Network Firewalls", dentro del cuadrante de Retadores o Líderes (Challengers o Leaders). Dicho informe de referencia deberá ser actualizado, es decir, debe ser la última publicación valida. Este documento debe ser anexado a la Propuesta.		
RDC05	La instalación y migración de los servicios, equipos, configuraciones y demás debe ser contemplada como parte de la propuesta; incluyendo la puesta en funcionamiento de las políticas de seguridad y monitoreo descritos en los requerimientos técnicos y funcionales. El cableado, Switches y demás componentes necesarios para la puesta en instalación y puesta en funcionamiento de las soluciones deben formar parte de la propuesta.		
RDC06	Deben dejar en correcto funcionamiento todo lo relacionado a la infraestructura propuesta. La implementación de los equipos y aplicativos citados en este pliego no debe afectar las operaciones diarias de la JI, por lo que el oferente debe tomar las medidas necesarias para este requerimiento.		
RDC07	Si el Oferente sub-contrata o integrara todos o parte de los servicios a ofrecer deberá presentar un acuerdo entre las partes donde indique su intención de trabajar en colaboración (Joint-Venture) en el proyecto de implementación de las soluciones. El Sub-contratado deberá contar con la anuencia de la Jurisdicción Inmobiliaria – Poder Judicial, siendo siempre el responsable ante la Institución el contratista (adjudicatario).		
RDC08	Las Marcas de los equipos ofertados (Firewalls) para la "Red Perimetral Externa" deben ser diferente a los ofertados para la "Red Perimetral Interna"		
Tiempos de Entrega y de Implementación.			
RDC09	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de Firewalls en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.		
RDC10	La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.		
RDC11	El oferente elaborará un documento informando los productos entregados e instalados; y validando los requerimientos técnicos que han sido cumplidos; así como los riesgos que han sido mitigados. Nota: Este documento debe contener la descripción de todas las políticas implementadas.		
Normas de Seguridad Industrial.			
RDC12	El Oferente presentará como parte de su propuesta los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.		

Responsabilidades del Oferente.			
RDC13	La presentación de las Propuestas debe cumplir con los siguientes requisitos: • Deben describir claramente la Marca y el Modelo ofertado. • Deben describir los detalles técnicos de todos los equipos presentados. • Las propuestas deberán ser presentadas en idioma español. • La propuesta presentada deberá describir (el **#** de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento. • Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte. • La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF) • El formato digital debe permitir realizar búsqueda dentro del documento (OCR). • Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.		
RDC14	El Oferente revisará y leerá detenidamente el contenido de este documento, y hará las preguntas necesarias conforme al protocolo descrito en estos términos de referencia.		
Requerimientos de Garantía y Soporte (RGS).			
Garantías y Soporte.			
RGS01	Las Soluciones propuestas de Firewallsy cualquier otro equipo (Ejemplo: Switches, Tokens, Licencias de Equipos, Software, entre otros) que esté contemplado en la propuesta de implementación contarán con una garantía en Piezas y Servicios (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo).**Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.		
RGS02	El Software de Administración de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo).**Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.		
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación, comenzará a aplicarse a partir de la instalación y puesta en funcionamiento de las mismas. Nota: Para fines de Inicio del Periodo de Garantía, la Puesta en Funcionamiento del Equipo estará aprobada a partir del Documento de Aceptación, el cual será firmado por la JI y el Oferente.		
RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación deberá ser posterior al tercer (3er.) año de garantía, tomando como referencia la fecha de esta licitación (Entrega/Apertura de Ofertas). Por lo que se solicita para validar este requerimiento que se presente la constancia escrita del fabricante de la Solución de Firewalls. La propuesta debe incluir equipos de última generación del fabricante.		
RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año. Ejemplo: Si el costo del soporte y de Licenciamiento cuando se adquirió el equipo fue de 100 Pesos, este no podrá costar más 115 Pesos, es decir, no podrá ser mayor a un 15%.		
RGS06	El Fabricante y el Oferente de las Soluciones propuestas de Firewalls y cualquier otro equipo que esté contemplado en la propuesta de implementación deben presentar garantías (documentaciones) de que mantienen en la República Dominicana el inventario de todas partes y piezas necesarias para dar soporte a dicho equipo después de su puesta en producción.		
Requerimientos de Capacitación.			
RGS07	Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes: ➢ Instalación, Configuración y Administración de los firewalls a instalar en la		

	red perimetral y la red LAN.). Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos: • Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos. • Las capacitaciones serán realizadas de forma Presencial. • El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. • Estas capacitaciones deberán ser impartidas en idioma español. • Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes. • Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente. • El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI. • El oferente cubrirá con todos los costos de la capacitación. • Estas capacitaciones deben impartirse previo a la implementación de los equipos, para que la JI pueda definir las mejores prácticas a ponerse en ejecución durante el proceso de implementación de dichos equipos. Los instructores deberá ser docentes calificados y certificados por el/los fabricante /s de las soluciones a instalar. La empresa suplidora deberá correr con los gastos de alojamiento, viáticos y pasaje aéreo del personal docente, si se necesitaré participación de los instructores Extranjeros.		

b) Requerimientos Técnicos para dos (2) Firewalls de la Red Perimetral Externa.

Req. Núm. Requerimientos Funcionales y Técnicos (RFT).	Descripción	Solución Propuesta	Número de Partes
RFT01	**Dos (2) Firewalls** de última generación (ambos instalados en la parte externa de la red perimetral de la JI) e instalados en modo HA. Estos equipos deberán ser de una Marca diferente a los que se instalen "Red Perimetral Interna". El propósito de estos firewall serán los de responder preventivamente antes a las amenazas externas de la red (outside), concentrar las conexiones VPN y delimitar el acceso a los servicios externos en la DMZ.		
RFT02	Los firewalls deben conectarse a 2 Switches Ethernet en modo Stack en el perímetro externo para soportar la infraestructura de los equipos que están en la DMZ. Características: • 1RU • 24 Puertos 1 Gigabit Ethernet. (Con sus Licencias y Transceiver incluidos) • 2 Puertos SFP+ a 10 Gigabit (Con sus Licencias y Transceiver incluidos) • Tecnología StackWise con 480 GB de throughput. • PowerSupply Redundante. • Tecnología StackPower. • Licencia IP Based. • Debe soportar IPv4, IPv6 routing, multicastrouting, modular quality of service (QoS), Flexible NetFlow (FNF) y característica de seguridad mejorada (enhancedsecurityfeatures). Estos equipos (Switches) deberá contar con características avanzadas de Quality of Service (QoS) y cumplir con todos los requerimientos de contratación y garantía citados en el pliego.		
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir un SO desarrollado por el fabricante específicamente para propósitos de Firewall.		
RFT04	La solución propuesta debe ser un equipo dedicado solo para estos fines.		
RFT05	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.		
RFT06	Debe cumplir con las siguientes especificaciones: • 35 Gbps de Stateful inspection firewall throughput. • 15 Gbps de Stateful inspection firewall throughput (multiprotocol). • 12 Gbps de throughput de NGWF (Firewall and Aplication Visibility and Control). • 10 Gbps de throughput de NGIPS. (IPS and Aplication Visibility and Control). • Multiples interface 10g. • High Availability Configurations and clustering. • Redundant Power Supplies. • Secure Boot. • Trust Anchor module.		

