



COMITÉ DE COMPRAS Y CONTRATACIONES

**PRESENTACION DE OFERTA**

Señores  
Consejo del Poder Judicial (CPJ).

17 de agosto de 2017

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

José Martín Guzmán en Calidad de Representante Legal debidamente autorizado para actuar en nombre y representación de Multicómputos S.R.L.

Firma

LPN-CPJ-12-2017





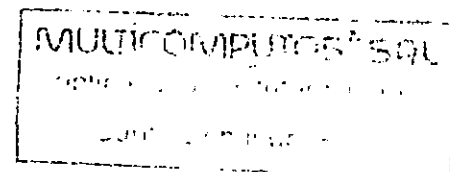
COMITÉ DE COMPRAS Y CONTRATACIONES

FORMULARIO DE INFORMACIÓN SOBRE EL OFERENTE

Página 1 de 1

Fecha: 17 de agosto de 2017

1. Nombre/ Razón Social del Oferente: Multicómputos SRL
2. Si se trata de una asociación temporal o Consorcio, nombre jurídico de cada miembro: N/A
3. RNC/ Cédula/ Pasaporte del Oferente: 1-0163880-1
4. RPE del Oferente: 39
5. Domicilio legal del Oferente: Abraham Lincoln, edificio Óptica Felix 4to. Piso
6. Información del Representante autorizado del Oferente: Nombre: José Martín Guzmán Dirección: Abraham Lincoln, edificio Óptica Felix 4to. Piso Números de teléfono y fax: 809-540-2846 / 809-540-2847 Dirección de correo electrónico: <a href="mailto:martin.guzman@multicomputos.com">martin.guzman@multicomputos.com</a> <a href="mailto:licitaciones@multicomputos.com">licitaciones@multicomputos.com</a> / <a href="mailto:laura.delgado@multicomputos.com">laura.delgado@multicomputos.com</a>



*J. Guzmán*

## Resumen Ejecutivo

El Consejo del Poder Judicial y La Jurisdicción Inmobiliaria, enmarcada en su visión de mantener su imagen de prestigio, credibilidad, transparencia y eficiencia, precisa de una infraestructura de seguridad de la información que le permita brindar servicios protegidos de las amenazas que ponen en riegos las operaciones propias de los registros de títulos a través de su plataforma tecnológica.

Multicómputos SRL presenta su propuesta de venta e implementación de la infraestructura de seguridad para responder a los desafío de la seguridad de la información de Jurisdicción Inmobiliaria. Para la elaboración de esta propuesta, hemos seleccionado las mejores soluciones disponibles del mercado para lograr los objetivos de la seguridad de la información sea escalable, segura, confiable, y que su operación sea centralizada y simplificada, garantizando la entrega de los servicios de manera ágil y segura.

Multicómputos SRL, como proveedor sólido con 30 años de experiencia en infraestructura tecnológica, incluyendo equipamiento para la seguridad de la información, ha seleccionado las soluciones del fabricante **Citrix** para llenar los requisitos de equipamiento de hardware y software que se hacen en la presente licitación.

Mediante una combinación de las tecnologías de optimización y balanceo más inteligentes, el NetScaler es capaz de evitar contingencias en los servidores de aplicaciones, provocadas por picos de requerimientos de los clientes. El NetScaler recibe todos los requerimientos y los envía a los servidores de acuerdo a algoritmos y políticas flexibles definidos por los administradores de las aplicaciones de Internet utilizando interfaces GUI muy intuitivas, garantizando así la disponibilidad y la calidad del servicio a los clientes bajo cualquier condición.

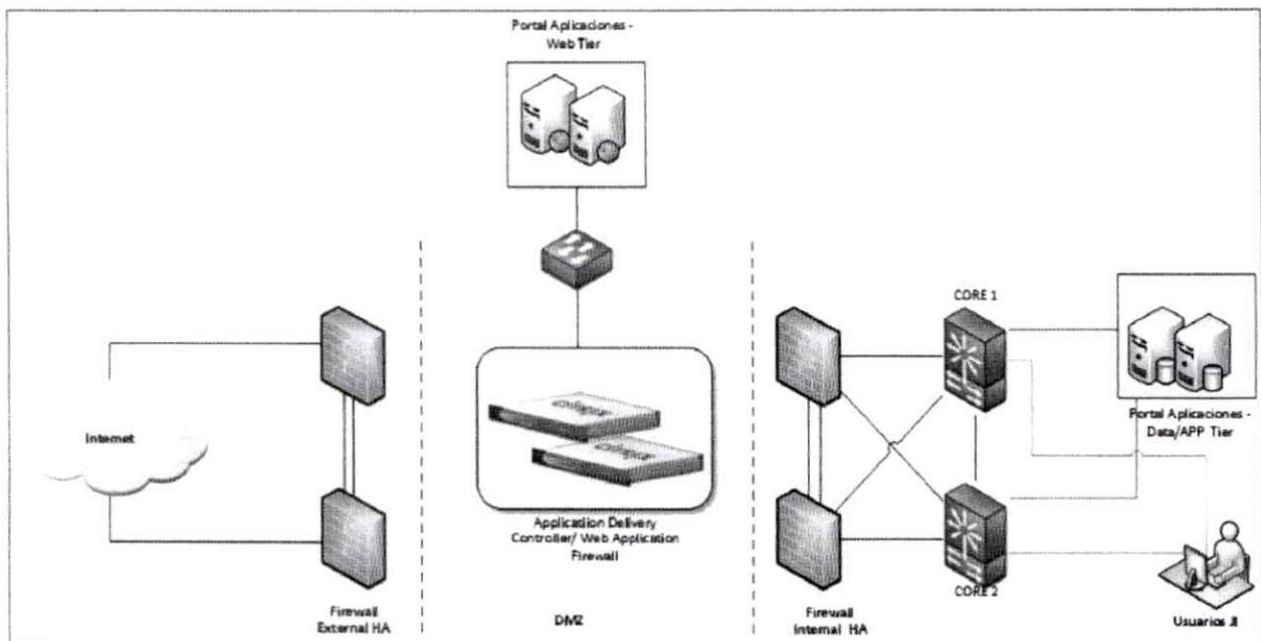


## Requerimientos de la Licitación

La jurisdicción inmobiliaria requiere equipos de seguridad de última generación para cubrir sus necesidades actuales y futuras de publicar sus servicios de manera segura, y al mismo tiempo blindar sus operaciones de infraestructura para minimizar y/o reducir el impacto las vulnerabilidades de algunos de procesos. Los equipos que la Jurisdicción inmobiliaria requiere son:

- A) Balanceadores - Application Delivery Controllers - En Alta Disponibilidad

## Arquitectura Propuesta



Los NetScaler tendrán la función de proveer toda la optimización y aceleración de la aplicación para brindar una mejor experiencia a los usuarios y de asegurar la aplicación con el módulo de Web Application Firewall.

## Resumen técnico de los equipos propuestos

En nuestra oferta proponemos una integración de todos elementos de seguridad trabajen de manera coordinada en la prevención y detección contra cualquier acción que sea capaz de afrentar los sistemas informáticos de la jurisdicción Inmobiliaria

En resumen nuestra propuesta incluye:

Lote 2:

- **Balanceadores Citrix NetScaler MPX8910 PE:** Los dos appliances Citrix NetScaler proveerá optimización y alta disponibilidad a las aplicaciones de la Jurisdicción Inmobiliaria. Con las funcionalidades de optimización de TCP, caching y compresión entregaremos una aplicación rápida y eficaz. Al mismo tiempo aumentamos la capacidad de manejar conexiones de los servidores mediante la aceleración de SSL y la multiplexación de conexiones. Agregamos un componente integrado en los NetScalers de Web Application Firewall (WAF) para brindar una capa de seguridad adicional en la capa de aplicación, protegiendo de ataques dirigidos específicamente a las aplicaciones, tales como SQL Injection, cross-site-scripting(xss), Cross-Site Request Forgery (CSRF), Insecure Direct Object References, entre otras amenazas que vayan en detrimento de la aplicación. Mediante el modelo de seguridad positivo, que agrega al modelo de protección por firmas, el WAF puede obligar políticas de uso estrictas en las aplicaciones, y bloquear cualquier intento de manipulación no identificado todavía en las bases de datos de firmas de ataques conocidos (ataques de día 0).

### Citrix NetScaler MPX8910 PE

Desempeño:

- **Platform attributes**
- **Memory :** 32 GB
- **Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3-2002/2005/2008/2012):** 4x10GE SFP+; 6x10/100/1000 CU
- **Transceivers support:** 10GE SFP+; SR, LR; 1G CU
- **Pay as you grow and BurstPack license upgrades:** Upgrade option to MPX 8920
- **Platform performance**
- **System throughput, Gbps :**10
- **HTTP requests/sec (MPX/SDX):** 1,400,000
- **SSL transactions/sec (2K key certificates):** 13,000
- **ECDHE transactions/sec:** 6,000
- **SSL throughput, Gbps (MPX / SDX):** 10
- **Compression throughput, Gbps (MPX / SDX):** 3.5
- **ICA Proxy/SSL VPN concurrent users:** 10,000



## Sobre Citrix:

Citrix® NetScaler® Platinum Edition es una solución de entrega de aplicaciones Web que reduce los costos del centro de cómputos y acelera el rendimiento de las aplicaciones hasta cinco veces. Proporciona visibilidad de la experiencia de aplicaciones del usuario final y seguridad integral de aplicaciones Web conjuntamente con administración avanzada del tráfico. NetScaler Platinum Edition se encuentra disponible como una familia de dispositivos con capacidad de ampliaciones diseñadas expresamente para organizaciones que necesitan optimizar el rendimiento y la disponibilidad de aplicaciones internas o públicas con niveles de servicio estrictos o con información confidencial que debe estar protegida de ataques a nivel de aplicaciones.

Citrix NetScaler realiza un análisis del tráfico de aplicaciones que pasa a través de él, para de manera inteligente distribuir, optimizar y asegurar el tráfico de red correspondiente a las aplicaciones y servicios críticos de la empresa.

Citrix NetScaler provee una combinación extensa y completa de capacidades que lo convierten en la plataforma de entrega de servicios líder del mercado, las cuales se agrupan en las áreas de seguridad de aplicaciones, aceleración, visibilidad y alta disponibilidad (incluyendo balanceo global o GSLB) a través de la línea más completa de plataformas tipo appliance, virtual appliance o multi-tenant.

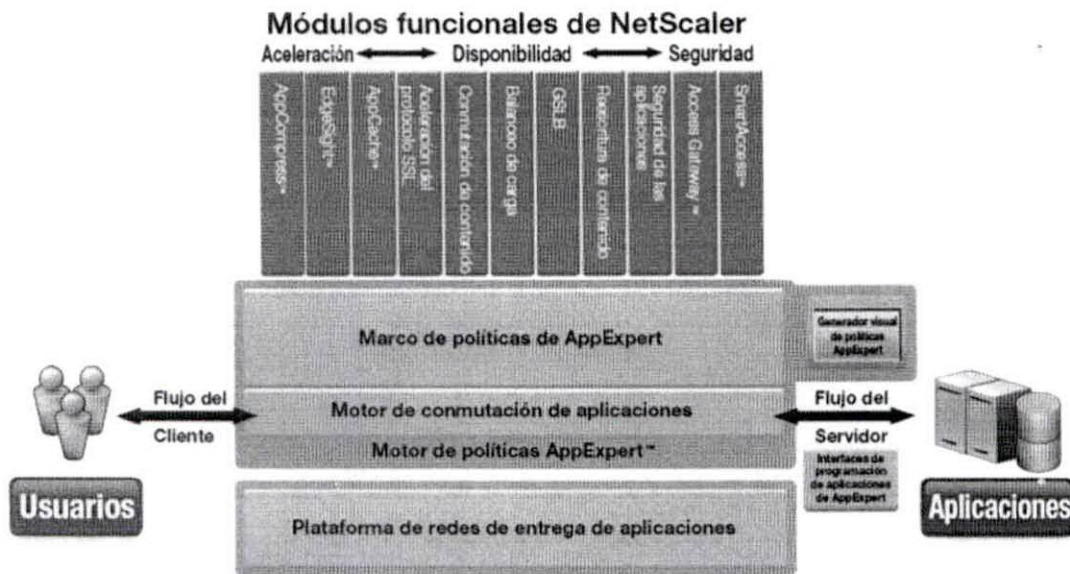
Citrix NetScaler puede ubicarse frente a los servidores Web y de Bases de Datos de la empresa, proveyéndoles balanceo de alta velocidad, switching de contenido, compresión de los datos, caching de contenido, aceleración de la encriptación SSL, optimización de la red, visibilidad de las aplicaciones y seguridad de las aplicaciones, todo esto en una sola plataforma completa. El efecto neto es que se mantiene el 100% de disponibilidad de los servicios con un buen desempeño para clientes y usuarios, a la vez que reduce y normaliza la carga de los servidores, de forma que se ahorra costos en infraestructura de servidores. Adicionalmente, con la compresión puede reducir el tráfico de manera promedio en más de un 75%, lo cual evita la congestión en los enlaces de Internet.

Citrix NetScaler también puede ubicarse en el perímetro externo de la empresa, para que además de ofrecer toda la optimización y alta disponibilidad del tráfico entrante hacia los servidores de aplicaciones que sirven contenido a clientes externos, también balancea de manera automática e inteligente el tráfico saliente a través de múltiples líneas o enlaces de Internet de diferentes proveedores. Para ello el Citrix NetScaler hace un monitoreo inteligente y en tiempo real de la condición de los enlaces, de manera que puede balancear tráfico con preferencia en los enlaces de mayor velocidad, menos latencia y menos ocupación, de manera que logra una utilización simultánea y balanceada de todos los enlaces. En cuanto a las fallas ocurridas en los enlaces o en las redes de los proveedores de Internet, Citrix NetScaler las puede detectar inmediatamente y tomar acción en el tráfico por medio de monitores inteligentes configurables, de manera que con el Citrix NetScaler estas fallas resultan imperceptibles para los usuarios internos y externos.

Citrix NetScaler se integra de manera completa con los equipos de la red, tanto a nivel de capa 2, como a nivel de capa 3, incluyendo los protocolos de enrutamiento estático y dinámicos (RIP, OSPF y BGP), soportando IP versiones 4 y 6. También NetScaler soporta funciones de NAT y RNAT para



integrarse con cualquier esquema de direccionamiento IP existente. Con el partnership de Citrix con el fabricante de equipos de redes Cisco, vigente desde hace más de dos años, NetScaler también se puede integrar a nivel de red y servicios con la línea de switches modulares Nexus mediante la tecnología RISE de Cisco, de forma que un appliance NetScaler puede asumir el rol de ser un módulo de servicios de los switches Nexus. Este tipo de integraciones agregan valor para las empresas que tengan sus redes basadas de Cisco.



### Aceleración del rendimiento de las aplicaciones

Citrix NetScaler puede incrementar el rendimiento de las aplicaciones hasta cinco veces. Citrix® AppCompress™ mejora el rendimiento del usuario final y reduce el consumo de ancho de banda mediante la compresión de datos de aplicaciones Web, independientemente de si están encriptados o no, antes de ser enviados al cliente. Citrix® AppCache® acelera la entrega del contenido a los usuarios al ofrecer caché rápido en memoria del contenido estático y dinámico de las aplicaciones HTTP.

Además, Citrix NetScaler ofrece múltiples optimizaciones de TCP para mejorar el rendimiento de la red y la infraestructura del servidor. Las optimizaciones de TCP de NetScaler son visibles para los clientes y los servidores, acelerando la entrega de cualquier aplicación empresarial o basada en la Web sin prácticamente requerir configuración.

### Balanceo de carga y conmutación de contenido inteligentes

Cuando NetScaler se implementa delante de los servidores de aplicaciones, ofrece dirección granular de las solicitudes de los clientes para garantizar la óptima distribución del tráfico. Además de la información del nivel 4 (protocolo y número de puerto), las políticas de administración del tráfico para las aplicaciones TCP pueden estar basadas en cualquier contenido a nivel de las aplicaciones. Los administradores pueden segmentar de manera granular el tráfico de las aplicaciones basándose

en la información contenida en el cuerpo de una solicitud HTTP o en la carga útil de TCP, así como también en la información de encabezado L4-7, como la URL, el tipo de datos de las aplicaciones o cookies. Numerosos algoritmos de balanceo de carga y un continuo chequeo del sistema proporcionan una mayor disponibilidad de las aplicaciones garantizando que las solicitudes del cliente sean dirigidas únicamente a los servidores que funcionan correctamente.

### **Seguridad integral de las aplicaciones**

Platinum Edition incluye la tecnología NetScaler Application Firewall que protege, de manera proactiva, las aplicaciones Web de ataques a nivel de aplicaciones, como inyección SQL, reescritura de comandos entre sitios, exploración forzada y envenenamiento de cookies, y ayuda a prevenir el robo y la filtración de datos valiosos de la empresa y de los clientes.

NetScaler Platinum Edition incluye defensas incorporadas y de alto rendimiento contra los ataques de negación de servicio (DoS). Las capacidades de inspección del contenido permiten que Citrix NetScaler identifique y bloquee los ataques basados en aplicaciones, como las sobrecargas GET y los ataques de extracción de datos de sitios. Los incrementos legítimos en el tráfico de aplicaciones, que desbordarían los servidores de aplicaciones, se manejan automáticamente con características configurables de Protección ante picos de demanda y Colas de prioridad (Surge Protection & Priority Queuing).

### **Visibilidad de la experiencia del usuario final**

Citrix InSight™ para NetScaler proporciona visibilidad a nivel de páginas del rendimiento de las aplicaciones Web. InSight para NetScaler instrumenta las páginas HTML del cliente en forma transparente mediante un control proactivo del tiempo de respuesta de las páginas Web desde la perspectiva del usuario final. Las mediciones del tiempo de respuesta se combinan con las estadísticas detalladas sobre las duraciones de las transmisiones de solicitudes y respuestas a través de la infraestructura de sitios Web y proporcionan así una visibilidad granular sobre cómo las aplicaciones Web están funcionando desde la perspectiva del usuario final.