	• Image signing.		
RFT07	Debe tener capacidad de balanceo de interfaces WAN. Nota: Si el Firewall no realiza de manera nativa esta función, el oferente podrá incluir un equipo adicional al Firewalls de propósito específico para cumplir con esta capacidad.		
RFT08	Debe tener las siguientes capacidades de prevención ataques DDoS: • Maximum mitigation capacity/throughput de 10 Gbps. • Maximum legitímate concurrent sessions de 209,000 Conexiones por Segundo (CPS) • Maximum DDoS flood attack prevention rate de 1,800,000 Paquetes por segundo (PPS).		
RFT09	El equipo debe tener al menos 8 Gbps de Throughput de VPN IPSec.		
RFT10	Debe tener capacidad de al menos 10 millones de sesiones simultáneas.		
RFT11	Debe tener capacidad de al menos 150,000.00 nuevas sesiones por segundo.		
RFT12	El equipo debe tener al menos 10,000.00 Túneles (IPsec Client / site-to-site VPN peers)		
RFT13	La solución ofertada debe incluir al menos 8 puertos de 10 Gbps. SFP+		
RFT14	Debe incluir al menos 10 FIREWALL virtuales.		
RFT15	Debe incluir al menos 40 zonas de seguridad distintas.		
RFT16	Debe soportar al menos 350 políticas.		
RFT17	Estos equipos deben abarcar todas las rutas críticas de los servicios que tenemos instalados en nuestra zona perimetral.		
RFT18	La solución propuesta debe ser de tipo Next Gen IPS / Next Gen Firewall con capacidad avanzada contra amenazas. Ejemplo de amenazas: Malware, Ataques día Cero, Denegación de Servicios, entre otros.		
RFT19	El equipo debe poder ser configurado en modo Gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá hacer modificaciones en la red en cuanto a enrutamiento o direccionamiento IP.		
RFT20	Debe tener Funcionalidades de: • NGIPS • NGFW • VPN – IPSec • DDoS • Anti-Malware		
RFT21	Debe poder hacer integración con soluciones de LDAP y tener integrado Sandboxings.		
RFT22	Debe tener capacidad para asignar parámetros de traffic shapping sobre reglas de firewall.		
RFT23	Debe soportar la creación de políticas de tipo Firewall , VPN, subtipo por dirección IP, tipos de dispositivo y por usuario.		
RFT24	Debe poder configurar la autenticación por usuario.		
RFT25	Debe ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.(Discriminación de Certificado en Base a Trafico).		
RFT26	Debe hacer escaneo de tráfico a profundidad dentro de todos o cierto rango de puertos configurados para este análisis.		
RFT27	Debe analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.		
RFT28	Debe permitir la creación de políticas de tipo VPN (IPSEC/SSL).		
RFT29	• Deberá soportar Clúster Firewalls con su sistema de análisis de red y management centralizado (Esta solución debe incluir el Sistema de Gestión y Análisis Centralizado para este Clúster) • El Clúster Firewalls deberá proveer al menos 8 interfaces 10Gbps. SFP+ (Con sus Licencias y Transceiver incluidos) • El Clúster Firewalls deberá proveer la creación de reglas de IPS. • Cluster de firewalls deberá proveer creación de VPN Site-To-Site en las versiones (IKEv1 y IKEv2). • Clúster de firewalls deberá proveer análisis de malware con los siguientes protocolos: Spero Analysis for MSEXE, Dynamic Analysis, Capacity Handling. • Para la configuración de cluster, en caso de caída de uno de los dispositivos, la VPN que estuviera establecida, debe restablecerse en el otro dispositivo sin solicitar autentificación nuevamente.		
RFT30	Debe ser capaz de analizar, establecer control de acceso, detener ataques y hacer Antivirus en tiempo real en al menos en los siguientes protocolos aplicativos: HTTP,		

	SMTP, IMAP, POP3, FTP.		
RFT31	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP debe estar completamente integrada a la administración del dispositivo.		
RFT32	El Antivirus debe incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.		
RFT33	El antivirus debe poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).		
RFT34	Debe tener capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).		
RFT35	El detector y preventor de intrusos debe soportar y captar ataques por variaciones de protocolo, por firmas de ataques conocidos (signature based / misuse detection), reconocimiento de comportamiento de red y ataques día cero.		
RFT36	Debe soportar actualización automática de firmas para el detector de intrusos.		
RFT37	El Detector de Intrusos debe mitigar los efectos de los ataques de negación de servicios.		
RFT38	Debe contar con funcionalidades de Sandboxing para que los archivos bloqueados sean ejecutados en un ambiente seguro para analizar su comportamiento.		
RFT39	Debe poder realizar protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats).		
RFT40	El Detector y Preventor de intrusos debe poder implementarse tanto en línea como fuera de línea.		
RFT41	Debe tener capacidad de detección de más de 4000 ataques.		
RFT42	Debe tener capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "Pull" (Consultar los centros de actualización por versiones nuevas).		
RFT43	Debe guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos.		
RFT44	Debe tener la capacidad de cuarentena, es decir, prohibir el tráfico subsiguiente a la detección de un posible ataque.		
RFT45	La alta disponibilidad debe ser transparente, sin pérdida de conexiones en caso de que un nodo falle.		
RFT46	Debe tener posibilidad de definir al menos dos interfaces para sincronía y poder gestionar cada equipo de manera independiente.		
RFT47	Debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		
RFT48	La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
RFT49	El listado de aplicaciones debe actualizarse periódicamente.		
RFT50	Debe soportar inspección de Contenido SSL.		
RFT51	La solución debe tener la capacidad de inspeccionar tráfico que esté siendo encriptado al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.		
RFT52	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.		
RFT53	El equipo debe ser capaz de analizar contenido cifrado.		
RFT54	La solución ofertada debe permitir la administración vía web, cli, syslog, snmp2. Administración basada en roles y debe ser centralizada para todos los firewalls propuestos.		
RFT55	Debe permitir almacenamiento de eventos de manera interna y/o en un repositorio que pueda consultarse luego con SQL.		
RFT56	Debe contar con Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.		
RFT57	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox, Chrome) instalado sin necesidad de instalación de ningún software adicional.		
RFT58	Debe poder virtualizar los servicios de seguridad.		
RFT59	Se debe incluir la licencia para al menos 10 (Diez) instancias virtuales dentro de la solución a proveer.		
RFT60	Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual.		
RFT61	Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el trafico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones deben poder realizarse incluso entre instancias virtuales.		
RFT62	Debe de ser capaz de realizar análisis continuo y retrospección de archivo o detección.		
RFT63	Debe ser posible obtener una visualización completa del alcance de una amenaza o ataque ya exitoso, como también contener, bloquear o poner en cuarentena.		
RFT64	La solución ofertada debe de ser capaz de hacer recomendaciones de políticas o modificaciones de firewall o NGIPS.		
RFT65	Debe de mostrar un perfil completo de los usuarios o direcciones IP internas, como		

	sistema operativos, vulnerabilidades, protocolos, etc.		
	OTROS REQUERIMIENTOS		
RFT66	Todos los equipos de este Lote I serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos (2) UPS independientes para alta disponibilidad.		
RFT67	Las Soluciones propuestas de **Firewalls** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad)		

c) Requerimientos Técnicos para 2 Firewalls de la Red Perimetral Interna.

Req. Núm.			
Requerimientos Funcionales y Técnicos (RFT).	**Descripción**	**Solución Propuesta**	**Número de Partes**
RFT01	2 Firewalls de última generación (ambos instalados en la parte interna de la red perimetral de la JI, en la parte frontal de nuestra red LAN) e instalados en modo HA. Estos equipos deberán ser de una Marca diferente a los que se instalen en la "Red Perimetral Externa". El propósito de estos firewalls serán los de detectar y bloquear amenazas desde y hacia el centro de la red (Red Interna). Estos firewall tendrán la característica de Proxy Server para defender y controlar las actividades de los usuarios.		
RFT02	Estos Firewalls estarán conectados a los Switches anteriormente citados en el RFT02 de la "Red Perimetral Externa".		
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un SO desarrollado por el fabricante específicamente para propósitos de Firewall.		
RFT04	La solución propuesta debe ser un equipo dedicado solo para estos fines.		
RFT05	Los equipos deben tener capacidad para crecer y escalar a una arquitectura de seguridad integral en el perímetro externo.		
RFT06	Debe cumplir con las siguientes especificaciones: • 80 Gbps de Throughput de Firewall (IPV4/IPV6). • 13 Gbps de Throughhput de IPS. • 5 Gbps de Threat Protection Throughput (Protección contra amenazas). • 7 Gbps de Throughput de NGWF. • Múltiple interface 10Gb. SFP+. • High Availability Configurations and clustering. • Redundant Power Supplies.		
RFT07	Debe tener Funcionalidades de: • Laboratorio de Investigación. • URL – Filtering. • Application Control. • IPS. • Antivirus.		
RFT08	Debe poder hacer integración con soluciones de LDAP y Sandboxings.		
RFT09	Debe tener capacidad de balanceo de interfaces WAN.		
RFT10	Debe tener capacidad de prevención contra ataques DDoS de 2 Gbps.		
RFT11	Debe tener capacidad (Throughput) de al menos 49 Gbps de VPN IPSec		
RFT12	Debe tener capacidad de al menos 11 Millones de sesiones simultáneas.		
RFT13	Debe tener capacidad de al menos 280,000.00 nuevas sesiones por segundo.		
RFT14	El equipo debe soportar al menos 20,000.00 túneles VPN IPSec / túnel.		
RFT15	• 16 Interfaces Ethernet 10/100/1000 (Con sus Licencias y Transceiver incluidos). • 8 Interfaces 10GB SFP+ (Con sus Licencias y Transceiver incluidos).		
RFT16	Debe tener capacidad de al menos 10,000.00 usuarios SSL VPN.		
RFT17	Debe tener capacidad de al menos 10 enrutadores virtuales.		
RFT18	Debe tener capacidad de al menos 40 zonas de seguridad distintas.		
RFT19	Debe tener capacidad de al menos 350 políticas.		
RFT20	Estos equipos deben abarcar todas las rutas críticas de los servicios que tenemos instalados entre nuestra zona perimetral y la red LAN.		
RFT21	La solución propuesta debe ser de tipo Next Gen Firewall.		
RFT22	El equipo debe poder ser configurado en modo gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.		
RFT23	Debe tener capacidad para asignar parámetros de traffic shapping sobre reglas de firewall.		
RFT24	Debe tener capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente.		
RFT25	Debe soportar la creación de políticas de tipo Firewall y VPN y subtipo por dirección IP, tipos de		

	dispositivo y por usuario.		
RFT26	Debe poder habilitar funcionalidades de (Antivirus, Filtrado Web, Control de Aplicaciones, IPS, Filtrado de correo, DLP, ICAP y VoIP) dentro de las políticas creadas.		
RFT27	Deberá contar con soporte para los siguientes servicios: • Soporte de al menos 128 redes virtuales vlans 802.1q, • Traducción de direcciones de red (nat) por fuente y destino, por direcciones ip dinámicas y pool de puertos. • Bgp, ospf y rip2, dhcp server y dhcp relay. • Protocolos de encriptación ike, 3des (con encriptación a 128, 192 y 256 bits), aes, sha1 y md5. • Soporte de pppoe. • Capacidad de firewall con identificación de aplicaciones de al menos 1 Gbps. • Identificación, control (uso de aplicaciones por usuario mediante interacción con ldap, directorio activo o radius y dirección ip)y visibilidad de aplicaciones incluyendo peer-to-peer, redes sociales, mensajería instantánea y web 2.0. • Identificación, control (uso de aplicaciones por usuario mediante interacción con ldap, directorio activo o radius y dirección ip)y visibilidad de aplicaciones incluyendo peer-to-peer, redes sociales, mensajería instantánea y web 2.0.		
RFT28	Debe poder configurar la autenticación por usuario.		
RFT29	El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en volumen de tráfico consumido.		
RFT30	Debe ejecutar inspección de trafico SSL en todos los puertos y seleccionar bajo que certificado será válido este tráfico.		
RFT31	Debe hacer escaneo de tráfico a profundidad dentro de todos o cierto rango de puertos configurados para este análisis.		
RFT32	Debe analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.		
RFT33	Debe permitir la creación de políticas de tipo VPN con capacidad de seleccionar campos como IPSEC o SSL según sea el tipo de VPN.		
RFT34	El filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.		
RFT35	El filtro URL debe ser configurable directamente desde la interfaz de administración del equipo.		
RFT36	Debe tener capacidad de filtrado de scripts en páginas web.		
RFT37	El filtrado de contenido debe estar basado en categorías en tiempo real, integrado a la plataforma de seguridad del equipo, sin necesidad de instalar un servidor de aplicaciones adicionales.		
RFT38	Debe poder definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.		
RFT39	Debe tener capacidad para realizar SSL VPNs.		
RFT40	Debe poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.		
RFT41	RFT66 Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.		
RFT42	La solución propuesta deberá permitir la creación de un clúster de hasta 23 unidades, tener un puerto dedicado para un failover rápido entre dos unidades de menos de un segundo, soporte de configuración activo-activo / activo-pasivo, todas las direcciones IP virtuales de las aplicaciones deberán ser soportadas por un clúster virtual, la configuración se deberá sincronizar entre las unidades pertenecientes al clúster. Failover automático cuando los servicios reales se encuentren abajo en alguna unidad, el tiempo de failover deberá ser programable.		
RFT43	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.		
RFT44	La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP debe estar completamente integrada a la administración del dispositivo.		
RFT45	El Antivirus debe incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.		
RFT46	El antivirus debe poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).		
RFT47	Debe tener capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).		
RFT48	El detector y preventor de intrusos debe soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / misuse detection).		
RFT49	Debe soportar actualización automática de firmas para el detector de intrusos.		
RFT50	Debe soportar modo sniffer, para inspección vía un puerto espejo del tráfico de datos de la red.		
RFT51	Debe soportar modo capa-2 (l2), para inspección de datos en línea y tener visibilidad y control del tráfico.		
RFT52	Debe soportar modo capa-3 (l3), para inspección de datos en línea y tener visibilidad y control del tráfico. Generar ruteo virtual para al menos 10 ruteadores virtuales, manejo de tráfico entre diferentes zonas de seguridad, sub-redes, soportando al menos 40 zonas de seguridad.		
RFT53	Debe soportar modo de trabajo mezclado sniffer, l2 y l3 en diferentes interfaces físicas.		