### **Aceleración del protocolo SSL**

NetScaler integra la aceleración del protocolo SSL basado en hardware para aliviar a los servidores Web de las arduas tareas de configuración de la conexión con protocolo SSL y del cifrado masivo. La aceleración del protocolo SSL reduce la utilización de CPU en servidores, lo que libera recursos de servidores disponibles para otras tareas. NetScaler Platinum Edition también se encuentra disponible en un modelo que cumple con las normas FIPS, que ofrece generación de claves y almacenamiento seguros.

### **Reducción de los costos operativos y de implementación**

Citrix NetScaler disminuye los costos de entrega de aplicaciones al reducir el número de servidores requeridos y al optimizar el uso de ancho de banda de red disponible. El intuitivo generador visual de políticas AppExpert permite la creación de políticas de entrega de aplicaciones sin necesidad de codificar programas o secuencias de comando complejos. Además, NetScaler reduce los gastos operativos continuos a través de la unificación de múltiples capacidades en una única solución. Para administrar múltiples dispositivos NetScaler, el Centro de comando de NetScaler, que se encuentra disponible para la venta por separado, proporciona una administración centralizada de la



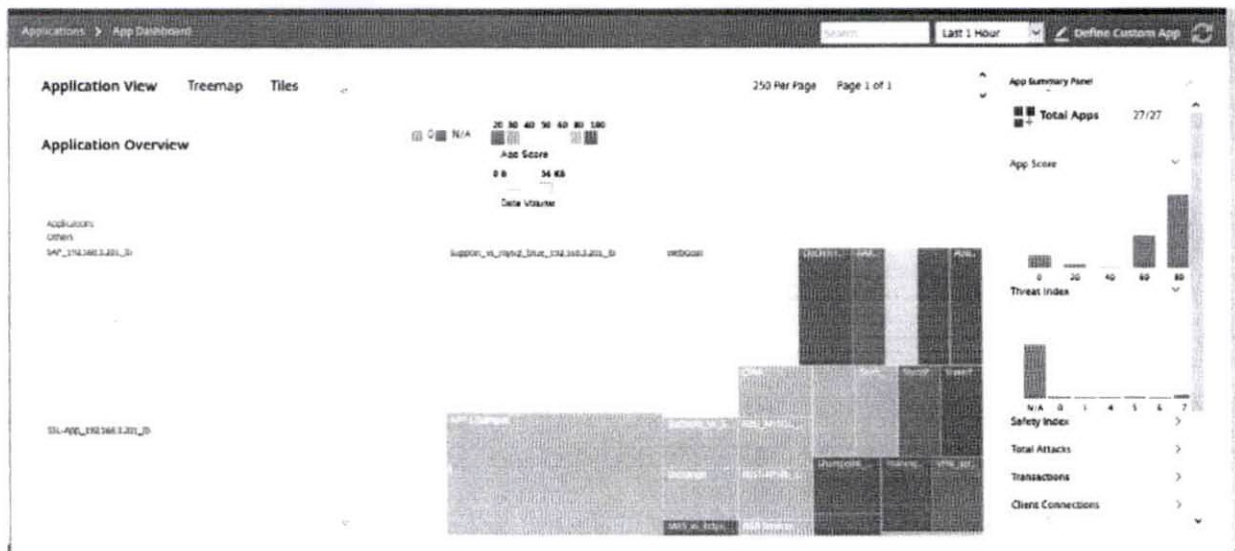


configuración del sistema, la administración de eventos, la administración del rendimiento y la administración de certificados SSL

## Citrix NetScaler MAS

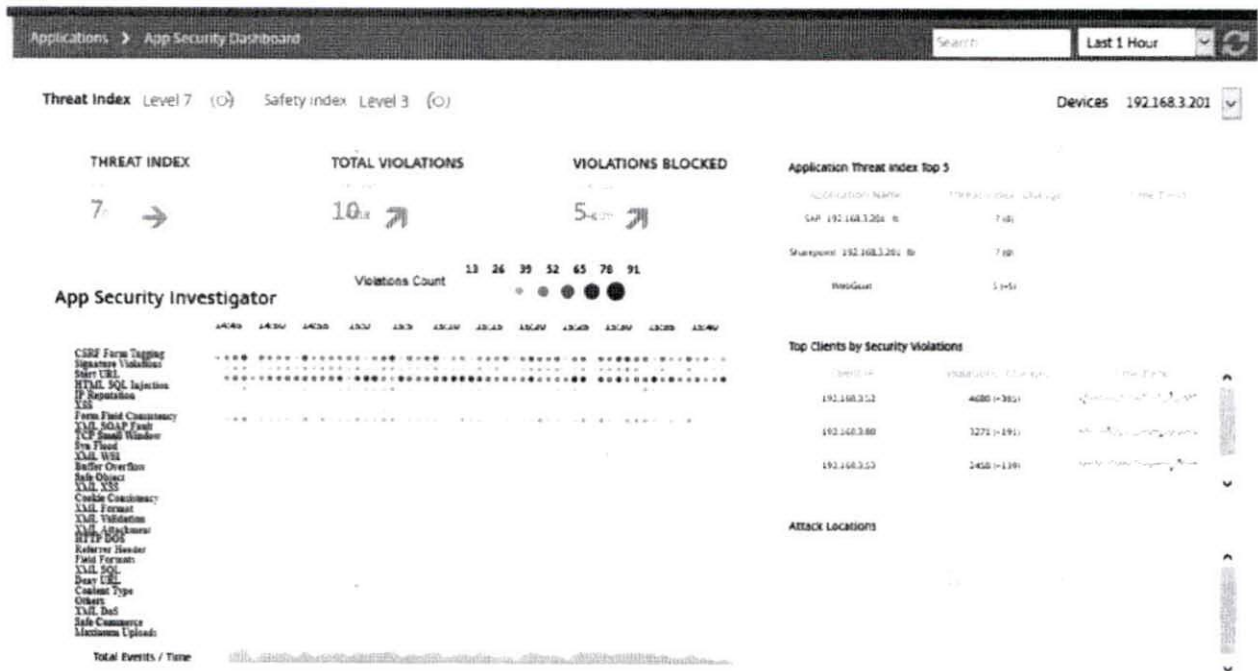
NetScaler Management and Analytics System (MAS) es una solución de administración centralizada que simplifica las operaciones proporcionando a los administradores visibilidad para toda la empresa y automatizando los trabajos de administración que deben ejecutarse en múltiples instancias. Puede administrar y supervisar los productos de redes de aplicaciones Citrix que incluyen Citrix NetScaler MPX, Citrix NetScaler VPX, Citrix NetScaler Gateway, Citrix NetScaler SDX, Citrix NetScaler CPX y Citrix NetScaler SD-WAN. Puede utilizar NetScaler MAS para administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una sola consola unificada. Desde un simple panel los administradores pueden visualizar, automatizar y administrar los servicios de NetScaler.

NetScaler MAS, un dispositivo virtual (Virtual Appliance) que se ejecuta en cualquier hipervisor de virtualización (Vmware, XenServer, etc). Aborda el desafío de visibilidad de las aplicaciones al recopilar información detallada sobre el tráfico de aplicaciones web y de escritorio virtual, como flujo, Los datos de rendimiento de página y la información de la base de datos que fluye a través de los dispositivos NetScaler, dispositivos NetScaler Gateway o dispositivos NetScaler SD-WAN en su sitio y proporciona informes ejecutables. Permite a los administradores de TI solucionar problemas y supervisar de forma proactiva los problemas de los clientes en cuestión de minutos.

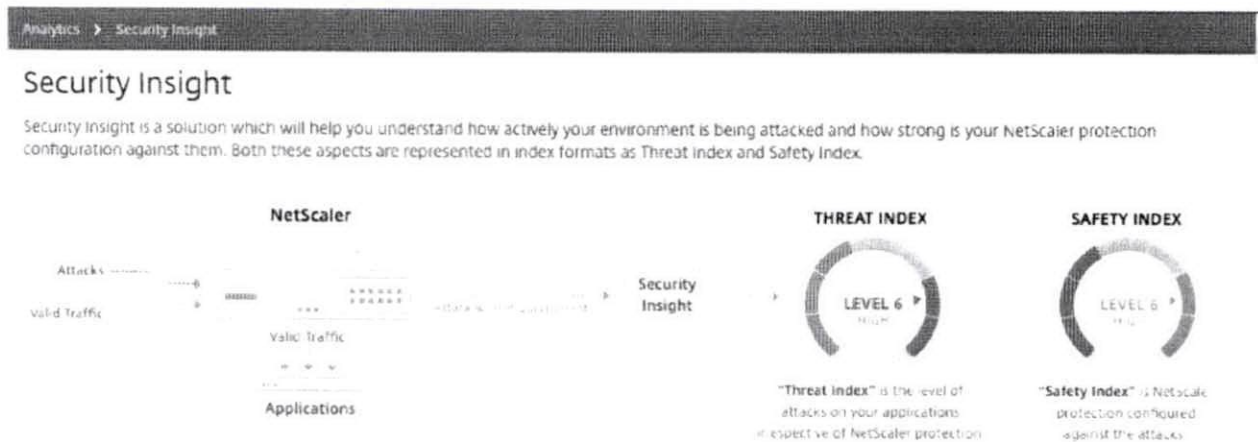


Visibilidad de las aplicaciones

MULTICOMPUTOS® S.R.L.  
optimizando el futuro juntos.  
Santo Domingo, R.D.



## APP Security Investigator

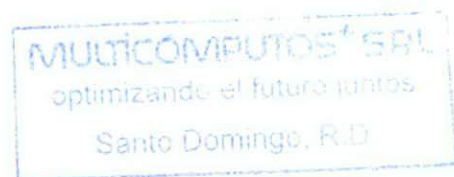


Welcome!

How to interpret these indexes?

High Threat Index and Low Safety Index combination assessment implies that your applications are being attacked actively and the protection configured on NetScaler is not as strong as it should be.

El módulo de Security Insight provee una capa de visibilidad y el índice de amenaza de nuestras aplicaciones. No solo podemos mitigar o detener una amenaza también podemos hacer configuraciones proactivas para prevenir incidentes de seguridad.



*Jorge*

# Sharepoint

1 Hour

18 August 2017 14:45:29 - 18 August 2017 15:45:29

## Application Summary

Total Violations  
4019

Violations By Severity  
Critical 2311

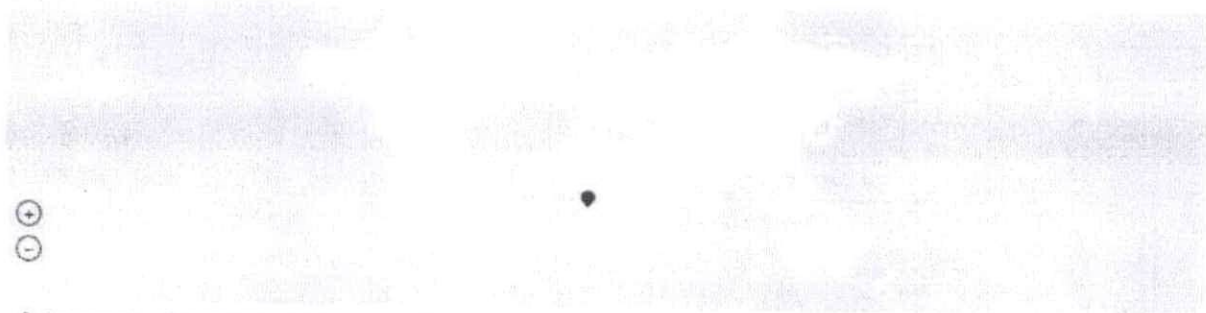
Violations By Action  
Blocked 3997

Violations By Category  
Cross-site Request Forgery 1525

TCP/HTTP Attacks  
0

Threat Index Level 7

Safety Index Level 6



Critical Attacks Medium Severity Attacks Low Severity Attacks

Security Check Violations

Level 6

Signature Violations

Level 6

IP Reputation

Level 7



Start URL ( 1,708 )  
1 / 2

Con el Mapa de la Geo localización podemos determinar de dónde se origina la amenaza y que tipo de amenaza.

MULTICOMPUTOS<sup>®</sup> SAL  
optimizando el futuro juntos  
Santo Domingo, R.D.

## Violations By Action

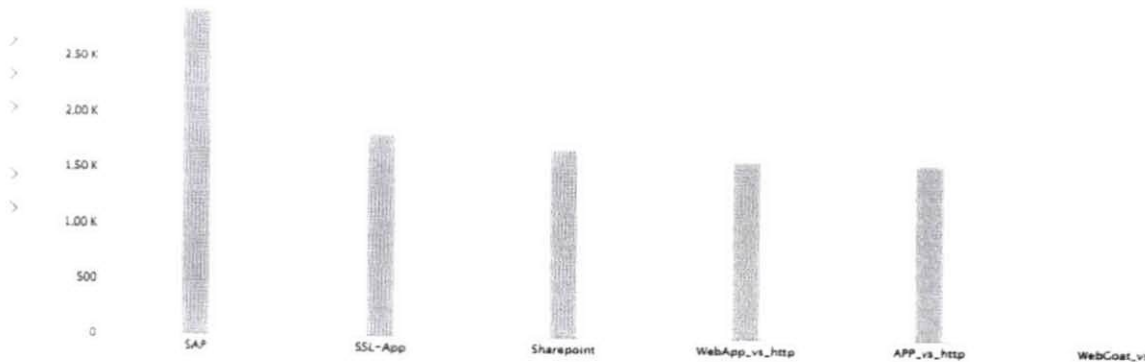
1 Hour

13 August 2017 14:46:15 - 13 August 2017 15:46:15



Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL
Aug 13 03:36 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:34 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:12 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:02 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:28 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:36 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:08 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 02:56 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:00 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:19 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo
Aug 13 03:09 PM	192.168.3.80	Start URL	Medium	Broken Authentication and Session Management	Blocked	http://192.168.3.68/bo

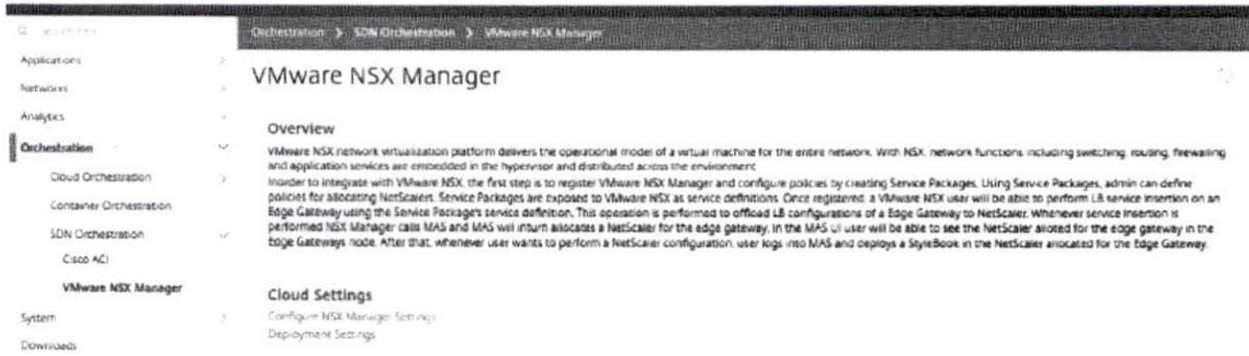
Podemos investigar incidentes de manera granular gracias a su codificación "Drill-Down".



Name	Hits	Bandwidth	Response Time
SAP	3.12 K	15.36 MB	998.07 ms
SSL-App	1.81 K	8.56 MB	36762.79 ms
Sharepoint	1.70 K	7.28 MB	649.52 ms
WebApp_vs_http	1.60 K	4.04 MB	761.18 ms
APP_vs_http	1.58 K	8.88 MB	4.12 ms
WebGoat_vs	1	1.45 KB	2.12 ms

Podemos medir el desempeño de nuestras aplicaciones, identificar rápidamente el mayor consumo entre cada una de las aplicaciones.





La plataforma de NetScaler MÁS se integra con cualquier plataforma de SDN.

## Configure Job



La plataforma de NetScaler MÁS puede automatizar las tareas en ventana de mantenimiento programadas, reduciendo el tiempo de interrupción de los servicios.

## NetScaler DataStream

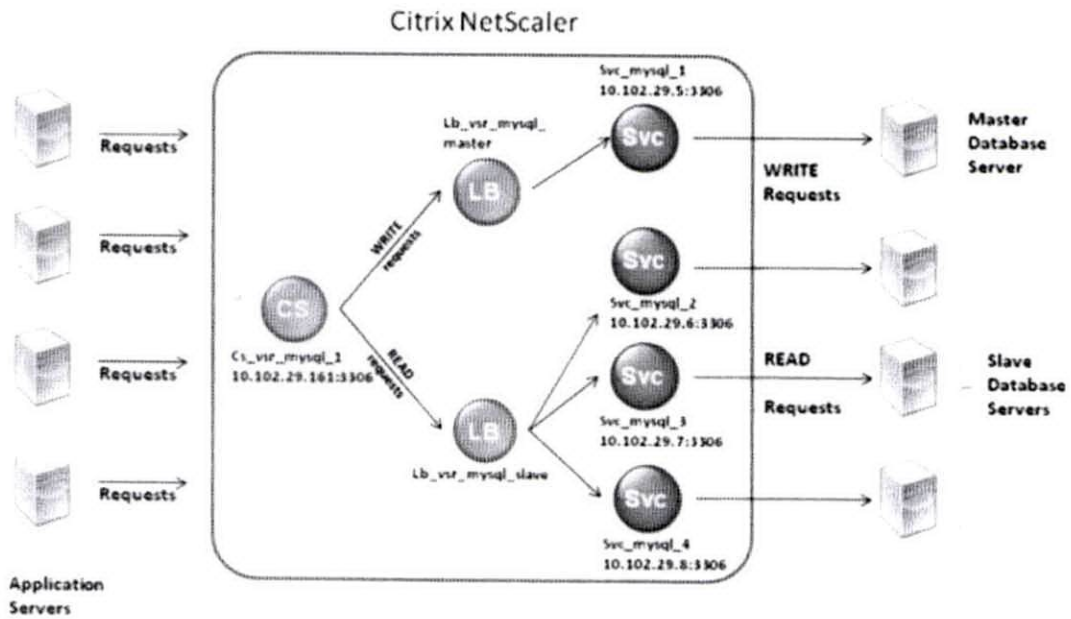
El DataStream es una funcionalidad única de Citrix NetScaler que provee mecanismo inteligente para distribuir tráfico en la capa de base de datos mediante la distribución de peticiones basadas en la consulta SQL que se envía

Cuando se despliega frente a servidores de bases de datos, NetScaler garantiza una distribución óptima del tráfico desde los servidores de aplicaciones y los servidores Web. Los administradores pueden segmentar el tráfico de acuerdo con la información en la consulta SQL y sobre la base de nombres de bases de datos, nombres de usuario, conjuntos de caracteres y tamaño de paquete.