RFT54	Debe poder realizar protección contra amenazas avanzadas y persistentes (Advanced Persistent Threats).		
RFT55	El Detector y preventor de intrusos debe poder implementarse tanto en línea como fuera de línea.		
RFT56	Debe tener capacidad de detección de más de 4000 ataques.		
RFT57	Debe tener capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).		
RFT58	Debe guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos.		
RFT59	Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque.		
RFT60	Debe poder definir el tiempo en que se bloqueará el tráfico.		
RFT61	Debe soportar control de tráfico ipv4 e ipv6.		
RFT62	Debe permitir observar en una consola las principales aplicaciones y amenazas en proceso.		
RFT63	La consola debe permitir la visualización detallada de los usuarios y sistemas más activos en la misma.		
RFT64	Deben poder establecerse filtros dinámicos por tipos de aplicaciones, usuarios y equipos que muestren el uso y comportamiento del tráfico.		
RFT65	Debe permitir la captura automática de paquetes cuando se detecta una amenaza. Esto debe poder ser activado y desactivado por política / perfil.		
RFT66	Debe permitir la administración del ancho de banda mediante políticas, que se apliquen a nivel de aplicación o de usuario.		
RFT67	Debe permitir definir clases de tráfico con parámetros de uso de ancho de banda y prioridad.		
RFT68	Debe permitir el monitoreo del uso del ancho de banda por las aplicaciones a nivel de cantidad de bytes, sesiones y por usuario.		
RFT69	Debe permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles ssl.		
RFT70	Debe contar con software cliente de vpn-ssl para los sistemas operativos Windows.		
RFT71	Debe permitir crear políticas para tráfico vpn-ssl.		
RFT72	Debe soportar autenticación de vpn-ssl con ldap, secure id y base de datos propia.		
RFT73	Debe permitir la creación de políticas basadas en el control por aplicación, categoría de aplicación, sub-categoría, tecnología y factor de riesgo, control por usuario, grupos de usuarios o dirección ip.		
RFT74	Debe permitir la creación de reportes personalizables y debe incluir al menos reportes de: sesiones por aplicación, utilización de ancho de banda, eventos, ataques, origen y destino del tráfico, usuarios más frecuentes, aplicaciones más frecuentes, amenazas más frecuentes, destinos más frecuentes.		
RFT75	Debe permitir el almacenamiento de logs internamente o en ubicaciones externas definidas por el administrador.		
RFT76	Debe poder manejar múltiples dominios de firewall.		
RFT77	La alta disponibilidad debe ser transparente, sin pérdida de conexiones en caso de que un nodo falle.		
RFT78	La alta disponibilidad debe poder configurarse en modo Activo- Activo / Activo-Pasivo.		
RFT79	Debe tener posibilidad de definir al menos dos interfaces para sincronía y poder gestionar cada equipo de manera independiente.		
RFT80	Debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		
RFT81	La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
RFT82	El listado de aplicaciones debe actualizarse periódicamente.		
RFT83	Debe soportar inspección de Contenido SSL.		
RFT84	La solución debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.		
RFT85	La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.		
RFT86	Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.		
RFT87	El equipo debe ser capaz de analizar contenido cifrado para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS.		
RFT88	La solución ofertada debe permitir la administración vía web, cli, syslog, snmp2. Administración basada en roles y debe ser centralizada para todos los firewalls propuestos.		
RFT89	Debe permitir almacenamiento de eventos de manera interna y/o en un repositorio que pueda consultarse luego con SQL.		
RFT90	Debe contar con Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.		
RFT91	Debe poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Edge, Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.		
RFT92	El oferente debe incluir los siguientes Software, Licencias y Equipos: • Autenticador-VM (Authenticator-VM) con licencia Perpetuas para 100 Usuarios. Este		

	Autenticador debe correr en diferente plataforma de Virtualización, tales como: VMWare y Microsoft Hyper-V. • Debe incluirse software y licencia perpetua para 50 Generadores de contraseñas (Tokens Virtuales) para dispositivos iOS, Android y Windows Phone. (Software one-time password tokens for iOS, Android and Windows Phone mobile devices. Perpetual licenses for 50 users. Electronic license certificate). • Deben incluirse 50 Tokens Físicos (Generador de contraseña basado en tiempo). Licencia Perpetua. **Nota:** Estas licencias y equipo deben tener las mismas condiciones de los Requerimientos de Garantía y Soporte (RGS) anteriormente citados en este pliego.		
	OTROS REQUERIMIENTOS		
RFT93	Todos los equipos de este Lote I serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos (2) UPS independientes para alta disponibilidad.		
RFT94	Las Soluciones propuestas de **Firewalls** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad).		

Lote No. 2 Balanceadores de Carga (Application Delivery Controllers (ADCs)).

a) Requerimientos de Contratación, Garantía y Soporte Balanceadores de Carga (Application Delivery Controllers (ADCs)).

Req. Núm. **Requerimientos de Contratación (RDC).**			
Acreditaciones y Experiencia del Oferente.	**Descripción**	**Solución Propuesta**	**Número de Partes**
RDC01	El Oferente debe contar con una experiencia mínima de tres (3) años y con tres (3) o más clientes, fuera o dentro del territorio dominicano, donde haya ejecutado proyectos de implementación de soluciones **Aplication Deilvery Controllers (ADCs)** de manera satisfactoria y cualquier otro equipo que esté contemplado en la propuesta de implementación. Para esto el Oferente presentará una carta de recomendación por cada uno de los tres (3) o más clientes referenciados, tal como se lista en las especificaciones del Pliego.		
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de **Aplication Deilvery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Para tal efecto, el Oferente presentará una Carta de Certificación del Fabricante, de que puede vender, dar soporte a los equipos y soluciones de este Fabricante en la República Dominicana.		
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones **Aplication Deilvery Controllers (ADCs)** y de cualquier otro equipo que esté contemplado en la propuesta de implementación. Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.		
RDC04	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** deben estar dentro del Informe de Gardner**, "Magic Quadrant for Application Delivery Controllers",** dentro del cuadrante de **Líderes (Leaders).** Dicho informe de referencia deberá ser actualizado, es decir, debe ser la última publicación valida. Este documento debe ser anexado a la Propuesta.		
RDC05	La instalación y migración de los servicios, equipos, configuraciones y demás debe ser contemplada como parte de la propuesta; incluyendo la puesta en funcionamiento de las políticas de seguridad y monitoreo descritos en los requerimientos técnicos y funcionales. El cableado, switches y demás componentes necesarios para la instalación y puesta en funcionamiento de las soluciones deben formar parte de la propuesta.		
RDC06	Deben dejar en correcto funcionamiento todo lo relacionado a la infraestructura propuesta. La implementación de los equipos y aplicativos citados en este pliego no debe afectar las operaciones diarias de la JI, por lo que el oferente debe tomar las medidas necesarias para este requerimiento.		
RDC07	Si el Oferente subcontrata o integrara todos o parte de los servicios a ofrecer deberá presentar un acuerdo entre las partes donde indique su intención de trabajar en colaboración (Joint-Venture) en el proyecto de implementación de las soluciones. El Subcontrato deberá contar con la anuencia de la Jurisdicción Inmobiliaria – Poder Judicial, siendo siempre el responsable ante la Institución el contratista (adjudicatario).		
Tiempos de Entrega y de Implementación.			
RDC08	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de **Aplication Deilvery Controllers (ADCs)** en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.		

RDC09	La JI requiere que este proyecto sea ejecutado en un plazo no mayor a dos (2) meses, a partir de la entrega de los equipos.		
RDC10	El oferente elaborará un documento informando los productos entregados e instalados; y validando los requerimientos técnicos que han sido cumplidos; así como los riesgos que han sido mitigados. Nota: Este documento debe contener las descripción de todas las políticas implementadas.		
Normas de Seguridad Industrial.			
RDC11	El Oferente presentará como parte de su propuesta los procedimientos y políticas que utiliza para la Seguridad de su Personal y la propiedad privada de la JI. Así como los recursos, tales como equipo, señalización y protección.		
Responsabilidades del Oferente.			
RDC12	La presentación de las Propuestas debe cumplir con los siguientes requisitos: • Deben describir claramente la Marca y el Modelo ofertado. • Deben describir los detalles técnicos de todos los equipos presentados. • Las propuestas deberán ser presentadas en idioma español. • La propuesta presentada deberá describir (el **#** de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento. • Las propuestas deben describir de forma detallada, clara y precisa los Costos de los Equipos (Hardware/Software), Costos de las Licencias y los Costos de la Garantía y el soporte. • La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF) • El formato digital debe permitir realizar búsqueda dentro del documento (OCR). • Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.		
RDC13	El Oferente revisará y leerá detenidamente el contenido de este documento, y hará las preguntas necesarias conforme al protocolo descrito en estos términos de referencia.		
Requerimientos de Garantía y Soporte (RGS).			
Garantías y Soporte.			
RGS01	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contarán con una garantía en Piezas y Servicios (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.		
RGS02	El Software de Administración de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionabilidades y la asistencia en la implementación de los mismos cuantas veces sean necesarias sin costo adicional) de tres (3) años, con nivel de atención 24 x 7 x 365, con cuatro (4) horas máximo de respuesta (Soporte Reactivo). **Nota:** Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.		
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, comenzará a aplicarse a partir de la instalación y puesta en funcionamiento de las mismas. **Nota:**Para fines de Inicio del Periodo de Garantía y la Puesta en Funcionamiento de los Equipo estará aprobada a partir del Documento de Aceptación, el cual será firmado por la JI y el Oferente.		
RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de **Aplication Deilvery Controller (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deberá ser posterior al tercer (3er.) año de garantía, tomando como referencia la fecha de esta licitación (Entrega/Apertura de Ofertas). Por lo que se solicita para validar este requerimiento que se presente la constancia escrita del fabricante de la Solución de **Aplication Deilvery Controller (ADCs)**. La propuesta debe incluir equipos de última generación del fabricante.		
RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, el costo de renovación de Soporte y Licenciamiento no será mayor al 15% de adquisición del Equipo, durante los años 4to y 5to año. Ejemplo: si el costo del soporte y de Licenciamiento cuando se adquirió el equipo fue de 100 Pesos, este no podrá costar más 115 Pesos, es decir, no podrá ser mayor a un 15%.		
RGS06	El Fabricante y el Oferente de las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación deben presentar garantías (documentaciones) de que mantienen en la República Dominicana el inventario de todas partes y piezas necesarias para dar soporte a dicho equipo después de su puesta en producción.		

Requerimientos de Capacitación.			
RGS07	Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes: ➢ Instalación, Configuración y Administración de los **Aplication Deilvery Controllers (ADCs).** Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos: • Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos. • Las capacitaciones serán realizadas de forma Presencial. • El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros. • Estas capacitaciones deberán ser impartidas en idioma español. • Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes. • Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente. • El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI. • El oferente cubrirá con todos los costos de la capacitación. • Estas capacitaciones deben impartirse previo a la implementación de los equipos, para que la JI pueda definir las mejores prácticas a ponerse en ejecución durante el proceso de implementación de dichos equipos. Los instructores deberá ser docentes calificados y certificados por el/los fabricante/s de las soluciones a instalar. La empresa suplidora deberá correr con los gastos de alojamiento, viáticos y pasaje aéreo del personal docente, si se necesitaré participación de los instructores Extranjeros.		

b) Requerimientos Funcionales y Técnicos para 2 Balanceadores de Carga (Application Delivery Controllers (ADCs)) en la Red Perimetral.

CARACTERÍSTICAS FÍSICAS Y DE RENDIMIENTO	Descripción	Solución Propuesta	Número de Partes
RFT01	2 **Application Delivery Controller (ADCs),** o solución de balanceo de servidores y de enlaces que permita mejorar el desempeño de las mismas y al mismo tiempo generar un esquema de alta disponibilidad; ambos instalados en modo HA.		
RFT02	El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado **"Appliance".**		
RFT03	El sistema operativo del equipo ofertado debe ser de propósito específico y no uno de uso genérico, es decir, un SO desarrollado por el fabricante específicamente para propósitos de Balanceo de Carga de Servicios y Aplicaciones basadas en IP (TCP/UDP) y servicios web.		
RFT04	Los valores de desempeño solicitados deberán ser logrados por el equipo **"Appliance"** como un sistema independiente y autónomo que cumpla el desempeño exigido y no como la suma o agregación de varios **"Appliance"** que logren sumar el valor solicitado.		
RFT05	Se debe ofrecer dos (2) equipos en Alta disponibilidad (HA) funcionando en configuración Activo-Activo / Activo-Pasivo. Por razones de eficiencia de uso de la energía, la climatización, uso de espacio en rack, administración y facilidad de configuración, no se aceptará soluciones basadas en clúster virtual de múltiples equipos.		
RFT06	Cada equipo debe cumplir con las siguientes características: • La solución debe soportar un Throughput en L4 de al menos 10 Gbps. • La solución debe soportar un Throughput en L7 de al menos 10 Gbps. • La solución debe soportar un Throughput en SSL de al menos 10 Gbps. • La solución debe soportar una Compresión de Throughput de al menos 3.5 Gbps. • La solución deberá tener al menos 32 GB de Memoria. • La solución debe soportar al menos 1,400,000.00 Millones de peticiones en L7 HTTP requests/sec. • La solución de soportar al menos 13,000.00 Transacciones en SSL (SSL transactions/sec (2K key certificates) • La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • La solución de soportar al menos 6,000.00 Transacciones en ECDHE (ECDHE transactions/sec)		
RFT07	Cada equipo debe tener al menos las siguientes Interfaces de red: • 4x10GE SFP+ (4 puertos SFP+ de 10 Gbps (Transceivers Incluidos)) • 6x10/100/1000 CU (con opción de conectividad de 1 Gbps cobre o fibra (Transceivers Incluidos)). • 2x1G For Management. **Nota:** Además de lo anteriormente mencionado, estos equipos deben tener Soporte de Transceivers 10G SFP+: SR, LR;XFP		

RFT08	Las interfaces de 10G deben soportar velocidades de 1G o 10G dependiendo el transceiver usado.		
RFT09	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 100 a 240 VAC.		
RFT10	Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.		
RFT11	Los equipos deben tener la característica de soportar alta disponibilidad, es decir, tener la capacidad de conectarse a una unidad similar y operar en modo activo y la otra unidad en modo pasivo (fail-over) y deberá contar con la capacidad de direccionamiento virtual. La Solución debe tener la capacidad de recuperar las sesiones del sistema en forma inmediata y automática, en caso de fallo de un adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico.		
RFT12	Cada equipo debe incluir 32 GB de Memoria RAM mínimo		
RFT13	Cada equipo debe incluir mínimo un Disco duro de 240 GB SSD.		
RFT14	El oferente deberá especificar detalladamente las especificaciones técnicas de los equipos ofertados, a nivel de Hardware y Software. Ejemplo: • Tipo de Memoria. • Cantidad de Memoria en GB. • Cantidad Slot de Memoria. • Capacidad máxima de Memoria Soportada. • Procesador. • Capacidad y Velocidad del procesador. • Marca del Procesador. • Cantidad de Núcleos del Procesador • Generación del Procesador. • Tipo de disco Duro (Sata, Sata III o Hibrido, SSD Etc.)		
RFT15	Debe soportar Clúster Activo/Activo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).		
RFT16	La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean plataformas no necesariamente idénticas (como equipos appliance físico, chasis o virtuales) con el fin de contar con un sistema a futuro altamente escalable y en demanda.		
RFT17	Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.		
RFT18	Ante la necesidad de conmutar el tráfico a otros dispositivos del grupo, el sistema deberá poder realizar cálculos para determinar el mejor dispositivo basado en: recursos, capacidad, carga de tráfico en cada dispositivo. Identificando la mejor opción cuando el ambiente sea heterogéneo en cuanto se refiere a plataformas.		
RFT19	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.		
2	**FUNCIONES DE ADMINISTRACIÓN DE TRÁFICO**		
RFT20	La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.		
RFT21	La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.		
RFT22	La solución debe tener arquitectura Full-Proxy, control de entrada y salida de conexiones distinguiendo conexiones del lado del cliente y del lado del servidor o los recursos.		
RFT23	La solución ofertada debe ser capaz de soportar balanceo amortiguado de los servidores que se agreguen nuevos, para prevenir la saturación de conexiones. De manera que servidores que se agregan al grupo de balanceo, reciban al inicio menos cantidad de peticiones por un tiempo determinado, hasta ser capaz de recibir la misma cantidad de peticiones que los que ya estaban en el grupo.		
RFT24	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones.		
RFT25	La solución debe permitir hacer control de balanceo de tráfico según se defina entre uno o varios tipos de algoritmos especializados de balanceo. Estos métodos deben realizarse de manera nativa y no por medio de configuración por scripting: • Round Robín. • Proporcional (Ratio). • Proporcional dinámico. • Respuesta más rápida. • Conexiones mínimas. • Menor número de sesiones. • Tendencia de menor cantidad de conexiones (observed). • Tendencia de desempeño (predictive).		
RFT26	Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM		
RFT27	El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)		
RFT28	El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.		
RFT29	La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica.		
RFT30	La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de:		