La funcionalidad de DataStream puede balancear la carga para cambiar las peticiones a la base de datos basándose en algoritmos de balanceo de carga o elaborar los criterios de conmutación (switching) configurando el cambio de contenido para tomar una decisión basada en parámetros de consulta SQL. También puede configurar monitores para realizar un seguimiento del estado de los

servidores de base de datos. Actualmente esta funcionalidad solo esta soportada para base de datos MS-SQL y MySQL

U



MULTICOMPUTOS<sup>®</sup> S.R.L.  
optimizando el futuro juntos  
Santo Domingo, R.D.

## Cronograma de Trabajo

### Lote II – Balanceadores DMZ

Fases	Descripción	Entregables	Tiempo (hora/semanas)
Definición del proyecto	Realizar actividades de gestión de proyecto.	<ul style="list-style-type: none"> <li>Acuerdo de trabajo (SOW).</li> <li>Project Plan (cronograma de trabajo).</li> </ul>	24 horas
Planificación	<p>Realizar actividades propias de la naturaleza de la oferta presentada, análisis de los requerimientos.</p> <p>Diseñar la arquitectura de la oferta.</p> <p>Definir las políticas de optimización para las aplicaciones de JI</p> <p>Definir las ventanas de mantenimientos, esquema pruebas y fechas importantes.</p>	<ul style="list-style-type: none"> <li>Documento de ingeniería</li> <li>Topología de la arquitectura.</li> <li>Diagrama Topológico de la solución</li> </ul>	128 Horas
Despliegue	<p>Instalación física de los equipos</p> <p>Publicación de los servicios</p> <p>Configuración de la plataforma de analítica</p> <p>Configuración de esquema de alta disponibilidad</p>	<ul style="list-style-type: none"> <li>Puesta en operación del firewall del perímetro.</li> <li>Puesta en operación del firewall del Datacenter</li> </ul>	232 horas

*[Handwritten signature]*

	Configuración de protección para las aplicaciones  Perfiles de optimización para las aplicaciones		
Cierre del proyecto	Realizar actividades de cierre de proyecto.  Definición de la transición del proyecto a soporte.	• Memoria técnica	56 horas

### Equipo de Trabajo Multicómputos

En el listado abajo se encuentran los roles y principales actividades del equipo de Multicómputos.

- **Consultores del proyecto.** Los líderes del proyecto y consultores del mismo tienen la responsabilidad de la ejecución de las actividades diarias y pre-definidas en el documento de alcance. El rol de los consultores es planear y ejecutar las actividades de cada día y ajustar el plan de acuerdo con el progreso del proyecto. Los consultores son el contacto principal del cliente.
- **Gerente de Proyecto.** El Gerente de Proyecto proporciona supervisión del proyecto, centrándose en elementos integrales (en oposición a las actividades diarias de gerencia del proyecto - Project Manager) para facilitar la satisfacción del cliente y el éxito del proyecto. El gerente del proyecto normalmente trabaja con el Líder de Proyecto para definir el plan de trabajo en alto nivel para hacer frente a los elementos del proyecto críticos y a partir de entonces ejecutar el plan de trabajo por el equipo del proyecto.
- **Arquitecto de Solución.** El Arquitecto de Solución llevará a cabo un proceso de validación de los conceptos técnicos, recomendaciones, procedimientos y prácticas conducentes incluidos en todo el proyecto (configuraciones, entregas, etc.).



## Formulario de Presentación de Propuestas

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

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

Req. Num			
Requerimientos de Contratación (RDC).			
Acreditaciones y Experiencia del oferente			
Descripción		Solución Propuesta	Numero 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 <b>Application Delivery Controllers (ADCs)</b> 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.	Multicomputos tiene alrededor de una década ofreciendo la tecnología de Citrix NetScaler participando activamente los principales proyectos de entrega de aplicaciones en diferentes instituciones y empresas dominicanas, logrando altísimas distinciones por la experiencia brindada y el beneficio neto de la solución de NetScaler.	
RDC02	El Oferente debe contar con la Certificación del Fabricante para poder ofertar las soluciones de <b>Application Delivery Controllers (ADCs)</b> 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.	Multicomputos posee las credenciales autorizadas para distribuir y soportar cualquier plataforma de Citrix. Es importante destacar que somos "Gold Partner" de la marca, la cual nos distingue.	
RDC03	El oferente de contar con un personal Certificado por el fabricante en cada una de las soluciones <b>Application Delivery Controllers (ADCs)</b> y de cualquier otro equipo que esté contemplado en la propuesta de implementación.  Nota: Se debe presentar documentación que demuestre dicha capacidad y conocimiento.	Multicomputos Posee un personal calificado, con las más alta certificaciones de Citrix Networking.	
RDC04	Las Soluciones propuestas de <b>Application Delivery Controllers (ADCs)</b> deben estar dentro del Informe de Gardner, "Magic Quadrant for <b>Application Delivery Controllers</b> ", dentro del cuadrante de Líderes (Leaders). Dicho informe de referencia deberá ser	La Solución de Citrix NetScaler se encuentra en el cuadrante de líderes del informe de Gardner para solución de "Application Delivery Controller"	

	actualizado, es decir, debe ser la última publicación válida. Este documento debe ser anexo a la Propuesta.	Referencia: Informe de Gardner. Adjunto en 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.	Incluimos en nuestra oferta la el plan de configuración de los equipos.  Referencia: Ver cronograma de trabajo.
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.	La planificación del trabajo lleva una gestión de proyecto, que estará vigilante a que se cumpla todas las expectativas del proyecto, tomando en cuenta las ventanas de mantenimientos para no interrumpir las operaciones de la institución.
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).	Multicomputos cuenta el personal y la experiencia para llevar a cabo la implementación, eliminando la necesidad de contratar recursos externos.
<b>Tiempos de Entrega y de Implementación.</b>		
RDC08	El Oferente estará en la capacidad de aprovisionar (Entrega de Equipos) las soluciones de Application Delivery Controllers (ADCs) en un plazo no mayor a cuarenta y cinco (45) días calendario a partir de la firma del contrato.	Multicomputos, luego de firma del contrato, estará haciendo la gestión legal y aduanal para la entrega en el plazo conforme a lo estipulado en el proyecto.
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.	La experiencia y liderazgo de Multicomputos en la entrega de Citrix NetScaler nos permite entregar hasta en menor tiempo nuestra solución.
<b>Normas de Seguridad Industrial.</b>		
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.	La naturaleza de nuestra empresa, es de consultoría y manejo de información. La garantía de dicha información contempla acuerdos legales y de confidencialidad.

<b>Responsabilidades del Oferente</b>		
RDC12	<p>La presentación de las Propuestas debe cumplir con los siguientes requisitos:</p> <ul style="list-style-type: none"> <li>• Deben describir claramente la Marca y el Modelo ofertado.</li> <li>• Deben describir los detalles técnicos de todos los equipos presentados.</li> <li>• Las propuestas deberán ser presentadas en idioma español.</li> <li>• La propuesta presentada deberá describir (el # de Parte, Licencia, Protocolos, entre otros) con que se cumplirá cada requerimiento.</li> <li>• 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.</li> <li>• La Propuesta deben ser presentada en formato físico (Impreso) y en Formato digital (PDF)</li> <li>• El formato digital debe permitir realizar búsqueda dentro del documento (OCR).</li> <li>• Las Propuestas en formato digital deben venir en una Memoria USB libre de Virus.</li> </ul>	En nuestra oferta técnica describimos la solución de Citrix Netscaler. .
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.	En fecha del 11 julio participamos en la reunión aclaratoria y firmamos los acuerdos de responsabilidad para este proyecto.
<b>Requerimientos de Garantía y Soporte (RGS)</b>		
RGS01	Las Soluciones propuestas de <b>Application Delivery Controllers (ADCs)</b> 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 funcionalidades 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). <b>Nota:</b> Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con laJI.	Multicomputos incluye en su oferta de valor el soporte postventa para mantener la plataforma por el tiempo del contrato, incluyendo el equipo de servicios de profesionales para el acompañamiento durante todo el ciclo de la garantía del contrato en la puesta en operaciones de nuevas funcionalidades. Además, nos hacemos acompañar de todo el equipo de soporte para mantenimiento de la plataforma.
RGS02	El Software de Administración de las Soluciones propuestas de <b>Application Delivery Controllers (ADCs)</b> y cualquier otro equipo que esté contemplado en la propuesta de implementación contará con soporte (Actualizaciones de Software, Actualización de	Multicomputos incluye en su oferta de valor el soporte postventa para mantener la plataforma por el tiempo del contrato, incluyendo el equipo de servicios de profesionales para el acompañamiento durante todo el ciclo

	Hardware, Upgrade de Hardware y Software, Configuración de nuevas funcionalidades 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). <b>Nota:</b> Este soporte deberá contar con la participación del fabricante y el suplidor intermediario con la JI.	de la garantía del contrato en la puesta en operaciones de nuevas funcionalidades. Además, nos hacemos acompañar de todo el equipo de soporte para mantenimiento de la plataforma.	
RGS03	El periodo de vigencia de la garantía para las Soluciones propuestas de <b>Application Delivery Controllers (ADCs)</b> 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. <b>Nota:</b> 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.	Cumplimos con este requerimiento.	
RGS04	El Ciclo de vida (END OF LIFE) de las Soluciones propuestas de <b>Application Delivery Controller (ADCs)</b> 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 <b>Application Delivery Controller (ADCs)</b> . La propuesta debe incluir equipos de última generación del fabricante.	El equipo que estamos ofreciendo son equipos de última generación, dichos equipos cuentan con garantía de 5 años de ciclo de desarrollo de este producto. Luego de este periodo, el equipo tendrá una vigencia de tres años más, cubriendo soporte.	
RGS05	Vencida la Garantía después del 3er. año de adquisición de las Soluciones propuestas de <b>Application Delivery Controllers (ADCs)</b> 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%.	Cumplimos con este requerimiento, en el 4to 5 5to ano, mantendremos el costo de 15% del precio de lista de los equipos, con soporte de fabricante y garantía local de multicomputos.	

RGS06	El Fabricante y el Oferente de las Soluciones propuestas de <b>Application Deilvery Controllors (ADCs)</b> 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.	Multicomputos cuenta con un inventario de piezas disponibles para estos equipos.	
-------	---	--	--

**Requerimientos de Capacitación.**

RGS07	<p>Como parte de la propuesta el Oferente ofrecerá a la JI los siguientes tres (3) cursos para cinco (5) participantes:</p> <ul style="list-style-type: none"> <li>➢ Instalación, Configuración y Administración de los <b>Application Deilvery Controllors (ADCs)</b>. Para estas capacitaciones el oferente deberá tomar en cuenta los siguientes aspectos: <ul style="list-style-type: none"> <li>• Las capacitaciones deberán cubrir la implementación de políticas y mejores prácticas de acuerdo a la función y uso de los equipos.</li> <li>• Las capacitaciones serán realizadas de forma Presencial.</li> <li>• El oferente deberá proveer el salón, refrigerios, almuerzo, material de apoyo (En español), equipos Tecnológicos, entre otros.</li> <li>• Estas capacitaciones deberán ser impartidas en idioma español.</li> <li>• Estas capacitaciones deberán incluir las respectivas certificaciones para 5 participantes.</li> <li>• Adicional a los 5 participantes el oferente proveerá la facilidad de que la JI incluya participantes como oyente.</li> <li>• El calendario de las capacitaciones se realizará en coordinación con JI y estarán sujetos a la disponibilidad de la JI.</li> <li>• El oferente cubrirá con todos los costos de la capacitación.</li> <li>• 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.</li> </ul> </li> </ul> <p>Los instructores deberá ser docentes</p>	En nuestra propuesta incluimos la capacitación de la solución de Citrix NetScaler.	
-------	--	--	--

	<p>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 necesitará participación de los instructores Extranjeros.</p>		
--	---	--	--

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

**Requerimientos Funcionales y Técnicos (RFT)**

<b>Características Físicas y Rendimiento</b>			
Descripción	Solución Propuesta		Numero de partes
RFT01	<p>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.</p>	<p>El Netscaler MPX 8910 es un potente y moderno ADC que controla con inteligencia nuestra infraestructura y aplicaciones mejorando el desempeño de las mismas.</p> <p>Referencia: Netscaler Datasheet : <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf</a></p>	3016984-EZ
RFT02	<p>El equipo ofertado debe ser una plataforma de hardware de propósito específico denominado "Appliance".</p>	<p>El equipo ofertado posee una plataforma de hardware diseñado para realizar las funciones específicas de un Application Delivery Controller.</p> <p>Referencia: Netscaler Datasheet <a href="https://lac.citrix.com/products/netscaler-adc/netscaler-data-sheet.html">https://lac.citrix.com/products/netscaler-adc/netscaler-data-sheet.html</a></p>	3016984-EZ
RFT03	<p>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.</p>	<p>La solución ofertada cuenta con un software desarrollado para uso específico, con la finalidad de realizar balanceo de carga de servicios y aplicaciones basadas en IP y servicios Web.</p> <p>Referencia: Netscaler Datasheet <a href="https://lac.citrix.com/products/netscaler">https://lac.citrix.com/products/netscaler</a></p>	3016984-EZ

		<a href="https://lac.citrix.com/products/netScaler-er-adc/netScaler-data-sheet.html">er-adc/netScaler-data-sheet.html</a>	
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.	Los equipos ofertados cumplen y superan las expectativas de desempeños solicitadas.  Referencia: Netscaler Datasheet <a href="https://lac.citrix.com/products/netScaler-er-adc/netScaler-data-sheet.html">https://lac.citrix.com/products/netScaler-er-adc/netScaler-data-sheet.html</a>	3016984-EZ
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.	Los equipos ofertados cumplen y superan las expectativas de desempeño solicitadas. Además, permite la configuración de Alta disponibilidad en modo Activo-Activo / Activo-Pasivo.  Referencia: Netscaler Datasheet <a href="https://lac.citrix.com/products/netScaler-er-adc/netScaler-data-sheet.html">https://lac.citrix.com/products/netScaler-er-adc/netScaler-data-sheet.html</a> <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netScaler-data-sheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netScaler-data-sheet.pdf</a>	3016984-EZ
RFT06	Cada equipo debe cumplir con las siguientes características: <ul style="list-style-type: none"> <li>• La solución debe soportar un Throughput en L4 de al menos 10 Gbps.</li> <li>• La solución debe soportar un Throughput en L7 de al menos 10 Gbps.</li> <li>• La solución debe soportar un Throughput en SSL de al menos 10 Gbps.</li> <li>• La solución debe soportar una Compresión de Throughput de al menos 3.5 Gbps.</li> <li>• La solución deberá tener al menos 32 GB de Memoria.</li> <li>• La solución debe soportar al menos 1,400,000.00 Millones de peticiones en L7 HTTP requests/sec.</li> <li>• La solución de soportar al menos 13,000.00 Transacciones en SSL (SSL transactions/sec (2K key certificates)</li> <li>• La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA.</li> <li>• La solución de soportar al menos 6,000.00 Transacciones en ECDHE (ECDHE transactions/sec)</li> </ul>	Cada equipo cumple con las siguientes características: <ul style="list-style-type: none"> <li>• Soportan un Throughput en L4 10 Gbps.</li> <li>• Soportan un Throughput en L7 de 10 Gbps.</li> <li>• Soportan un Throughput en SSL de 10 Gbps.</li> <li>• Soportan una Compresión de Throughput de 3.5 Gbps.</li> <li>• Cuentan con 32 GB de Memoria.</li> <li>• Soportan 1,400,000.00 Millones de peticiones en L7 HTTP requests/sec.</li> <li>• Soportan 13,000.00 Transacciones en SSL (SSL transactions/sec (2K key certificates)</li> <li>• Soportan 10,000 de Conexiones Concurrentes SSL VPN / ICA.</li> <li>• Soportan 6,000.00 Transacciones en ECDHE (ECDHE transactions/sec)</li> </ul> Referencia:  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-">https://www.citrix.com/content/dam/citrix/en_us/documents/products-</a>	3016984-EZ

		<a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">solutions/netscaler-data-sheet-full.pdf</a>	
RFT07	<p>Cada equipo debe tener al menos las siguientes Interfaces de red:</p> <ul style="list-style-type: none"> <li>• 4x10GE SFP+ (4 puertos SFP+ de 10 Gbps (Transceivers Incluidos))</li> <li>• 6x10/100/1000 CU (con opción de conectividad de 1 Gbps cobre o fibra (Transceivers Incluidos)).</li> <li>• 2x1G For Management.</li> </ul> <p><b>Nota:</b> Además de lo anteriormente mencionado, estos equipos deben tener Soporte de Transceivers 10G SFP+: SR, LR;XFP</p>	<p>Cada equipo posee las siguientes Interfaces de red:</p> <ul style="list-style-type: none"> <li>• 4x10GE SFP+ (4 puertos SFP+ de 10 Gbps (Transceivers Incluidos))</li> <li>• 6x10/100/1000 CU (con opción de conectividad de 1 Gbps cobre o fibra (Transceivers Incluidos)).</li> <li>• 2x1G For Management.</li> </ul> <p>Además de lo anteriormente mencionado, estos equipos cuentan con Soporte de Transceivers 10G SFP+: SR, LR;XFP</p> <p>Referencia: Netscaler Datasheet</p> <p><a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a></p>	3016984-EZ
RFT08	Las interfaces de 10G deben soportar velocidades de 1G o 10G dependiendo el transceiver usado.	Las interfaces de 10G soportan velocidades de 1G a 10 G en función del transceiver utilizado.	3016984-EZ
RFT09	Cada equipo debe contar con fuentes de poder redundantes AC, entradas de voltaje de 100 a 240 VAC.	El equipo cuenta con fuentes de poder redundantes AC y entradas de voltaje 100 -240 full range.	3016984-EZ
RFT10	Los equipos deberán ser instalados en rack estándar de 19", máximo 1RU.	Los equipos serán instalados en rack estándar de 19", máximo 1RU.	No aplica
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.	Los dispositivos cuentan con la configuración de alta disponibilidad, estableciendo uno en modo activo y la otra unidad en modo pasivo (fail-over). El dispositivo en modo pasivo monitorea constantemente el activo, y en caso de fallo del adaptador, cable de red, canal de controladora o alimentación de fluido eléctrico, el dispositivo en modo activo recupera de forma inmediata y automática las sesiones del sistema.	3016984-EZ
		Referencia:	



		Netscaler (How High Availability Works) <a href="http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-configuration-mgmt-wrapper-con/ng-ha-intro-wrapper-con/ng-ha-how-it-works-con.html">http://docs.citrix.com/en-us/netscaler-gateway/10-5/ng-configuration-mgmt-wrapper-con/ng-ha-intro-wrapper-con/ng-ha-how-it-works-con.html</a>	
RFT12	Cada equipo debe incluir 32 GB de Memoria RAM mínimo	El equipo posee 32 GB de Memoria RAM.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
RFT13	Cada equipo debe incluir mínimo un Disco duro de 240 GB SSD.	Los dispositivos incluyen cada uno un Disco duro de estado sólido desmontable de 240 GB.  Referencia: Netscaler 8910 Docs  <a href="https://docs.citrix.com/en-us/netscaler/10-5/ns-gen-hardware-wrapper-10-con/ns-hardware-platforms-con/citrix-netscaler-mpx-8900.html">https://docs.citrix.com/en-us/netscaler/10-5/ns-gen-hardware-wrapper-10-con/ns-hardware-platforms-con/citrix-netscaler-mpx-8900.html</a>	3016984-EZ
RFT14	El oferente deberá especificar detalladamente las especificaciones técnicas de los equipos ofertados, a nivel de Hardware y Software. Ejemplo: <ul style="list-style-type: none"> <li>• Tipo de Memoria.</li> <li>• Cantidad de Memoria en GB.</li> <li>• Cantidad Slot de Memoria.</li> <li>• Capacidad máxima de Memoria Soportada.</li> <li>• Procesador.</li> <li>• Capacidad y Velocidad del procesador.</li> <li>• Marca del Procesador.</li> <li>• Cantidad de Núcleos del Procesador</li> <li>• Generación del Procesador.</li> <li>• Tipo de disco Duro (Sata, Sata III o Híbrido, SSD Etc.)</li> </ul>	En la propuesta técnica describimos los componentes del NetScaler.	3016984-EZ
RFT15	Debe soportar Clúster Activo/Activo entre dos o más plataformas, soportando diferentes modelos de hardware (no solamente del mismo modelo).	La solución permite configurar clúster entre múltiples equipos. Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
RFT16	La solución debe permitir configurar clúster entre más de dos equipos y permitir que sean	La solución es altamente escalable pues permite clustering de hasta 32	3016984-EZ

	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.	equipos.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	
RFT17	Para mejorar el rendimiento de la sincronización de configuración deberá poder sincronizar la configuración de manera incremental.	El equipo cuenta con tecnologías que garantizan un alto rendimiento de la sincronización de la configuración.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
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.	La tecnología incorporada en el Netscaler permite identificar cual es el dispositivo más óptimo para responder a las peticiones.	3016984-EZ
RFT19	La configuración será sincronizada entre todos los dispositivos del grupo pudiendo escoger si la sincronización se realiza de manera automática o manual.	Durante el proceso de sincronización de la configuración se selecciona un nodo para coordinación de la misma.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
<b>FUNCIONES DE ADMINISTRACION DE TRAFICO</b>			
RFT20	La solución debe realizar funciones de balanceo de tráfico a aplicaciones basadas en TCP/UDP, incluidos servicios web.	La solución está perfectamente diseñada para la realización del balanceo de tráfico a las aplicaciones basadas en TCP/UDP, incluyendo Servicios web.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-</a>	3016984-EZ

		<a href="#">howitworks-con.html</a>	
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.	El equipo permite definir una ip virtual donde los clientes realizan las solicitudes y este distribuye la carga entre los servidores.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-howitworks-con.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-howitworks-con.html</a>	3016984-EZ
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.	La solución será configurada con una arquitectura Full-Proxy, control de entrada y salida de conexiones, añadiendo así una capa de seguridad.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-howitworks-con.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-howitworks-con.html</a>	3016984-EZ
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.	Con la finalidad de prevenir la congestión de las conexiones el Netscaler tiene la capacidad de ir asignándole carga a los servidores nuevos de manera paulatina hasta que sean capaces de soportar más peticiones.	3016984-EZ
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.	El Dispositivo permite la hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida.	3016984-EZ
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: <ul style="list-style-type: none"> <li>• Round Robin.</li> <li>• Proporcional (Ratio).</li> <li>• Proporcional dinámico.</li> <li>• Respuesta más rápida.</li> </ul>	La solución permite controla el balanceo del tráfico según se especifique entre uno o varios tipos de algoritmos especializados de balanceo. Todos estos métodos se realizan de forma nativa sin necesidad de la configuración de por scripting. Los métodos soportados son:	3016984-EZ

	<ul style="list-style-type: none"> <li>• Conexiones minimas.</li> <li>• Menor número de sesiones.</li> <li>• Tendencia de menor cantidad de conexiones (observed).</li> <li>• Tendencia de desempeño (predictive).</li> </ul>	<ul style="list-style-type: none"> <li>• LEAST-CONNECTION</li> <li>• ROUND-ROBIN</li> <li>• LEAST-RESPONSE-TIME</li> <li>• URL-HASH</li> <li>• DOMAIN-HASH</li> <li>• DESTINATION-IP-HASH</li> <li>• SOURCE-IP-HASH</li> <li>• SRC-IP-DEST-IP-HASH</li> <li>• CALLID-HASH</li> <li>• SRC-IP-SRC-PORT-HASH</li> <li>• LEAST-BANDWIDTH</li> <li>• LEAST-PACKETS</li> <li>• CUSTOM-LOAD</li> <li>• TOKEN</li> <li>• LRTM</li> </ul> <p>Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-customizing-lbalgorithms-wrapper-con.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-customizing-lbalgorithms-wrapper-con.html</a></p>	
RFT26	Debe permitir balancear a una granja de servidores y seleccionar el destino basado en la carga de estos, como memoria/RAM	El método de balanceo Custom load balancing permite a los equipos balancer de acuerdo al uso de CPU, Memoria y tiempo de respuesta.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-customizing-lbalgorithms-wrapper-con/ns-lb-customizing-about-custom-con.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-customizing-lbalgorithms-wrapper-con/ns-lb-customizing-about-custom-con.html</a>	3016984-EZ
RFT27	El equipo debe no tener restricciones en el número de servicios virtuales que se pueden configurar (Virtual Servers, Virtual IP, granjas)	El Netscaler ADC no tiene limitaciones en el número de servicios virtuales configurables.	3016984-EZ
RFT28	El sistema debe ser capaz de identificar fallos en servicios para redundancia de las aplicaciones.	El Dispositivo realiza un monitoreo constante con el fin de identificar fallos en los servicios.  Referencia:	3016984-EZ

		Netscaler (Support) <a href="https://support.citrix.com/article/CTX134009">https://support.citrix.com/article/CTX134009</a>	
RFT29	La solución debe tener reglas que permitan el control de ancho de banda de manera dinámica.	La solución cuenta con reglar para controlar ancho de banda de manera dinámica.  Referencia: Netscaler (Support) <a href="https://support.citrix.com/article/CTX134009">https://support.citrix.com/article/CTX134009</a>	3016984-EZ
RFT30	La solución debe realizar monitoreo de la salud de los Servidores que gestione el equipo de Balanceo de tráfico, por medio de: <ul style="list-style-type: none"> <li>• Ping.</li> <li>• Chequeo a nivel de TCP y UDP a puertos específicos.</li> <li>• Monitoreo http y https.</li> <li>• Monitoreo del hardware y software mediante Windows Management Instrumentation (WMI) o mediante un sistema similar reconocido y aprobado por Microsoft.</li> <li>• Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos.</li> <li>• Ejecución de scripts para determinar la respuesta emulando un cliente.</li> <li>• Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red.</li> <li>• Monitoreos en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma.</li> <li>• Monitoreo de aplicaciones de mercado: <ul style="list-style-type: none"> <li>◦ LDAP</li> <li>◦ FTP</li> <li>◦ SMTP</li> <li>◦ IMAP/POP3</li> <li>◦ Oracle</li> <li>◦ MSSQL</li> <li>◦ MySQL</li> <li>◦ RADIUS</li> <li>◦ SIP</li> <li>◦ Protocolo SASP</li> <li>◦ SOAP</li> <li>◦ WMI</li> <li>◦ SNMP</li> </ul> </li> </ul>	El Dispositivo cuenta con novedosa tecnologías y métodos de monitoreo para asegurarse de la disponibilidad de los servicios y conexiones. Favor consultar referencia para revisar los detalles.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-monitors-builtin-con.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-monitors-builtin-con.html</a>	3016984-EZ
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: <ul style="list-style-type: none"> <li>• Dirección IP origen.</li> </ul>	El Nescaler permite configurar persistencias a las aplicaciones publicados a través de él, con los siguientes criterios: los siguientes: <ul style="list-style-type: none"> <li>• Dirección IP origen.</li> <li>• Dirección IP destino.</li> <li>• Cookies.</li> <li>• Hash.</li> <li>• Entre otros</li> </ul>	3016984-EZ

	<ul style="list-style-type: none"> <li>• Dirección IP destino.</li> <li>• Cookies.</li> <li>• Hash.</li> <li>• SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia.</li> <li>• Sesiones SSL.</li> <li>• Microsoft Remote Desktop.</li> <li>• Entre otros.</li> </ul>	Referencia:  <a href="http://docs.citrix.com/zh-cn/netscaler/12/load-balancing/load-balancing-persistence/persistence.html">http://docs.citrix.com/zh-cn/netscaler/12/load-balancing/load-balancing-persistence/persistence.html</a>	
RFT32	Debe Permitir crear persistencia por cualquier valor del paquete por medio de reglas.	El Netscaler permite la creación de persistencia sin importar el valor del paquete.	3016984-EZ
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.	La solución permite definir un servidor para responder solicitudes específicas.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-cs-wrapper-con-10.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-cs-wrapper-con-10.html</a>	3016984-EZ
RFT34	El sistema debe ser capaz de realizar un método secundario de persistencia, en caso de que el primer método no pueda ejecutarse por factores externos a la plataforma.	El sistema cuenta con un método alternativo de persistencia para casos en el que el método primario no pueda ejecutarse.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-persistence-wrapper-con/ns-lb-persistence-config-backup-persistence-tsk.html">http://docs.citrix.com/en-us/netscaler/10-1/ns-tmg-wrapper-10-con/ns-lb-wrapper-con-10/ns-lb-persistence-wrapper-con/ns-lb-persistence-config-backup-persistence-tsk.html</a>	3016984-EZ
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.	La solución soporta Scripts de programación para añadir múltiples funciones.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
RFT36	Soporte de API para construir aplicaciones de administración o monitoreo personalizadas: <ul style="list-style-type: none"> <li>• 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</li> </ul>	La solución está diseñada para soportar la incorporación de API's lo que le permite la capacidad de interactuar con todos los lenguajes citados en la descripción.	3016984-EZ

	(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	El netscaler es capaz de integrarse con API esto le permite trabajar de manera eficiente con el protocolo REST el que permite de manera facil asociarse a plataformas de automatización.  Referencia: <a href="https://www.citrix.com/blogs/2014/09/19/scripting-automating-netscaler-configurations-using-nitro-rest-api-and-powershell-part-1/">https://www.citrix.com/blogs/2014/09/19/scripting-automating-netscaler-configurations-using-nitro-rest-api-and-powershell-part-1/</a>	3016984-EZ
RFT38	Soporte de RESTful API	La Solución soporta RESTful API.  Referencia: <a href="http://docs.citrix.com/ko-kr/netscaler/11/nitro-api/nitro-rest.html">http://docs.citrix.com/ko-kr/netscaler/11/nitro-api/nitro-rest.html</a>	3016984-EZ
RFT39	La solución debe tener la capacidad de ampliarse para soportar la creación de alta disponibilidad entre Datacenters a través de GSLB.	La solución está diseñada para el posible crecimiento y además soporta la tecnología GSLB.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-5/ns-tmg-wrapper-10-con/netscaler-gslb-gen-wrapper-10-con.html">http://docs.citrix.com/en-us/netscaler/10-5/ns-tmg-wrapper-10-con/netscaler-gslb-gen-wrapper-10-con.html</a>	3016984-EZ
RFT40	La solución debe soportar la configuración de un portal de acceso unificado con capacidad de ofrecer n-factores de autenticación.	La solución puede ser configurada desde un portal unificado con capacidad de definir parámetros para autenticación.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ

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).	La solución permite 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).  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-5/ns-optimization-wrapper-10-con/ns-feo-con.html">http://docs.citrix.com/en-us/netscaler/10-5/ns-optimization-wrapper-10-con/ns-feo-con.html</a>	3016984-EZ
RFT42	Deberá ser posible modificar el contenido HTML utilizando objetos de configuración y sin necesidad de generar scripts.	La solución permite la modificación del contenido HTML utilizando objetos de configuración y sin necesidad de Generar scripts.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-5/ns-optimization-wrapper-10-con/ns-feo-con/ns-feo-working-use-case.html">http://docs.citrix.com/en-us/netscaler/10-5/ns-optimization-wrapper-10-con/ns-feo-con/ns-feo-working-use-case.html</a>	3016984-EZ
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.	La solución soporta el protocolo MQTT para administración de tráfico desde dispositivos IoT. Además, permite identificar mensajes dentro del protocolo MQTT, proveer estadísticas y exponer API para acceder a la Información de los mensajes MQTT.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/12/netscaler-extensions/netscaler-protocol-extensions/tutorial-examples.html">http://docs.citrix.com/en-us/netscaler/12/netscaler-extensions/netscaler-protocol-extensions/tutorial-examples.html</a>	3016984-EZ
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.	La solución soporta Scripts de programación para añadir múltiples funciones que no se encuentran por defecto.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ

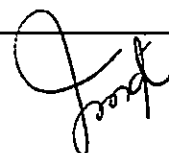


RFT46	El equipo debe ser compatible con tráfico IPSEC y ser certificado por ICSA Labs como dispositivo IPSEC.	El equipo es compatible con tráfico IPSEC y está certificado por ICSA Labs como dispositivo IPSEC.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
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	El ADC permite pueda tomar decisiones basado en una base de Datos de continentes, países y de direcciones IP.  Por otro lado, la base de datos de Geo localización debe incluye a los países de América Latina y está disponible en el mismo equipo sin necesidad de acceso a Internet (offline).  Referencia: Netscaler (Support Knowledge Center) <a href="https://support.citrix.com/article/CTX200332">https://support.citrix.com/article/CTX200332</a>	3016984-EZ

**FUNCIONES DE SEGURIDAD GENERALES**

RFT48	Cada equipo debe soportar seguridad SSL con las siguientes características: <ul style="list-style-type: none"> <li>Incluir el soporte de Aceleración SSL usando Hardware Dedicado</li> <li>Incluir mínimo 13,000.00 Transacciones por segundo SSL (2K Keys)</li> <li>Incluir mínimo 6,000.00 Transacciones concurrente de Curva elíptica (ECDHE)</li> <li>Soportar al menos 10 Gbps SSL (Throughput SSL)</li> <li>La solución debe soportar al menos 10.000 de Conexiones Concurrentes SSL VPN / ICA.</li> <li>Soporte de llaves SSL de 1024, 2048 y 4096 bits</li> </ul>	Cada equipo soporta seguridad SSL con las siguientes características: <ul style="list-style-type: none"> <li>Incluyen el soporte de Aceleración SSL usando Hardware Dedicado</li> <li>soportan 13,000.00 Transacciones por segundo SSL (2K Keys)</li> <li>soportan 6,000.00 Transacciones concurrente de Curva elíptica (ECDHE)</li> <li>Soportan 10 Gbps SSL (Throughput SSL)</li> <li>La solución soportan 10.000 de Conexiones Concurrentes SSL VPN / ICA.</li> <li>Soportan llaves SSL de 1024, 2048 y 4096 bits</li> </ul> Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
-------	---	---	------------