	• Ping. • Chequeo a nivel de TCP y UDP a puertos específicos. • Monitoreo http y https. • Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft. • Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. • Ejecución de scripts para determinar la respuesta emulando un cliente. • Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. • Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma. • Monitoreo de aplicaciones de mercado: o LDAP o FTP o SMTP o IMAP/POP3 o Oracle o MSSQL o MySQL o RADIUS o SIP o Protocolo SASP o SOAP o WMI o SNMP		
RFT31	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes: • Dirección IP origen. • Dirección IP destino. • Cookies. • Hash. • SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia. • Sesiones SSL. • Microsoft Remote Desktop. • Entre otros.		
RFT32	Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.		
RFT33	Debe garantizar afinidad del servidor, de tal forma que una solicitud de un cliente y cada solicitud posterior se dirijan al mismo servidor de la granja.		
RFT34	El sistema debe ser capar de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.		
RFT35	Soporte de Scripts de Programación que permita crear funcionalidades que por defecto no se encuentran en el menú de configuración u opciones a través de un lenguaje gráfico.		
RFT36	Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: • Soporte de SOAP/XML, que sea base del Sistema Operativo. Que permita la integración con aplicaciones como VMWare vCenter, Microsoft System Center Virtual Machine Manager (SCVMM), Soporte de Java, .NET, PERL, PHP, PowerShell y Python. Las interfaces de control deben ser accesibles por conexiones SSL con requerimientos de autenticación vía http básica, para evitar accesos no autorizados.		
RFT37	Debe permitir la integración con plataformas de automatización a través del protocolo REST		
RFT38	Soporte de RESTful API		
RFT39	La solución debe tener la capacidad de ampliarse para soportar la creación de alta disponibilidad entre Datacenters a través de GSLB.		
RFT40	La solución debe soportar la configuración de un portal de acceso unificado con capacidad de ofrecer n-factores de autenticación.		
RFT41	Debe permitir la optimización de la interfaz y el tráfico presentado a los clientes que consumen las aplicaciones a través de la plataforma ADC (Front End Optimization).		
RFT42	Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.		
RFT43	Debe soportar el protocolo TDS para balanceo de MSSQL y SQL SERVER.		
RFT44	Debe soportar el protocolo MQTT para administración de tráfico desde dispositivos IoT. Debe permitir identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la información de los mensajes MQTT.		
RFT45	El sistema deberá soportar scripts de programación basados en un lenguaje estructurado que permita crear funcionalidades que por defecto no se encuentren en el menú de configuración u opciones y debe soportar la creación de Procedimientos o funciones que pueden ser utilizadas desde cualquier otro script.		
RFT46	El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC.		
RFT47	Debe soportar e incluir Geolocalización, de manera que pueda tomar decisiones basado en una base de datos de continentes, países y de direcciones IP.		

	La Base de datos de Geolocalización debe incluir los países de América Latina y estar disponible en el mismo equipo sin necesidad de acceso a Internet (offline).		
3	**FUNCIONES DE SEGURIDAD GENERALES**		
RFT48	Cada equipo debe soportar seguridad SSL con las siguientes características: • Incluir el soporte de Aceleración SSL usando Hardware Dedicado • Incluir mínimo 13,000.00 Transacciones por segundo SSL (2K Keys) • Incluir mínimo 6,000.00 Transacciones concurrente de Curva elíptica (ECDHE) • Soportar al menos 10 Gbps SSL (Throughput SSL) • La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA. • Soporte de llaves SSL de 1024, 2048 y 4096 bits		
RFT49	La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL.		
RFT50	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características • Session ID. • Session Ticket. • OCSP Stapling (on line certificate status protocol). • Dynamic Record Sizing. • ALPN (Application Layer Protocol Negotiation). • Forward Secrecy.		
RFT51	La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital SignatureAlgorithm (DSA) y Elliptic Curve Cryptography (ECDHE).		
RFT52	El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall). Nota: Debe Agregar certificación.		
RFT53	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.		
RFT54	Cada equipo debe incluir protección contra ataques de DDoS de mínimo 2,500,000.00 SYN/sec		
RFT55	Firmado criptográfico de cookies para verificar su integridad.		
RFT56	Capacidad de integración con dispositivos HSM "Hardware Security Module" (Módulo de Seguridad Hardware) externos. Deberá soportar al menos ThalesnShield YSafenet (Gemalto) Luna.		
RFT57	La solución debe permitir la funcionalidad Proxy SSL, esta funcionalidad permite que sesión SSL se establezca directamente entre el usuario y el servidor final, sin embargo el equipo balanceador debe ser capaz de desencriptar, optimizar y reencriptar el trafico SSL sin que el balanceador termine la sesión SSL.		
RFT58	Se requiere que soporte la extensión STARTTLS para el protocolo SMTP de manera de poder cambiar una conexión en texto plano a una conexión encriptada sin necesidad de cambiar el puerto.		
RFT59	Debe soportar HSTS (HTTP Strict Transport Security).		
RFT60	Debe soportar por medio de agregación de subscripción a futuro, un sistema de reputación IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías. • Scanners • Exploits Windows • Denial of Service • Proxies de Phishing • Botnets • Proxies anónimos		
4	**FUNCIONES DE ACELERACIÓN DE TRÁFICO**		
RFT61	La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de: • Memoria cache. • Compresión tráfico HTTP • Optimización de conexiones a la aplicación a nivel TCP • Multiplexación de conexiones hacia los servidores		
RFT62	El sistema deberá permitir comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Edge, Google Chrome, Mozilla Firefox, Safari, etc.		
RFT63	Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 3.5 Gbps o superior		
RFT64	Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.		
RFT65	Debe soportar el protocolo HTTP y funcionar como Gateway para este protocolo.		
RFT66	Permitir la modificación de los Tags de cache para cada objeto del sitio web de manera independiente, pudiendo respetar los Tags generados por el Web server o modificarlos.		
5	**FIREWALL DE APLICACIONES WEB (WAF)**		
RFT67	La solución debe incluir funcionalidad de Firewall de Aplicaciones (WAF) en la misma caja, no debe ser un Appliance independiente (para optimización de latencias, administración, espacio en rack, energía eléctrica, soportes de fabricante).		
RFT68	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.		
RFT69	La funcionalidad de WAF debe permitir la personalización de la política, de manera que se pueda ajustar finamente de acuerdo al servicio específico que estará protegiendo, sus URLs,		