RFT49	La solución debe soportar mirroring de sesiones SSL. Sin el equipo primario falla el equipo secundario debe mantener la sesión SSL.	La solución soporta mirroring de sesiones SSL para que si el equipo primario falla el equipo secundario mantenga la sesión SSL.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/10-5.html">http://docs.citrix.com/en-us/netscaler/10-5.html</a>	3016984-EZ
RFT50	El Stack TLS del equipo debe soportar las siguientes funcionalidades/características <ul style="list-style-type: none"> <li>• Session ID.</li> <li>• Session Ticket.</li> <li>• OCSP Stapling (on line certificate status protocol).</li> <li>• Dynamic Record Sizing.</li> <li>• ALPN (Application Layer Protocol Negotiation).</li> <li>• Forward Secrecy.</li> </ul>	El Stack TLS del equipo soporta las siguientes funcionalidades/características: <ul style="list-style-type: none"> <li>• Session ID.</li> <li>• Session Ticket.</li> <li>• OCSP Stapling (on line certificate status protocol).</li> <li>• Dynamic Record Sizing.</li> <li>• ALPN (Application Layer Protocol Negotiation).</li> <li>• Forward Secrecy.</li> </ul> Referencia: Netscaler Docs <a href="http://docs.citrix.com/ja-ip/netscaler/11/system/http-configurations/configuring-http2.html">http://docs.citrix.com/ja-ip/netscaler/11/system/http-configurations/configuring-http2.html</a>	3016984-EZ
RFT51	La solución debe manejar AES, AES-GCM, SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman, Digital Signature Algorithm (DSA) y Elliptic Curve Cryptography (ECDHE).	La solución maneja de forma óptima, AES, AES-GCM, SHA1/MD5 y soporta algoritmos de llave pública: RSA, Diffie Hellman, Digital SignatureAlgorithm (DSA) y Elliptic Curve Cryptography (ECDHE).  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
RFT52	El equipo o sistema operativo debe estar certificado por ICSA Labs como Firewall de Red (Corporate Firewall). Nota: Debe Agregar certificación.	El NetScaler es un dispositivo de propósito de garantizar optimización, alta disponibilidad y seguridad para las aplicaciones web. Y precisamente sobre este último, el Netscaler incluye un Web Application Firewall reconocido como uno de los equipos con más alta	3016984-EZ



		<p>eficacia en detección de amenaza, conforme a NSS LABS.</p> <p>Como el NetScaler es un equipo diseñado para garantizar la optimización y la seguridad de las aplicaciones, delega la tarea de inspección de tráfico en capa 3 (firewall red) a otros equipos dedicados para esos propósitos. Por lo tanto, la inspección de capa 3 es una característica de los firewalls.</p>	
RFT53	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.	<p>El sistema operativo está certificado por ICSA Labs como Web Application Firewall.</p> <p>Referencia: Certificación</p> <p><a href="https://www.icsalabs.com/sites/default/files/Citrix_WAF_20160506_Report.pdf">https://www.icsalabs.com/sites/default/files/Citrix_WAF_20160506_Report.pdf</a></p> <p>ICSA <a href="https://www.icsalabs.com/product/citrix-netscaler-appfirewall">https://www.icsalabs.com/product/citrix-netscaler-appfirewall</a></p>	3016984-EZ
RFT54	Cada equipo debe incluir protección contra ataques de DDoS de mínimo 2,500,000.00 SYN/sec	<p>El Netscaler incluye configuraciones de para mitigar y proteger ataques de DDoS. Con la configuración de rate limiting, DDoS protection y Syn Cookie podemos detener ataques de más 2,500,0000 Syn/Sec.</p> <p><a href="https://support.citrix.com/article/CTX131681">https://support.citrix.com/article/CTX131681</a></p>	3016984-EZ
RFT55	Firmado criptografico de cookies para verificar su integridad.	<p>El dispositivo permite el firmado criptográfico de cookies para verificar su integridad.</p> <p>Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/11/security/ns-httpdosp-wrapper-con-10/ns-syn-dos-protection-">http://docs.citrix.com/en-us/netscaler/11/security/ns-httpdosp-wrapper-con-10/ns-syn-dos-protection-</a></p>	3016984-EZ

		<a href="http://con.html?_ga=2.50709289.1204929635.1500380218-1240731058.1499172359">con.html?_ga=2.50709289.1204929635.1500380218-1240731058.1499172359</a>	
RFT56	Capacidad de integración con dispositivos HSM "Hardware Security Module" (Módulo de Seguridad Hardware) externos. Deberá soportar al menos ThalesnShield Y Safenet (Gemalto) Luna.	La Solución posee capacidad de integración con dispositivos HSM "Hardware Security Module" (Módulo de Seguridad Hardware) externos. Además, soporta ThalesnShield Y Safenet (Gemalto) Luna.  Referencia: Netscaler Docs <a href="https://docs.citrix.com/en-us/netscaler/10-5/ns-tmg-wrapper-10-con/ns-ssl-wrapper-con-10/support-for-thales-con.html">https://docs.citrix.com/en-us/netscaler/10-5/ns-tmg-wrapper-10-con/ns-ssl-wrapper-con-10/support-for-thales-con.html</a>	3016984-EZ
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 tráfico SSL sin que el balanceador termine la sesión SSL.	La solución permite la funcionalidad de Proxy SSL.  Referencia: Netscaler Docs <a href="https://docs.citrix.com/en-us/netscaler-gateway/12/vpn-user-config/configure-plugin-connections/ng-plugin-enable-proxy-support-tsk.html">https://docs.citrix.com/en-us/netscaler-gateway/12/vpn-user-config/configure-plugin-connections/ng-plugin-enable-proxy-support-tsk.html</a>	3016984-EZ
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.	La solución soporta la extensión STARTTLS para el protocolo SMTP.  Referencia: Netscaler Docs <a href="https://docs.citrix.com/en-us/netscaler/12/ssl/other-tcp-protocols.html">https://docs.citrix.com/en-us/netscaler/12/ssl/other-tcp-protocols.html</a>	3016984-EZ
RFT59	Debe soportar HSTS (HTTP Strict Transport Security).	La solución soporta HSTS (HTTP Strict Transport Security).  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/12/ssl/ssl-support-for-hsts.html">http://docs.citrix.com/en-us/netscaler/12/ssl/ssl-support-for-hsts.html</a>	3016984-EZ
RFT60	Debe soportar por medio de agregación de suscripción a futuro, un sistema de reputación	La solución centra con IP reputación lo que permite que el dispositivo pueda	3016984-EZ

	<p>IP para prevenir conexiones bidireccionales (entrantes y salientes) a direcciones IP no confiables y agrupadas en categorías.</p> <ul style="list-style-type: none"> <li>• Scanners</li> <li>• Exploits Windows</li> <li>• Denial of Service</li> <li>• Proxies de Phishing</li> <li>• Botnets</li> <li>• Proxies anónimos</li> </ul>	<p>identificar la direcciones ip que están enviando solicitudes no deseadas. La categoria de las amenazas son:</p> <ul style="list-style-type: none"> <li>• SPAM_SOURCES,</li> <li>• WINDOWS_EXPLOITS,</li> <li>• WEB_ATTACKS,</li> <li>• BOTNETS,</li> <li>• SCANNERS,</li> <li>• DOS,</li> <li>• REPUTATION,</li> <li>• PHISHING,</li> <li>• PROXY,</li> <li>• NETWORK,</li> <li>• CLOUD_PROVIDERS</li> <li>• MOBILE_THREATS.</li> </ul> <p>Referencia: Netscaler Docs  <a href="http://docs.citrix.com/en-us/netscaler/12/reputation/ip-reputation.html">http://docs.citrix.com/en-us/netscaler/12/reputation/ip-reputation.html</a></p>	
--	--	---	--

**FUNCIONES DE ACCELERACION DE TRAFICO**

<p><b>RFT61</b></p>	<p>La implementación de la solución debe incluir la capacidad de hacer aceleración de aplicación a nivel de:</p> <ul style="list-style-type: none"> <li>• Memoria cache.</li> <li>• Compresión tráfico HTTP</li> <li>• Optimización de conexiones a la aplicación a nivel TCP</li> <li>• Multiplexación de conexiones hacia los servidores</li> </ul>	<p>La solución es de hacer aceleración de aplicación a nivel de:</p> <ul style="list-style-type: none"> <li>• Memoria cache.</li> <li>• Compresión tráfico HTTP</li> <li>• Optimización de conexiones a la aplicación a nivel TCP</li> <li>• Multiplexación de conexiones hacia los servidores.</li> </ul> <p>Referencia:  Netscaler Docs  <a href="http://docs.citrix.com/en-us/netscaler/12/optimization.html">http://docs.citrix.com/en-us/netscaler/12/optimization.html</a></p>	<p>3016984-EZ</p>
<p><b>RFT62</b></p>	<p>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.</p>	<p>El sistema permite comprimir tráfico http a través del estándar GZIP y compatible con browsers como MS Internet Explorer, Edge, Google Chrome, Mozilla Firefox, Safari, etc.</p> <p>Referencia:  Netscaler Docs  <a href="http://docs.citrix.com/en-us/netscaler/12/optimization/http-compression.html">http://docs.citrix.com/en-us/netscaler/12/optimization/http-compression.html</a></p>	<p>3016984-EZ</p>

RFT63	Cada equipo debe contar con una capacidad de compresión de tráfico a una tasa de 3.5 Gbps o superior	Los equipos cuenta con capacidad de compresión de tráfico a una tasa de 3.5 Gbps.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet-full.pdf</a>	3016984-EZ
RFT64	Debe soportar el protocolo SPDY y funcionar como Gateway SPDY aun cuando los servidores Web no soporten esta característica.	Los Dispositivos soportan el protocolo SPDY y funcionan como Gateway SPDY aun cuando los servidores Web no soporten esta característica.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/12.html">http://docs.citrix.com/en-us/netscaler/12.html</a>	3016984-EZ
RFT65	Debe soportar el protocolo HTTP y funcionar como Gateway para este protocolo.	La solución soporta el protocolo HTTP y puede funcionar como Gateway para este protocolo.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/12.html">http://docs.citrix.com/en-us/netscaler/12.html</a>	3016984-EZ
<b>FIREWALL DE APLICACIONES WEB (WAF)</b>			
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).	La solución funciona como Firewall de Aplicaciones (WAF) sin necesidad de otro equipo.  Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT68	El equipo o sistema operativo debe estar certificado por ICSA Labs como Web Application Firewall. Nota: Debe Agregar certificación.	El sistema operativo está certificado por ICSA Labs como Firewall de Red.  Referencia: Certificación <a href="https://www.icsalabs.com/sites/default">https://www.icsalabs.com/sites/default</a>	3016984-EZ

		<p><a href="#">t/files/Citrix WAF 20160506 Report.pdf</a></p> <p>ICSA  <a href="https://www.icsalabs.com/product/citrix-netscaler-appfirewall">https://www.icsalabs.com/product/citrix-netscaler-appfirewall</a></p>	
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.	<p>La funcionalidad de WAF permite la personalización de las políticas.</p> <p>Referencia:  Netscaler Docs  <a href="http://docs.citrix.com/ia-&lt;br/&gt;ip/netscaler/11/security/application-firewall.html">http://docs.citrix.com/ia- ip/netscaler/11/security/application-firewall.html</a></p>	3016984-EZ
RFT70	Debe trabajar en un esquema proxy TCP Reverso y/o Transparente.	<p>El equipo trabaja en un esquema proxy TCP Reverso y/o Transparente.</p> <p>Referencia: Firewall de Aplicaciones Web.</p> <p>Referencia:  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT71	Debe soportar la creación automática de políticas	<p>Un avanzado motor de aprendizaje determina automáticamente el Comportamiento esperado de las aplicaciones web empresariales y genera políticas recomendadas.</p> <p>Referencia:  Firewall de Aplicaciones Web.</p> <p><a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
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.	<p>Para proteger completamente sus importantes propiedades web, el equipo proporciona protección a través de todas las capas de la cadena informática, desde la red y servicios y protocolos de la capa de aplicación hasta las aplicaciones de</p>	3016984-EZ

		<p>infraestructuras.</p> <p>Referencia:          Firewall de Aplicaciones Web  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	
RFT73	La creación automática de políticas deberá unificar múltiples URLs explícitas utilizando wildcards de manera de reducir la cantidad de objetos en la configuración.	<p>El WAF permite la unificación de políticas con la finalidad de reducir la cantidad de objetos en la configuración.</p> <p>Referencia:          Firewall de Aplicaciones Web  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT74	Debe trabajar en modo de bloqueo o en modo informativo	<p>El Dispositivo es capaz de trabajar en modo de bloqueo o en modo informativo.</p> <p>Referencia:          Firewall de Aplicaciones Web  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT75	Debe permitir diferentes políticas de seguridad para diferentes aplicaciones	<p>La solución permite definir políticas de seguridad para distintas aplicaciones.</p> <p>Referencia:          Firewall de Aplicaciones Web  <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT76	Debe permitir la creación de firmas personalizadas	<p>La solución permite la creación de firmas personalizadas con el fin mitigar</p>	3016984-EZ



		<p>la posibilidad de infección de los sistemas.</p> <p>Referencia: Firewall de Aplicaciones Web</p> <p><a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	
RFT77	Debe trabajar con modelos de seguridad positiva y negativa	<p>El WAF está diseñado para evitar los posibles eventos de falsos positivos y falsos negativos.</p> <p>Referencia: Firewall de Aplicaciones Web</p> <p><a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT78	Debe poder aprender el comportamiento de la aplicación automáticamente sin intervención humana.	<p>Un avanzado motor de aprendizaje determina automáticamente el comportamiento esperado de las aplicaciones web empresariales y genera políticas recomendadas legibles por el ser humano.</p> <p>Referencia: Firewall de Aplicaciones Web</p> <p><a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT79	Debe permitir personalizar las páginas de bloqueo incluyendo la capacidad de responder a webservices mediante un código HTTP 500.	<p>Bloquear ataques que explotan vulnerabilidades en propiedades de web personalizadas.</p> <p>Referencia:</p>	3016984-EZ

		Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a>	
RFT80	El WAF debe permitir personalizar las páginas de bloqueo	El WAF permite la personalización de las páginas de bloqueo. Referencia: <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-nginx-appfirewall.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-nginx-appfirewall.pdf</a>	3016984-EZ
RFT81	Debe prevenir exponer el "OS fingerprinting"	A través de política de rewrite y responde podemos evitar "OS Fingerprinting"	3016984-EZ
RFT82	Debe permitir la integración con Herramientas de verificación de vulnerabilidades, en particular WhiteHat, Cenxic, Qualys, IBM AppScan, HP WebInspect.	El Waf contiene una amplia cantidad de firmas que le permiten protegerse contra de las amenazas de L7 y HTTP. El Firewall la integración de aplicaciones de terceros para la escaneo de amenazas tales como , WhiteHat, Cenxic, Qualys, IBM AppScan, HP WebInspect.  Referencia: <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-nginx-appfirewall.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-nginx-appfirewall.pdf</a>	3016984-EZ
RFT83	El WAF Debe soportar: <ul style="list-style-type: none"> <li>• Restringir protocolo y versión utilizada.</li> <li>• Multi-byte language encoding.</li> <li>• Validar URL-encoded characters.</li> <li>• Restringir la longitud del método de request.</li> <li>• Restringir la longitud del URI solicitado.</li> <li>• Restringir el número de Encabezados (headers).</li> <li>• Restringir la longitud del nombre de los encabezados.</li> <li>• Restringir la longitud del valor de los encabezados.</li> </ul>	El WAF cumple y soporta las siguientes funcionalidades: <ul style="list-style-type: none"> <li>• Restringir protocolo y versión utilizada.</li> <li>• Multi-byte language encoding.</li> <li>• Validar URL-encoded characters.</li> <li>• Restringir la longitud del método de request.</li> <li>• Restringir la longitud del URI solicitado.</li> <li>• Restringir el número de Encabezados (headers).</li> <li>• Restringir la longitud del nombre de</li> </ul>	3016984-EZ

	<ul style="list-style-type: none"> <li>• Restringir la longitud del cuerpo (body) de la solicitud.</li> <li>• Restringir la longitud del nombre y el valor de las cookies.</li> <li>• Restringir el número de cookies.</li> <li>• Restringir la longitud del nombre y valor de los parámetros.</li> <li>• Restringir el número de parámetros.</li> </ul>	los encabezados. <ul style="list-style-type: none"> <li>• Restringir la longitud del valor de los encabezados.</li> <li>• Restringir la longitud del cuerpo (body) de la solicitud.</li> <li>• Restringir la longitud del nombre y el valor de las cookies.</li> <li>• Restringir el número de cookies.</li> <li>• Restringir la longitud del nombre y valor de los parámetros.</li> <li>• Restringir el número de parámetros.</li> </ul>	
RFT84	El WAF Debe incluir protección a Web Services XML y restringir el acceso a métodos definidos vía Web Services Description Language (WSDL)	El WAF incluye protección a Web Services XML y restringe el acceso a métodos definidos vía Web Services Description Language (WSDL).  Referencia:  Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT85	El WAF debe incluir protección contra el Top 10 de ataques definidos en OWASP.	El dispositivo permite protección contra el Top 10 definido por OWASP. Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT86	El WAF debe incluir protección contra Web Scraping.	Podemos configurar políticas de protección contra Web Scraping utilizando los siguientes métodos: <ul style="list-style-type: none"> <li>• specific cookies</li> <li>• response methods like captcha</li> <li>• user agent is valid</li> <li>• rate of requests</li> </ul> Referencia:  <a href="https://www.citrix.com/blogs/2011/09/18/scrapers-and-bots-how-to-tame-them-with-netscaler/">https://www.citrix.com/blogs/2011/09/18/scrapers-and-bots-how-to-tame-them-with-netscaler/</a>	3016984-EZ
RFT87	Debe ser Session-aware es decir identificar y	El NetScaler posee diferente para	3016984-EZ

	forzar que el usuario tenga una sesión e identificar los ataques por usuario.	forzar la autenticación legítima de un usuario. Y con la plataforma de visibilidad podemos identificar las acciones violatorias desde una sesión de un 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).	La solución permite definir y detectar 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).  Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT89	Debe permitir verificar las firmas de ataque en las respuestas del servidor al usuario	El análisis de firmas es uno de los mecanismos utilizados por el equipo para detección de amenazas.  Referencia: Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a>	3016984-EZ
RFT90	Debe permitir el enmascaramiento de información sensible filtrada por el servidor	El dispositivo oculta dinámicamente la información sensible de la respuesta del servidor, para que esta no pueda ser utilizada por atacantes.  Referencia: Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a>	3016984-EZ
RFT91	Debe poder bloquear basado en la ubicación geográfica e incluir la base de datos de	El ADC nos permite construir nuestra base de datos para aplicar políticas	3016984-EZ

	Geolocalización.	<p>basadas en ubicación geográfica. Esto con el fin de bloquear e identificar el origen de los ataques.</p> <p>Referencia: Citrix support center <a href="https://support.citrix.com/article/CTX200332">https://support.citrix.com/article/CTX200332</a></p>	
RFT92	Debe permitir la integración con servidores Antivirus.	<p>El dispositivo permite la integración de servidores de antivirus.</p> <p>Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler/12.html">http://docs.citrix.com/en-us/netscaler/12.html</a></p>	3016984-EZ
RFT93	Debe brindar reportes respecto a la normativa PCI DSS 3.1 MINIMO.	<p>La solución esta en cumplimiento con la normativa PCI DSS 6.6</p> <p>Referencia: Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT94	Debe proteger contra ataque DoS /DDoS de Capa 4 Y 7.	<p>El dispositivo asegura el sistema en contra de ataques DoS /DDoS de Capa 4 Y 7.</p> <p>Referencia: Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a></p>	3016984-EZ
RFT95	Una vez detectado un ataque deberá ser posible descartar todos los paquetes que provengan de una dirección IP sospechosa.	<p>El equipo protege conforme a política de negación, de prevención y aísla toda IP relacionada a un ataque.</p> <p>Referencia: Netscaler Docs. <a href="http://docs.citrix.com/en-">http://docs.citrix.com/en-</a></p>	3016984-EZ

		<a href="http://us/netscaler/11-1/reputation.html">us/netscaler/11-1/reputation.html</a>	
RFT96	En caso de detectarse un ataque se requiere tener la posibilidad de iniciar una captura de tráfico para poseer información forense.	Este WAF nos permite inspeccionar de manera minuciosa los paquetes que estén relacionados a un ataque.  Referencia: Netscaler Docs. <a href="http://docs.citrix.com/en-us/netscaler/11-1/security.html">http://docs.citrix.com/en-us/netscaler/11-1/security.html</a>	3016984-EZ
RFT97	Debe soportar tecnologías AJAX y JSON .	La solución soporta las tecnologías AJAX y JSON.  Referencia: Netscaler Docs. <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
RFT98	Debe proteger como mínimo: <ul style="list-style-type: none"> <li>• Ataques de Fuerza Bruta.</li> <li>• Cross-site scripting (XSS).</li> <li>• Cross Site Request Forgery.</li> <li>• SQL injection.</li> <li>• Parameter and HPP tampering.</li> <li>• Sensitive information leakage.</li> <li>• Session high jacking.</li> <li>• Buffer overflows.</li> <li>• Cookie manipulation.</li> <li>• Various encoding attacks.</li> <li>• Broken access control.</li> <li>• Forceful browsing.</li> <li>• Hidden fields manipulation.</li> <li>• Requests mugging.</li> <li>• XML bombs/DoS.</li> </ul>	El equipo protege efectivamente la red de ataques como: Debe proteger como mínimo: <ul style="list-style-type: none"> <li>• Ataques de Fuerza Bruta.</li> <li>• Cross-site scripting (XSS).</li> <li>• Cross Site Request Forgery.</li> <li>• SQL injection.</li> <li>• Parameter and HPP tampering.</li> <li>• Sensitive information leakage.</li> <li>• Session high jacking.</li> <li>• Buffer overflows.</li> <li>• Cookie manipulation.</li> <li>• Various encoding attacks.</li> <li>• Broken access control.</li> <li>• Forceful browsing.</li> <li>• Hidden fields manipulation.</li> <li>• Requests mugging.</li> <li>• Open Redirect. • XML bombs/DoS.</li> </ul> Referencia: Firewall de Aplicaciones Web <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a>  Netscaler Docs	3016984-EZ

		<a href="http://docs.citrix.com/en-us/netscaler/12.html">http://docs.citrix.com/en-us/netscaler/12.html</a>	
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.	La protección Dinámica permite la identificación y configuración de URLs que generen un alto consumo de recursos en los servidores, para así garantizar la protección de ataques de DoS.	3016984-EZ
RFT100	Debe permitir verificaciones de seguridad y validación a protocolos FTP y SMTP	El equipo valida la legitimidad de protocolos como SMTP, FTP, HTTP, entre otros.	3016984-EZ
RFT101	Debe permitir comparar dos políticas de seguridad y mostrar las diferencias entre ambas	El NetScaler incluye la funcionalidad de comparación de configuración.	3016984-EZ
RFT102	Debe incluir firmas de BOTS para detectar y bloquear tráfico originado por estos.	Con la ayuda de IP reputation el dispositivo puede fácilmente detectar la dirección IP origen que está enviando tráfico no deseado	3016984-EZ
RFT103	Debe soportar CAPTCHA como método de prevención para mitigar ataques de denegación hacia las aplicaciones protegidas.	Dentro de los métodos de verificación de solicitudes legítimas utilizado por el WAF se encuentra CAPTCHA.  Referencia: Citrix support <a href="https://support.citrix.com/article/CTX216091">https://support.citrix.com/article/CTX216091</a>	3016984-EZ
RFT104	Debe ofrecer protección sobre tráfico basado en Web Sockets.	El dispositivo asegura las comunicaciones Full duplex TCP entre los clientes y los servidores.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/zh-tw/netscaler/11/system/http-configurations.html">http://docs.citrix.com/zh-tw/netscaler/11/system/http-configurations.html</a>	3016984-EZ
RFT105	El WAF debe identificar de manera única a los usuarios por medio de Fingerprint del navegador (Browser Fingerprint) y haciendo tracking del dispositivo.	El dispositivo identifica los certificados insertados en el header HTTP.  Referencia: Netscaler Docs <a href="https://docs.citrix.com/en-us/netscaler/12/ssl/config-ssl-actions-policies/config-ssl-based-hdr-insertion.html">https://docs.citrix.com/en-us/netscaler/12/ssl/config-ssl-actions-policies/config-ssl-based-hdr-insertion.html</a>	3016984-EZ
RFT106	Debe proteger las aplicaciones contra ataques de denegación de servicio a nivel de	La solución mitiga de manera efectiva	3016984-EZ

	L4 y L7	los ataques de DoS a nivel de L4 y L7.  Referencia: Netscaler WAF <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/web-application-firewall-delivering-must-have-protection-for-the-modern-enterprise-es.pdf</a>	
<b>ESTÁNDARES DE RED</b>			
RFT107	Soporte VLAN 802.1q, Vlantagging.	Soporte de VLAN 802.1q, Vlantagging.  Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT108	Soporte de 802.3ad para definición de múltiples troncales	Soporte de Link Aggregation 802.3ad.  Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT109	Soporte de NAT, SNAT	La Solución soporta NAT, SNAT.	3016984-EZ
RFT110	Soporte de IPv6: El equipo debe funcionar como Gateway entre redes IPv6 e IPv4 permitiendo tener ambos tipos de redes simultáneamente.	El Equipo permite la integración simultánea de redes IPv6 e IPv4.  Referencia: Citrix NetScaler AppFirewall Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-netscaler-application-firewall-datasheet.pdf</a>	3016984-EZ
RFT111	Soporte de Rate Shapping.	El dispositivo permite limitar el número de conexiones y uso de bandwidth utilizadas por los clientes.  Referencia: Citrix Support <a href="https://support.citrix.com/article/CTX134009">https://support.citrix.com/article/CTX134009</a>	



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.	El netscaler te permite crear múltiples dominios de enrutamientos cada uno con su propio default gateway.  Referencia: Netscaler Docs <a href="https://docs.citrix.com/en-us/netscaler/11/networking/traffic-domains.html">https://docs.citrix.com/en-us/netscaler/11/networking/traffic-domains.html</a>	3016984-EZ
RFT113	Debe soportar VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.	El equipo maneja de forma eficiente VXLAN, VXLAN Gateway, NVGRE y Transparent Ethernet Bridging para entornos de redes virtualizadas.  Referencia: Netscaler docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
RFT114	Debe soportar protocolos de enrutamiento BGP, RIP, OSPF, IS-IS,	El Dispositivo soporta múltiples protocolos de enrutamiento tales como: BGP2, RIP1/2, OSPF, IS-IS.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf</a>	3016984-EZ
<b>ADMINISTRACION DEL SISTEMA</b>			
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)	La solución permite ofrece la gran ventaja de ser administradas por distitas vías tales como: CLI, SSH, HTTPS y Telnet.  Referencia: Netscaler Datasheet <a href="https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf">https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/netscaler-data-sheet.pdf</a>	3016984-EZ
RFT116	La solución debe integrarse con Directorio Activo Windows 2003 o superior, para la	La solución permite la integración del active directory de Windows.	3016984-EZ

	autenticación de usuarios para gestión de la herramienta.	Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	
RFT117	La solución debe integrarse con LDAP, para la autenticación de usuarios para gestión de la herramienta.	La soporta la integración LDAP.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
RFT118	La solución debe integrarse con RADIUS y TACACS+ para la autenticación de usuarios para gestión de la herramienta.	La solución soporta los métodos de autenticación RADIUS y TACACS+ .  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
RFT119	La solución debe incluir comunicación cifrada y permitir la autenticación del equipo y de los usuarios administradores/supervisores con Certificados Digitales	El equipo asegura la comunicación utilizando encriptaciones robustas y utilizando certificados digitales.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
RFT120	La solución debe soportar el envío de alertas y eventos a un Sistema Centralizado mediante: <ul style="list-style-type: none"> <li>• Protocolo SysLog</li> <li>• Notificación vía SMTP</li> <li>• SNMP versión.2.0 o superior.</li> </ul>	La solución soporta el envío de alertas y eventos a un Sistema Centralizado mediante: <ul style="list-style-type: none"> <li>• Protocolo SysLog</li> <li>• Notificación vía SMTP</li> <li>• SNMP versión.2.0 o superior.</li> </ul> Referencia: Netscaler Support <a href="https://support.citrix.com/article/CTX121728">https://support.citrix.com/article/CTX121728</a>	3016984-EZ
RFT121	El sistema de administración debe ser totalmente independiente del sistema de procesamiento de tráfico.	El sistema de procesamiento y de tráfico se encuentra de manera independiente.	3016984-EZ
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.	La solución cuenta con el módulo de administración LOM, el cual le permite encender/apagar el Sistema de manera remota. Además, nos permite visualizar el proceso de arranque.  Referencia:	3016984-EZ

		Netscaler Docs. <a href="https://docs.citrix.com/en-us/netscaler/11/netscaler-hardware-installation/netscaler-mpx-lights-out-management-port-lom.html">https://docs.citrix.com/en-us/netscaler/11/netscaler-hardware-installation/netscaler-mpx-lights-out-management-port-lom.html</a>	
RFT123	La interfaz gráfica debe contar con un Dashboard personalizable que permita monitorear el estado del equipo en tiempo real	La GUI cuenta con un intuitivo y personalizable Dashboard, el cual nos permite monitorear en tiempo real todo lo que sucede en el equipo.  Referencia: Netscaler Docs <a href="http://docs.citrix.com/en-us/netscaler.html">http://docs.citrix.com/en-us/netscaler.html</a>	3016984-EZ
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.	La solución permite visualizar de forma gráfica el comportamiento de las aplicaciones HTTP, y además, no ofrece información detallada de las latencias, congestiones, Throughput y diversas estadísticas para darnos una visión granular de nuestra red.	3016984-EZ
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.	La solución cuenta con plantillas como :  *Microsoft OWA *Microsoft Exchange *Microsoft SharePoint *Citrix Storefront *Citrix Web Interface *Oracle *SAP	3016984-EZ
RFT126	Se debe un incluir una Herramienta de Análisis con su respectivo Licenciamiento, la cual permitirá una mejor gestión la solución ADCs Propuesta.	Incluimos la herramienta de gestión y configuración " <b>NetScaler MAS</b> ".	3016984-EZ
<b>OTROS REQUERIMIENTOS</b>			
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.	Incluimos la instalación física de los equipos.	
RFT128	Las Soluciones propuestas de Application Delivery 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).



## ENTRENAMIENTOS

En nuestra propuesta estamos presentando los entrenamientos pertinentes para la solución que estamos ofertando.

### ➤ Citrix NetScaler 11 Essentials and Networking

Duración: 40 horas

Horario: 9:00 AM - 6:00PM

Modalidad: Presencial Privado

Cantidad de personas: 5 a 10 participantes

Idioma: Español

Fecha Inicio: Pendiente Coordinar con Cliente

Incluye:

- Materiales originales del fabricante (Idioma Ingles)
- Certificado de participación por el fabricante
- Laboratorios y Guía mediante instructor
- Almuerzo
- Coffee Break

\*\*\*NOTA: Para cancelaciones, favor informar con 8 días hábiles de anticipación al día de la capacitación, de lo contrario el cliente deberá cubrir el 100% del valor de la capacitación.

### ➤ Citrix NetScaler 11 Advanced Implementation

Duración: 40 horas

Horario: 9:00 AM - 6:00PM

Modalidad: Presencial Privada

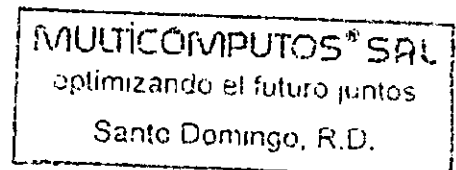
Cantidad de personas: 5 a 10 participantes

Idioma: Español

Fecha Inicio: Pendiente Coordinar con Cliente

Incluye:

- Materiales originales del fabricante (Idioma Ingles)
- Certificado de participación por el fabricante
- Laboratorios y Guía mediante instructor
- Almuerzo
- Coffee Break



\*\*\* NOTA: Para cancelaciones, favor informar con 8 días hábiles de anticipación al día de la capacitación, de lo contrario el cliente deberá cubrir el 100% del valor de la capacitación\*\*\*

## CONDICIONES DE LA PROPUESTA

**VALIDEZ DE LA PROPUESTA:** Treinta (30) días hábiles

**FORMA DE PAGO:**

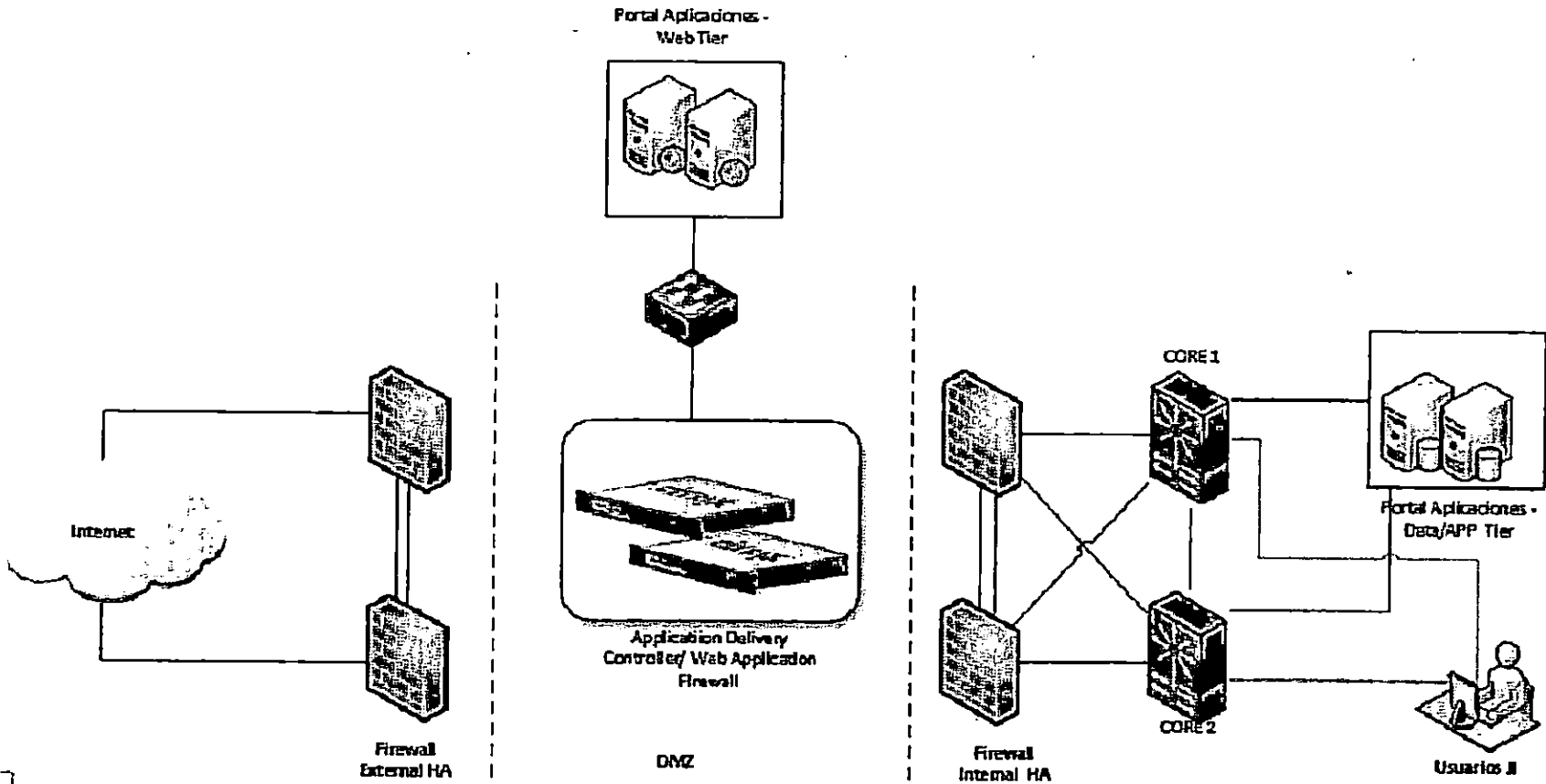
- un primer pago correspondiente al avance de un veinte por ciento (20%) del monto total adjudicado.
- Un segundo pago equivalente a un cuarenta (40%) del monto total de la propuesta presentada luego de recibido los equipos.
- Un pago final equivalente al cuarenta por ciento (40%) del monto total de la propuesta presentada, el cual se hará posterior a la culminación de los servicios.