	parámetros, métodos, de manera específica.		
RFT70	Debe trabajar en un esquema proxy TCP Reverso y/o Transparente.		
RFT71	Debe soportar la creación automática de políticas		
RFT72	Debe trabajar con políticas de seguridad por capas, donde se configura una política de seguridad base y las políticas de seguridad hijas heredan sus configuraciones y permita que solo cambios específicos se apliquen a las políticas hijas.		
RFT73	La creación automática de políticas deberá unificar múltiples URLs explicitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.		
RFT74	Debe trabajar en modo de bloqueo o en modo informativo		
RFT75	Debe permitir diferentes políticas de seguridad para diferentes aplicaciones		
RFT76	Debe permitir la creación de firmas personalizadas		
RFT77	Debe trabajar con modelos de seguridad positiva y negativa		
RFT78	Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana.		
RFT79	Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.		
RFT80	El WAF debe permitir personalizar las páginas de bloqueo		
RFT81	Debe prevenir exponer el "OS fingerprinting"		
RFT82	Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenzic, Qualys, IBM AppScan, HP WebInspect.		
RFT83	El WAF Debe soportar: • Restringir protocolo y versión utilizada. • Multi-byte language encoding. • Validar URL-encoded characters. • Restringir la longitud del método de request. • Restringir la longitud del URI solicitado. • Restringir el número de Encabezados (headers). • Restringir la longitud del nombre de los encabezados. • Restringir la longitud del valor de los encabezados. • Restringir la longitud del cuerpo (body) de la solicitud. • Restringir la longitud del nombre y el valor de las cookies. • Restringir el número de cookies. • Restringir la longitud del nombre y valor de los parámetros. • Restringir el número de parámetros.		
RFT84	El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)		
RFT85	El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP.		
RFT86	El WAF debe incluir protección contra Web Scraping.		
RFT87	Debe ser Session-aware es decir identificar y forzar que el usuario tenga una sesión e identificar los ataques por usuario.		
RFT88	Permitir la definición y detección de las condiciones a cumplir para que una aplicación externa que vía Java realiza un requerimiento Cross-Domain, permitiendo evitar un CORS (Cross-Origin Resource Sharing).		
RFT89	Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario		
RFT90	Debe permitir el enmascaramiento de información sensible filtrada por el servidor		
RFT91	Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de Geolocalización.		
RFT92	Debe permitir la integración con servidores Antivirus.		
RFT93	Debe brindar reportes respecto a la normativa PCI DSS 3.1 MINIMO.		
RFT94	Debe proteger contra ataque DoS /DDoS de Capa 4 Y 7.		
RFT95	Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa.		
RFT96	En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico para poseer información forense.		
RFT97	Debe soportar tecnologías AJAX y JSON .		
RFT98	Debe proteger como mínimo: • Ataques de Fuerza Bruta. • Cross-site scripting (XSS). • Cross Site Request Forgery. • SQL injection. • Parameter and HPP tampering. • Sensitive information leakage. • Session high jacking. • Buffer overflows. • Cookie manipulation. • Various encoding attacks. • Broken access control. • Forceful browsing.		

	• Hidden fields manipulation. • Requests muggling. • XML bombs/DoS. • Open Redirect.		
RFT99	Debe poder identificar y configurar URLs que generen un gran consumo de recursos en los servidores como método de protección de ataques de denegación de servicios.		
RFT100	Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP		
RFT101	Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas		
RFT102	Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.		
RFT103	Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.		
RFT104	Debe ofrecer protección sobre tráfico basado en Web Sockets.		
RFT105	El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.		
RFT106	Debe proteger las aplicaciones contra ataques de denegación de servicio a nivel de L4 y L7		
6	**ESTÁNDARES DE RED**		
RFT107	Soporte VLAN 802.1q, Vlantagging.		
RFT108	Soporte de 802.3ad para definición de múltiples troncales		
RFT109	Soporte de NAT, SNAT		
RFT110	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.		
RFT111	Soporte de Rate Shapping.		
RFT112	Soporte de dominios de Enrutamiento, donde cada uno pueda tener su propio Default Gateway y estar conectados a redes IP con el mismo direccionamiento.		
RFT113	Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.		
RFT114	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS,		
7	**ADMINISTRACIÓN DEL SISTEMA**		
RFT115	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS)		
RFT116	La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la autenticación de usuarios para gestión de la herramienta.		
RFT117	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.		
RFT118	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.		
RFT119	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales		
RFT120	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: • Protocolo SysLog • Notificación vía SMTP • SNMP versión.2.0 o superior.		
RFT121	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.		
RFT122	El equipo debe contar con un módulo de administración tipo lightsout que permita encender/apagar el sistema de manera remota y visualizar el proceso de arranque.		
RFT123	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real		
RFT124	Debe contar con un módulo de reportes que permita visualizar gráficamente el comportamiento de las aplicaciones HTTP como latencias hacia los servidores, latencias en los URL, Direcciones IPs que acceden las aplicaciones, URLs más visitados en las aplicaciones, Throughput hacia los servidores y estadísticas acerca de los servicios creados y los servidores físicos.		
RFT125	Debe Contar con plantillas para la implementación rápida de aplicaciones de mercado conocidas (Ejemplo: Oracle, Microsoft, SAP, IBM) y permitir crear plantillas personalizadas que puedan ser actualizadas/exportadas entre equipos.		
RFT126	Se debe un incluir una Herramienta de Análisis con su respectivo Licenciamiento, la cual permitirá una mejor gestión las solución ADCs Propuesta.		
8	**OTROS REQUERIMIENTOS**		
RFT127	Todos los equipos de este Lote serán instalados en un Gabinete (Rack) APC Netshelter SX 42U (Part No. AR3100), ya existente. Con dos (2) PDUs, que a su vez deberán estar conectadas a dos UPS independientes para alta disponibilidad.		
RFT128	Las Soluciones propuestas de **Aplication Deilvery Controllers (ADCs)** y cualquier otro equipo que esté contemplado en la propuesta de implementación, se conectaran a dos (2) UPS de 40KVA, trifásico a 208V. Estos UPS pueden proveer salidas monofásicas y trifásicas. Sera responsabilidad del Oferente la interconexión eléctrica del Gabinete hacia los dos (2) UPS (Los materiales utilizados deben ser certificados y de alta calidad).		

OFERTA ECONOMICA (ANEXO 1)

NOMBRE DEL OFERENTE:

Lote	Descripción del Bien, Servicio u Obra	Número de partes	Cantidad[2]	Precio Unitario	ITBIS	Precio Unitario Final

VALOR TOTAL DE LA OFERTA EN CIFRAS: ..... RD$

VALOR TOTAL DE LA OFERTA EN LETRAS:.....

.....nombre y apellido..... en calidad de ....., debidamente autorizado para actuar en nombre y representación de (poner aquí nombre del Oferente y sello de la compañía, si procede)

Firma

_____...../...../.....

.... fecha

[2]Si aplica.

PRESENTACION DE OFERTA (ANEXO 2)

Señores
Indicar Nombre de la Entidad

Nosotros, los suscritos, declaramos que:

a) Hemos examinado y no tenemos reservas al Pliego de Condiciones para la Licitación de referencia, incluyendo los documentos o enmiendas que lo conforman.

b) De conformidad con los Pliegos de Condiciones y según el plan de entrega especificado, nos comprometemos a suministrar los servicios y bienes establecidos en la licitación pública nacional No. LPN-CPJ-12-2017.

c) Nuestra oferta se mantendrá vigente por un período de (120) días, contado a partir de la fecha límite fijada para la presentación de ofertas, de conformidad con los Pliegos de Condiciones de la Licitación. Esta oferta nos obliga y podrá ser aceptada en cualquier momento hasta antes del término de dicho período.

a) Si nuestra oferta es aceptada, nos comprometemos a obtener una garantía de fiel cumplimiento del Contrato, de conformidad con los Pliegos de Condiciones de la Licitación, por el importe del **CUATRO POR CIENTO (4%)** del monto total de la adjudicación, para asegurar el fiel cumplimiento del Contrato.

b) Para esta licitación no somos partícipes en calidad de Oferentes en más de una Oferta, excepto en el caso de ofertas alternativas, de conformidad con los Pliegos de Condiciones de la Licitación.

c) Nuestra firma, sus afiliadas o subsidiarias, incluyendo cualquier subcontratista o proveedor de cualquier parte del Contrato, no han sido declarados inelegibles por el Comprador para presentar ofertas.

d) Entendemos que esta Oferta, junto con su aceptación por escrito que se encuentra incluida en la notificación de adjudicación, constituirán una obligación contractual, hasta la preparación y ejecución del Contrato formal.

e) Entendemos que el Comprador no está obligado a aceptar la Oferta evaluada como la más baja ni ninguna otra de las Ofertas que reciba.

(Nombre y apellido) _____en calidad de _____ debidamente autorizado para actuar en nombre y representación de (poner aquí nombre del Oferente)

Firma _____

Sello(Persona o personas autorizadas a firmar en nombre del Oferente)

FORMULARIO DE INFORMACION SOBRE EL OFERENTE (ANEXO 3)

[El Oferente deberá completar este formulario de acuerdo con las instrucciones siguientes. No se aceptará ninguna alteración a este formulario ni se aceptarán sustitutos.]

Fecha: _____

1. Nombre/ Razón Social del Oferente: *[indicar el nombre jurídico del Oferente]*
2. Si se trata de una asociación temporal o Consorcio, nombre jurídico de cada miembro: *[indicar el nombre jurídico de cada miembro del Consorcio]*
3. RNC/ Cédula/ Pasaporte del Oferente:
4. RPE del Oferente: *[indicar el número del Registro de Proveedores del Estado]*
5. Domicilio legal del Oferente:
6. Información del Representante legal autorizado del Oferente: Nombre: *[indicar el nombre del representante autorizado]* Dirección: *[indicar la dirección del representante autorizado]* Números de teléfono y fax*: [indicar los números de teléfono y fax del representante autorizado]* Dirección de correo electrónico: *[indicar la dirección de correo electrónico del representante autorizado]*

DECLARACIÓN JURADA (Anexo 4)

Quien suscribe, ___(nombre)_____, (generales)____, en calidad de __(cargo que desempeña)_____, actuando en nombre y representación de _(nombre de la persona física o jurídica)_____, _____(generales y domicilio de la sociedad), conforme a los poderes que me fueran otorgados, en virtud de mis facultades estatutarias, por medio de presente documento, y en respuesta a los requerimientos de la convocatoria de licitación No. LPN-CPJ-12-2017 del Consejo del Poder Judicial para la adquisición de _____, declaro BAJO LAS MÁS SOLEMNE FE DEL JURAMENTO, lo siguiente:

1. No nos encontramos en ninguna de las situaciones de prohibiciones de contratar establecidas en el pliego de condiciones.
2. Que ningún funcionario o empleado del Poder Judicial tiene interés pecuniario en la oferta.
3. Que no hay ningún acuerdo de parte de **(nombre de la empresa oferente)**con persona particular, sociedad, corporación o firma para someter varias ofertas bajo nombres distintos.
4. Que ni nosotros ni nuestro personal directivo ha sido sometido ni condenado por un delito relativo a su conducta profesional o por declaración falsa o fraudulenta acerca de su idoneidad para firmar un contrato adjudicado.
5. Que no tenemos juicios pendientes con el Estado Dominicano.
6. Que no estamos sometidos a un proceso de quiebra ni liquidación.
7. Que estamos al día en el pago de nuestras obligaciones de la Seguridad Social y Tributarias, conforme a la legislación vigente.
8. Que no estamos embargados; nuestros negocios no han sido puestos bajo administración judicial, y nuestras actividades comerciales no han sido suspendidas ni se ha iniciado procedimiento judicial en nuestra contra por cualquiera de los motivos precedentes;

La presente DECLARACIÓN JURADA ha sido realizada en la ciudad de _____, República Dominicana a los ( ) días del mes de _____ del año dos mil diecisiete (2017).

_____

(Coletilla del Notario)

_____
Notario Público

CURRICULUM DEL PERSONAL PROFESIONAL PROPUESTO

1. Cargo propuesto [*solamente un candidato deberá ser nominado para cada posición]:*

_____

2. Nombre de la firma: *[inserte el nombre de la firma que propone al candidato]:*

_____

3. Nombre del individuo: *[inserte el nombre completo]:*

_____

4. Fecha de nacimiento: _____ **Nacionalidad:** _____

5. Educación: [*Indicar los nombres de las universidades y otros estudios especializados del individuo, dando los nombres de las instituciones, grados obtenidos y las fechas en que los obtuvo.*]

6. Asociaciones profesionales a las que pertenece:

_____

_____

7. Otras especialidades *[Indicar otros estudios significativos después de haber obtenido los grados indicados en el 5 – Dónde obtuvo la educación]:*

_____

8. Países donde tiene experiencia de trabajo: *[Enumere los países donde el individuo ha trabajado en los últimos diez años]:*

_____

_____

9. Idiomas *[Para cada idioma indique el grado de competencia: bueno, regular, pobre, en hablarlo, leerlo y escribirlo]:*

_____

_____

10. Historia Laboral *[Empezando con el cargo actual, enumere en orden inverso cada cargo que ha desempeñado desde que se graduó el candidato, indicando para cada empleo (véase el formulario siguiente): fechas de empleo, nombre de la organización, cargos desempeñados]:*

Desde [*Año]:* _____ Hasta [*Año*] _____ Empresa: _____

Cargos desempeñados: _____

11. Detalle de las actividades asignadas:	**12. Trabajos que ha realizado que mejor demuestran la capacidad para ejecutar las tareas asignadas:**
[Enumere todas las tareas que desempeñará bajo este trabajo]	*[Entre todos los trabajos que el individuo ha desempeñado, complete la siguiente información para aquellos que mejor demuestran su capacidad para ejecutar las tareas enumeradas bajo el punto 11.]* Nombre de la tarea o proyecto: _____ Año: _____ Lugar: _____ Contratante: _____ Principales características del proyecto: _____ Actividades desempeñadas:_____

13. Certificación:

Yo, el abajo firmante, certifico que, según mi mejor conocimiento y mi entender, este currículo describe correctamente mi persona, mis calificaciones y mi experiencia. Entiendo que cualquier declaración voluntariamente falsa aquí incluida puede conducir a mi descalificación o la cancelación de mi trabajo, si fuera contratado.

_____ Fecha: _____

[Firma del individuo o del representante autorizado del individuo] *Día / Mes / Año*

Nombre completo del representante autorizado: _____