MULTICOMPUTOS® S.R.L.  
optimizando el futuro juntos  
Santo Domingo, R.D.

---

## Diagrama

---



MULTICOMPUTROS SGL  
 optimizando el futuro de los  
 Santo Domingo, R.D.

*[Handwritten signature]*



ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	F	S	Aug
1		<b>Implementación ADC's</b>	<b>36 days</b>	<b>Mon 8/14/17</b>	<b>Mon 10/2/17</b>				
2		<b>Definicion del Proyecto</b>	<b>3 days</b>	<b>Mon 8/14/17</b>	<b>Wed 8/16/17</b>				
3		Definir alcance del proyectos y los requerimientos del negocios	1 day	Mon 8/14/17	Mon 8/14/17				
4		Kickoff Meeting	1 day	Tue 8/15/17	Tue 8/15/17				
5		Entregable: S.O.W	1 day	Wed 8/16/17	Wed 8/16/17				
6		<b>Planificacion</b>	<b>16 days</b>	<b>Thu 8/17/17</b>	<b>Thu 9/7/17</b>				
7		<b>Gestion del Proyecto</b>	<b>2 days</b>	<b>Thu 8/17/17</b>	<b>Fri 8/18/17</b>				
8		Ajustes plan de trabajo	1 day	Thu 8/17/17	Thu 8/17/17				
9		Revisión y aceptacion del plan de trabajo	1 day	Fri 8/18/17	Fri 8/18/17				
10		<b>Analisis de los requerimientos</b>	<b>1 day</b>	<b>Mon 8/21/17</b>	<b>Mon 8/21/17</b>				
11		Levantamiento de requerimientos de aceleracion y seguridad de aplicaciones	1 day	Mon 8/21/17	Mon 8/21/17				
12		<b>Arquitectura</b>	<b>6 days</b>	<b>Tue 8/22/17</b>	<b>Tue 8/29/17</b>				
13		Diseño de Alto Nivel	1 day	Tue 8/22/17	Tue 8/22/17				
14		Alcance y Objetivo de los ADC's	1 day	Wed 8/23/17	Wed 8/23/17				
15		Crear Diseno Alto Nivel (topologia y flujo de datos)	1 day	Thu 8/24/17	Thu 8/24/17				
16		Revision del Diseno	1 day	Fri 8/25/17	Fri 8/25/17				
17		Aceptacion del Diseño de alto Nivel	1 day	Mon 8/28/17	Mon 8/28/17				
18		Entregable: Diseño (topologia) de alto Nivel	1 day	Tue 8/29/17	Tue 8/29/17				
19		<b>Ambiente de QA</b>	<b>3 days</b>	<b>Wed 8/30/17</b>	<b>Fri 9/1/17</b>				
20		Definir Metodologia de QA	1 day	Wed 8/30/17	Wed 8/30/17				

Sano Domingo  
 MONTAÑANA  
 S.A.

Project: JI\_NetScaler  
 Date: Sat 8/12/17

Task		Inactive Summary		External Tasks	
Split		Manual Task		External Milestone	
Milestone		Duration-only		Deadline	
Summary		Manual Summary Rollup		Progress	
Project Summary		Manual Summary		Manual Progress	
Inactive Task		Start-only			
Inactive Milestone		Finish-only			

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	F	S	Aug
21	★	Revisión de la metodología de QA	1 day	Thu 8/31/17	Thu 8/31/17				
22	★	Aceptación de la metodología de QA	1 day	Fri 9/1/17	Fri 9/1/17				
23	★	Definición de Políticas de aceleración y seguridad de las aplicaciones	3 days	Mon 9/4/17	Wed 9/6/17				
24	★	Análisis de las aplicaciones	1 day	Mon 9/4/17	Mon 9/4/17				
25	★	Definición de integración con sistemas externos (syslogs server, mail, etc)	1 day	Wed 9/6/17	Wed 9/6/17				
26	★	Entregable: Documento de ingeniería	1 day	Thu 9/7/17	Thu 9/7/17				
27	★	Despliegue	29 days	Mon 8/14/17	Thu 9/21/17				
28	★	Gestión del Proyecto	2 days	Mon 8/14/17	Tue 8/15/17				
29	★	Ajustes plan de trabajo	1 day	Mon 8/14/17	Mon 8/14/17				
30	★	Revisión y aceptación del plan de trabajo	1 day	Tue 8/15/17	Tue 8/15/17				
31	★	Instalación	4 days	Wed 8/16/17	Mon 8/21/17				
32	★	Instalación física de los NetScaler	1 day	Wed 8/16/17	Wed 8/16/17				
33	★	Despliegue del NetScaler MAS	1 day	Thu 8/17/17	Thu 8/17/17				
34	★	Instalación del cableado requerido	1 day	Fri 8/18/17	Fri 8/18/17				
35	★	Instalación de licenciamiento y upgrade de software	1 day	Mon 8/21/17	Mon 8/21/17				
36	★	Configuración							
37	☛	Networking	1 day	Tue 8/22/17	Tue 8/22/17				
38	☛	Configuración de NSIP	2 hrs	Tue 8/22/17	Tue 8/22/17				
39	☛	Configuración de SNIP	2 hrs	Tue 8/22/17	Tue 8/22/17	38			
40	☛	Configuración Rutas	2 hrs	Tue 8/22/17	Tue 8/22/17	39			
41	☛	Configuración de DNS	2 hrs	Tue 8/22/17	Tue 8/22/17	40			

Task		Inactive Summary		External Tasks	
Split		Manual Task		External Milestone	
Milestone		Duration-only		Deadline	
Summary		Manual Summary Rollup		Progress	
Project Summary		Manual Summary		Manual Progress	
Inactive Task		Start-only			
Inactive Milestone		Finish-only			

Project: JL\_NetScaler  
Date: Sat 8/12/17

Santo Domingo  
 2017

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	Aug		
							F	S	S
42		<b>Publicacion de servicios/Aplicaciones</b>	1.5 days	Wed 8/23/17	Thu 8/24/17				
43		Configuracion de LBVS	4 hrs	Wed 8/23/17	Wed 8/23/17				
44		Configuracion de monitores	4 hrs	Wed 8/23/17	Wed 8/23/17	43			
45		configuracion de servicios	4 hrs	Thu 8/24/17	Thu 8/24/17	44			
46		<b>Configuracion de Optimizacion</b>	4 days	Fri 8/25/17	Wed 8/30/17				
47		Configuracion HTTPCompress	1 day	Fri 8/25/17	Fri 8/25/17				
48		Configuracaon de AppCache	1 day	Mon 8/28/17	Mon 8/28/17	47			
49		Configuracion de TCP Profiles	1 day	Tue 8/29/17	Tue 8/29/17	48			
50		Configuracion Front-End-Optimization	1 day	Wed 8/30/17	Wed 8/30/17	49			
51		<b>Configuracion de WebApp Firewall</b>	13 days	Thu 8/31/17	Mon 9/18/17				
52		Configuracion en modo learning	1 day	Thu 8/31/17	Thu 8/31/17				
53		configuracion de relaxing rules	3 days	Fri 9/1/17	Tue 9/5/17	52			
54		configuracaon de proteccion basada en OSWAP10 2017	5 days	Wed 9/6/17	Tue 9/12/17	53			
55		Configuracion de signatures	1 day	Wed 9/13/17	Wed 9/13/17	54			
56		configuracion modo activo (protection mode)	3 days	Thu 9/14/17	Mon 9/18/17	55			
57		<b>Configuracion de plataforma analitica</b>	3 days	Tue 9/19/17	Thu 9/21/17				
58		configuracion de reportes	1 day	Tue 9/19/17	Tue 9/19/17				
59		configuracion de vista	1 day	Wed 9/20/17	Wed 9/20/17	58			
60		configuracion de dashboard	1 day	Thu 9/21/17	Thu 9/21/17	59			
61		<b>Entregable: Puesta en funcionamiento Citrix NetScaler</b>							
62		<b>Cierre del Proyecto</b>	7 days	Fri 9/22/17	Mon 10/2/17				
63		Transicion a soporte	3 days	Fri 9/22/17	Tue 9/26/17				

Task		Inactive Summary		External Tasks	
Split		Manual Task		External Milestone	
Milestone		Duration-only		Deadline	
Summary		Manual Summary Rollup		Progress	
Project Summary		Manual Summary		Manual Progress	
Inactive Task		Start-only			
Inactive Milestone		Finish-only			

MUY COMPUNTO S.A.  
 optimizando el futuro jn1058  
 Santo Domingo, D.R.

Project: JI\_NetScaler  
 Date: Sat 8/12/17

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors	F		S		Aug	
64		acta de cierre de proyecto	1 day	Wed 9/27/17	Wed 9/27/17							
65		Entregable: Memoria Tecnica	3 days	Thu 9/28/17	Mon 10/2/17							

MULTICOMPUTOS S.A.  
 optimizando el trabajo  
 Santo Domingo, R.D.

Project: JI_NetScaler Date: Sat 8/12/17	Task		Inactive Summary		External Tasks	
	Split		Manual Task		External Milestone	
	Milestone		Duration-only		Deadline	
	Summary		Manual Summary Rollup		Progress	
	Project Summary		Manual Summary		Manual Progress	
	Inactive Task		Start-only			
	Inactive Milestone		Finish-only			

*Handwritten signature*

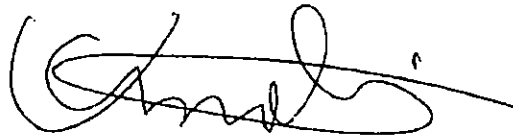
### A QUIEN PUEDA INTERESAR

Por este medio certificamos que la compañía MULTICOMPUTOS, S.R.L., debidamente representada por su Presidente el señor Virgilio S. Albert F., Cédula de identidad personal y electoral número 001-0201987-4, a solicitud de la parte interesada nos requieren como referencia del proyecto.

Multicómputos SRL, trabajó junto a nosotros en un proyecto de seguridad con el producto de NETSCALER, dicha empresa nos brindó apoyo en la dimensión, implementación, hands-on training y soporte post-venta de la solución, obteniendo resultados de calidad, eficiencia y responsabilidad dentro de los parámetros establecidos por esta institución en la ejecución de los mismos.

A la espera de su acostumbrada receptividad y reiterándonos a su disposición para cualquier información adicional al respecto.

Dado en Santo Domingo, Distrito Nacional, a los veintiséis (26) días del mes de julio del 2017.



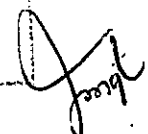
**Victor A. Noboa Risk**  
Vicepresidente de Tecnología  
Unipago, S.A.



**Unipago**<sup>SA</sup>

VAN/FG/gp  
VPT-003-2017

MULTICOMPUTOS S.R.L.  
Calle José Amado Soler East Esq. Abraham Lincoln  
Edificio Gampsa I, 4to. Piso  
Santo Domingo, República Dominicana  
Tel.: 809-227-2007 • Fax 809-227-2005  
E-mail: info@unipago.com.do





"Año del Desarrollo Agroforestal"

Santo Domingo, R.D.  
18 de Julio del 2017.

### A QUIEN PUEDA INTERESAR

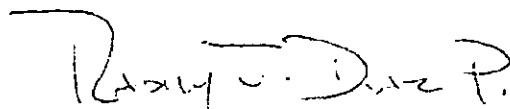
Distinguidos señores:

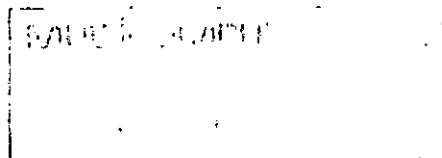
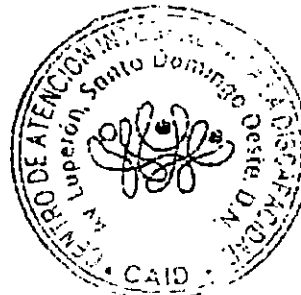
Por este medio certificamos que por medio a la compañía MULTICOMPUTOS, SRL. (RNC número 101-63880-1), debidamente representada por su Presidente el señor Virgilio S. Albert F., Cedula de identidad personal y electoral número 001-0201987-4, a solicitud de la parte interesada nos requieren como referencia del proyecto.

Multicómputos SRL, trabajó junto a nosotros en un proyecto de respaldo, con el producto de NETSCALER, dicha empresa nos brindó apoyo en la dimensión, implementación, hands on training y soporte post venta de la solución, obteniendo resultados de calidad, eficiencia y responsabilidad dentro de los parámetros establecidos por esta institución en la ejecución de los mismos.

A la espera de su acostumbrada receptividad y reiterándonos a su disposición para cualquier información adicional al respecto.

Muy atentamente,

  
Radhy J. Diaz Peña  
Enlace Tecnología DPD-CAID



Avda. Luperón, casi esquina Avenida Enriqueillo  
Santo Domingo Oeste, República Dominicana  
Tel. 809 637 5174 RNC. 424000468

[www.primeradama.gob.do](http://www.primeradama.gob.do)





República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

"AÑO DEL FOMENTO DE LA VIVIENDA"

0 0 0 6 3 3

3 OCT. 2016

## CERTIFICACION

### A QUIEN PUEDA INTERESAR

Por este medio certificamos que **Multicomputos, S.R.L.**, sociedad comercial constituida de acuerdo a las leyes de República Dominicana, Registro Nacional del Contribuyente (RNC) No.: 1-01-63880-1; que conforme los expedientes activos que reposan en nuestros archivos ha sido Proveedor del Programa de Administración Financiera Integrada (PAFI), para las modalidades de Licitación Pública, Comparación de Precios y Proveedor Único, en las siguientes adquisiciones de financiamientos externos y nacionales:

**Programa de Modernización de la Administración de los Recursos Públicos, Convenio de Préstamo 1809/OC-DR, del Banco Interamericano de Desarrollo (BID), concluyó su ejecución en el 2015:**

<b>Contrato 2015 Proveedor Único</b>	<b>Proveedor de Soporte Técnico Premium (HITACHI Y 5545526)</b>
<b>Equipo 5545526</b>	Sun fire X4600 XATO Model Sun fire X4600 M2 x64 Server
<b>Equipo Hitachi</b>	AMS500 Rack Mount Systems + UPGRADE AMS500 Rack Mount Systems + UPGRADE AMS200 Rack Mount Systems (5) Dummy Drive for DF600-RKAAT (SATA) (10) df700 72 gb fc 10k rpm hdd (2) df700 1gb Cache memory 1x1 GB DIMM Sphereon 4400 Base unit Sphereon 4400 Base unit



Stamp: PROGRAMAS DE ADMINISTRACIÓN FINANCIERA INTEGRADA  
 Date: 03 OCT 2016  
 Signature: [Handwritten Signature]



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

<b>Contrato 2015 Proveedor Único</b>	<b>Proveedor de Soporte Técnico EXADATA (Incluyendo Hardware y Software)</b>
<b>Soporte Técnico Exadata</b>	Exadata Database Machine X2-2 HP Quarter Rack Oracle Customer Data and Device Retention Exadata Storage Server Software-Disk Drive Perpetual Oracle Software Update License and Support

<b>Contrato No. Contrapartida-CP- 005-2014</b>	<b>Licencia versión Standard, VmWare Vsphere versión 5.1 para un servidor Sun modelo SunFire 4440 con cuatro procesadores y el Soporte Técnico por tres años a un procesador</b>
<b>Licencias</b>	Licencia versión Standard, VmWare Vsphere versión 5.1 para un servidor Sun modelo SunFire 4440 con cuatro procesadores  Soporte Técnico por tres años

<b>Contrato No. BID- LPN-006-2014</b>	<b>Proveedor de Renovación de Servicios de Soporte Equipos Fortinet</b>
	Renovación Servicios de soporte UTM Bundle por un año (24x7 FortiCare Plus NGFW, Web Filtering y Servicios Antispam) para Equipos marca Fortinet, modelo FortiGate-3140B
	Renovación Servicios de soporte UTM Bundle por un año (8x5 FortiCare Plus NGFW, Web Filtering y Servicios Antispam) para Equipos marca Fortinet, modelo FortiGate-110c







República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

0 0 0 6 3 3

<b>Contrato No. Contrapartida-CD-004-2014 (Proveedor único)</b>	<b>Proveedor de Soporte Técnico Premium en los Sistemas Oracle-Solución Backups</b>
<b>Soporte Técnico Premium en los Sistemas Oracle-Solución Backups</b>	<p>Sun fire X4170 M2 server</p> <p>StorageTek SL500 tape library</p> <p>StorageTek LTO tape drive: 1 HP LTO5 8 Gb FC tape drive for StorageTek SL500 modular library system</p> <p>StorageTek LTO tape drive: 1 HP LTO5 8 Gb FC tape drive for StorageTek SL500 modular Library system</p>

<b>Contrato No. BID-CP-004-2014</b>	<b>Proveedor de Equipos Informáticos de los ítems 4, 5, 6 y 9</b>
	Ítem 04 "Zero Client"
	Ítem 05 "Licencias Sistema para virtualización"
	Ítem 06 "Licencias Antivirus Para Virtualización"
	Ítem 09 "Paquetes de Oficina"





República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

Contrato No. Contrapartida-CD- 002-2014 (Proveedor único)	Proveedor de Soporte Técnico Premium
5545526	Sun fire X4600 XATO Model Sun fire X4140 x64 Server Sun fire X4600 M2 x64 Server
Hitachi	AMS500 Rack Mount Systems + UPGRADE AMS500 Rack Mount Systems Backline Support AMS200 Rack Mount Systems (5) Dummy Drive for DF600-RKAAT (SATA) (10) df700 72 gb fc 10k rpm hdd (2) df700 1gb Cache memory 1x1 GB DIMM Sphereon 4400 Base unit

Contrato No. Contrapartida-CD- 001-2013 (Proveedor único)	Proveedor de Soporte Técnico Premium
5545526	Sun fire X4600 XATO Model Sun fire X4140 x64 Server Sun fire X4600 M2 x64 Server
Hitachi	AMS500 Rack Mount Systems + UPGRADE AMS500 Rack Mount Systems Backline Support AMS200 Rack Mount Systems





República Dominicana

*Ministerio de Hacienda*

*Programa de Administración Financiera Integrada*

000633

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

(5) Dummy Drive for DF600-RKAAT (SATA)
(10) df700 72 gb fc 10k rpm hdd
(2) df700 1gb Cache memory 1x1 GB DIMM
Sphereon 4400 Base unit

<b>Contrato No. BID-CD-001-2012 (Proveedor único)</b>	<b>Proveedor de Oracle Systems y Licencias Oracle</b>
<b>4.1.1 Licenciamiento de programas Oracle según la modalidad del ULA</b>	Oracle Database Enterprise Edition– Processor Perpetual Oracle Real Application Clusters– Processor Perpetual Partitioning– Processor Perpetual Diagnostics Pack– Processor Perpetual Tunning Pack– Processor Perpetual Change Management Pack– Processor Perpetual Configuration Management Pack for Oracle Database– Processor Perpetual
	Provisioning and Patch Automation Pack for Database– Processor Perpetual Oracle Advanced Compression– Processor Perpetual Weblogic Suite– Processor Perpetual
<b>4.1.2 Licenciamiento de programas Oracle según métricas abajo indicadas</b>	Oracle Business Intelligence Suite Enterprise Edition – Processor Perpetual Oracle Business Intelligence Suite Enterprise Edition – Named User Plus Perpetual



Handwritten signature and stamp area with the text "Programa de Administración Financiera Integrada" and "Ministerio de Hacienda".



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

000633

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

	<p>Data Integrator Enterprise Edition - Processor Perpetual          Soporte Técnico de las Licencias Oracle del Licenciamiento del ULA</p>
--	---

<p>Contrato No. BID-CP-001-2012</p>	<p>Proveedor de Procesadores y Memorias</p>
<p>Procesadores y Memorias</p>	<p>CPU/Memory Module Opteron Quad-core 8347HE, 1.9 GHz, 55W CPU para servidor Sunfire X4600 M2          4 GB (2GB DDR2-667 Registered ECC DIMMs) para servidor Sunfire X4600 M2          Discos 300GB FC 10k rpm para Hitachi AMS500 con sus rieles          Garantía en piezas y servicios por un (1) año</p>

<p>Contrato No. BID-CP-002-2012</p>	<p>Proveedor de Tres (3) Drives LTO-5 FC para el equipo StorageTek SL-500, cintas de limpieza, servicios de instalación y configuración del Drive LTO-5 FC</p>
<p>Tres (3) Drives LTO-5 FC para el equipo StorageTek SL-500, cintas de limpieza, servicios de instalación y configuración del Drive LTO-5 FC</p>	<p>Drive LTO-5 FC para StorageTek SL-500 Cuatro (4) Gbps          Cintas de limpieza (LTO cleaning tape)          Instalación y configuración del Drive LTO-5 FC para StorageTek SL-500 Cuatro (4) Gbps          Garantía por un (1) año y seis (6) meses para los Drives LT05</p>



*Handwritten signature*



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

<b>Contrato No. BID-CP-003-2011</b>	<b>Proveedor de Computadores chassis tipo Tower Workstation</b>
Computadores chassis tipo Tower Workstation	<p>Computadoras de Marca Registrada (no clones)</p> <p>Mínimo Procesador de 4 NUCLEOS I7 8MB Cache 2.0 Ghz L3 64-bit</p> <p>Disco duro mínimo de 500GB SATA 3.0Gb/s 16MB de Cache</p> <p>Memoria mínima 8GB DDR3 SDRAM 1333Mhz</p> <p>DVD +/- RW SATA</p> <p>Monitor Panel plano mínimo de 22" Widescreen con entradas VGA y DVI Igual Marca Registrada CPU</p> <p>Tarjeta de Red 10/100/1000</p> <p>Teclado y Mouse USB Igual Marca Registrada que el CPU y Monitor</p> <p>Sistema Operativo Windows® 7 Professional 64-Bit</p> <p>Certificado de garantía del fabricante en sitio, piezas y servicio de (3) años</p> <p>Servicio de entrega y puesta en operación</p>

<b>Contrato No. BID- CP-004-2011</b>	<b>Proveedor de Fortinet Fortigate 110C para el Proyecto del Portal del Ciudadano Dominicano</b>
Fortinet Fortigate 110C para el Proyecto del Portal del Ciudadano Dominicano	<p>Throughput inspeccionado: 500 Mbps</p> <p>Throughput IPS: 200 Mbps</p> <p>Sesiones concurrentes: 400,000</p> <p>Proveer los siguientes mecanismos de protección: Filtrado Web, prevención de intrusos, filtrado de mails y antivirus</p> <p>Instalación</p> <p>Soporte técnico por 3 años</p>



REPUBLICA DOMINICANA  
 MINISTERIO DE HACIENDA  
 PROGRAMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA

*[Firma manuscrita]*



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

<b>Contrato No. Contrapartida-CP-001-2011</b>	<b>Proveedor de Capacitaciones en cursos de Oracle</b>
Curso	Oracle BI Publisher 10g-R3 Fundamentals
Curso	Oracle BI Server Admin 10g-Build Repositories
Curso	Oracle BI Suite EE 10g R3 Create Reports and Dashboards New
Curso	Oracle BI Suite EE 10g R3 Build Repositories
Curso	Warehouse Builder 10g-Administration
Curso	Warehouse Builder 10g I
Curso	Warehouse Builder 10g II

<b>Contrato No. BID-LPI-002-2011</b>	<b>Proveedor de Equipos de Infraestructura de Seguridad y Redes</b>
Protección Perimetral y de Infraestructura de Redes	Firewall Tier-1 FortiGate-3140B Firewall Tier-2 FortiGate-3150B IPS (Sistema de Prevención de Intrusos) Entrenamiento: Implementing Intrusion Detection and Prevention (3-day course) JUNOS Entrenamiento: Administración básica FortiGate 2 días Entrenamiento: Profesional 3 días Servidor de administración Instalación y configuración



PROGRAMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA  
 Santo Domingo, R.D.

*Handwritten signature*



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

000633

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016


<p>Protección de Host y de información de usuario</p>	<p>SYMC MESSAGING GATEWAY 9.5 PER USER SUB LIC GOV BAND H BASIC 36 MONTHS</p> <p>SYMC MESSAGING GATEWAY CONTENT ENCRYPTION 9.5 PER USER SUB LIC GOV BAND H BASIC 36 MONTHS</p> <p>SYMC WEB GATEWAY 4.5 PER USER SUB LIC BAND H BASIC 36 MONTHS</p> <p>SYMC WEB GATEWAY URL FILTERING ADD-ON 4.5 PER USER SUB LIC GOV BAND H BASIC 36 MONTHS</p> <p>SYMC PROTECTION SUITE ENTERPRISE EDITION 3.0 PER USER BNDL COMP UG LIC BASIC 12 MONTHS GOV BAND H</p> <p>SYMC CRITICAL SYSTEM PROTECTION CLIENT EDITION 5.2 NODE BNDL COMP UG LIC GOV BAND H BASIC 12 MO</p> <p>ALTIRIS MANAGEMENT SOLUTION FOR CLIENTS 7.1 XPLAT PER NODE SUB LIC GOV BAND S BASIC 36 MONTHS</p> <p>SYMC BRIGHTMAIL 8360 APPLNC WITH 3YR HWR WARRANTY LA</p> <p>SYMC WEB GATEWAY 8450 APPLNC WITH 3YR HWR WARRANTY LA</p> <p>SYMC NETWORK ACCESS CONTROL 6100 SERIES APPLNCE WITH 3 YEAR HARDWARE WARRANTY LA</p> <p>Servidores para instalación de software</p> <p>Entrenamiento virtual para todos los productos de Symantec</p> <p>Instalación y configuración</p>
<p>Inteligencia para la Gestión de Incidentes</p>	<p>SYMC CONTROL COMPLIANCE SUITE VULNERABILITY MANAGER 10.0 1000 PER NODE BNDL STD LIC GOV BAND S BASIC 12 MONTHS</p> <p>SYMC SECURITY INFORMATION MANAGER 4.7 PER SERVER BNDL STD LIC GOV BAND S BASIC 12 MONTHS</p> <p>SYMC SECURITY INFORMATION MANAGER MONITORED SERVER OR NETWORK NODE 4.7 PER MGD DEVICE BNDL STD LIC GOV</p>



Página 9 de 13

PAF  
 PROGRAMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA

Santo Domingo





República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

	<p>BAND S BASIC 12 MONTHS</p> <p>Servidores para instalación de software</p> <p>Entrenamiento virtual para todos los productos Symantec</p> <p>Instalación y configuración</p>
Escalabilidad de la Red y Optimización de Tráfico	<p>Citrix NetScaler MPX 75000 Platinum Edition (8X10/100/1000)</p> <p>3 Years Gold Maintenance-Citrix NetScaler MPX 75000 Platinum Edition</p> <p>Citrix NetScaler MPX (7500 9500 10500 12500) 450W AC Power Supply</p> <p>Citrix NetScaler AC Power Cable- US (Rating:15A 125V)</p> <p>Citrix Access Gateway- x1 Concurrent User Connection with Subscription Advantage (Universal)- 1-2499 Users-Multilanguage</p> <p>Citrix access Gateway Universal License Subscription Advantage Add-on 2 Years 1-2499 Users</p> <p>Citrix NetScaler MPX 7500 Standard Edition (8X10/100/1000)</p> <p>3 Years Gold Maintenance-Citrix NetScaler MPX-7500 Standard Edition</p> <p>Citrix NetScaler AppCompress Option-Standard Edition</p> <p>3YR SUP for Citrix NetScaler AppCompress Option-NetScaler Standard Edition</p>
Entrenamiento	<p>Administración Básica de Citrix NestScaler</p> <p>Instalación</p>
Infraestructura de Redes	<p>Catalyst 3750X 48 Port Data IP Base</p> <p>Catalyst 3750X 24 Port Data IP Base</p>



PROGRAMA DE ADMINISTRACIÓN FINANCIERA INTEGRADA

*[Firma manuscrita]*





República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

0 0 0 6 3 3

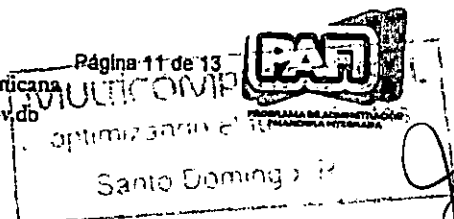
"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

Instalación	Instalación Switches  PowerEdge Rack 4220 Dell 4220 42U Rack With Doors  z600 Workstation
-------------	---

**Recursos Nacionales:**

<b>Licitación Pública Nacional MH-PAFI-CCC-LPN-2015-01</b>	<b>Lote No. 2 "Switches y Firewall"</b> <b>Lote No. 3 "Servidores y Almacenamiento"</b>
<b>Switches y Firewall</b>	Switches del Core  Switches Internet  Cables  Cables de Fibra Óptica 50/125µm 10GB Multimode Duplex LC-LC de 1 metro de longitud  Cables de Fibra Óptica 50/125µm 10GB Multimode Duplex LC-LC de 5 metros de longitud  Cables UTP Cat 6 de 10 pies de longitud  Organizadores de Cables (trasero)  Organizadores de Cables (horizontal)  Firewalls Perimetrales
<b>Servidores y Almacenamiento</b>	Servidores de Base de Datos  Servidores de Administración  Servidores de Producción  Almacenamiento. Network Unified Storage (NUS)





República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

"AÑO DEL FOMENTO DE LA VIVIENDA"

3 OCT. 2016

000633

	Switch Fiber Channel (FC) Switch InfiniBand
--	--

<b>Procedimiento de Excepción de Proveedor Único MH-PAFI-CCC-PE-2016-01</b>	<b>Renovación de servicios soporte de los equipos Hitachi y Sunfire del PAFI</b>
<b>Equipo 5545526 (Sunfire)</b>	Sun fire X4600 XATO Model Sun fire X4600 M2 x64 Server
<b>Equipo Hitachi</b>	AMS500 Rack Mount Systems + UPGRADE AMS500 Rack Mount Systems + UPGRADE AMS200 Rack Mount Systems (5) Dummy Drive for DF600-RKAAT (SATA) (10) df700 72 gb fc 10k rpm hdd (2) df700 1gb Cache memory 1x1 GB DIMM Sphereon 4400 Base unit Sphereon 4400 Base unit

<b>Procedimiento de Excepción de Proveedor Único MH-PAFI-CCC-PE-2016-02</b>	<b>Renovación de los servicios de soporte técnico del equipo EXADATA (incluye Hardware y Software)</b>
<b>Soporte Técnico Exadata</b>	Exadata X2-2: Model Family Serial (AK00035804)



RECIBIDO  
 DIRECCIÓN GENERAL DE ADMINISTRACIÓN FINANCIERA  
 3 OCT 2016  
 [Firma]



República Dominicana  
**Ministerio de Hacienda**  
*Programa de Administración Financiera Integrada*

"AÑO DEL FOMENTO DE LA VIVIENDA"

0 0 0 6 3 3

<p><b>Incluye Hardware y Software</b></p>	<p>Oracle Customer Data and Device Retention          Serial (AK00035804)          Oracle Software Update License and Support</p>
---	---

Esta certificación tiene una vigencia de seis (6) meses, a partir de la fecha y se expide a solicitud de la parte interesada.

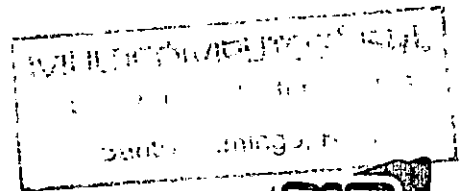
Dado en Santo Domingo de Guzmán, Distrito Nacional, República Dominicana, a los tres (3) días del mes de octubre del año dos mil dieciséis (2016).

Atentamente,

  
 Ing. Ramón E. Sarante  
 Director Técnico del PAFI



rdlc



Página 13 de 13



MULTICOMPUTOS

viernes, 28 de abril de 2017  
Santo Domingo, Rep. Dom.

Señores:  
Contraloría General de la República Dominicana  
Ciudad

ATENCION: Sr. Carmen Matilde Mejía Vasquez, Directora de Tecnología

ASUNTO: Documentación de cierre "ADQUISICION DE EQUIPOS, ACCESORIOS Y LICENCIAS DE INFORMÁTICA, REFERENCIA: CGR-LPN-002-2015"

Señorada Señora,  
Con relación a nuestra propuesta 201509-75181 "ADQUISICION DE EQUIPOS, ACCESORIOS Y LICENCIAS DE INFORMÁTICA, REFERENCIA: CGR-LPN-002-2015" se va la presente comunicación como certificación de cierre de la implementación de la misma.

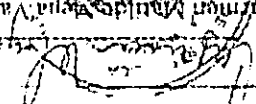
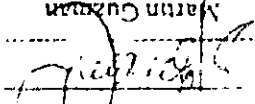
Le informamos que las actividades correspondientes a la instalación de la referida solución fueron completadas de forma satisfactoria por el personal técnico de Multicomputos S.R.L. Las mismas fueron ejecutadas por nuestros ingenieros y fueron aprobadas por parte del equipo técnico asignado al proyecto por parte de Contraloría General de la República Dominicana.

A partir de la fecha de emisión de este documento inicia un periodo de Quince (15) días de garantía de la solución implementada. Una vez culminado este periodo los servicios técnicos relacionados con esta implementación podrán estar sujetos a cotización y posterior facturación.

Agradecemos de usted el apoyo autorizando el cierre del proyecto.

Nos reiteramos a sus órdenes y agradecemos la oportunidad de servirle.

Para constancia suscriben la presente acta

<p>Carmen Matilde Mejía Vasquez Directora de Tecnología Contraloría General de la República Dominicana</p> 	<p>Martin Guzman Director de Operaciones y Servicios MULTICOMPUTOS</p> 
---	--


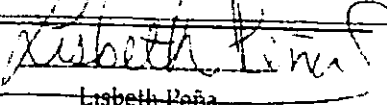
Este es Proyecto "ADQUISICION DE EQUIPOS, ACCESORIOS Y LICENCIAS DE INFORMÁTICA"

REFERENCIA CGR-LPN-002-2015  
SAN PH-Entren\_C-IM-0000060

04-2015-04-010

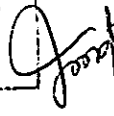
MULTICOMPUTOS S.R.L.

MUL COMPUTOS  
MULTIPLICANDO EL FUTURO DE LOS RICOS

 Laura Delgado Ejecutivo de Cuentas MULTICOMPUTOS	 Lisbeth Peña Coordinadora de Proyectos MULTICOMPUTOS
---	---

Entrega Proyecto "ADQUISICIÓN DE EQUIPOS, ACCESORIOS Y LICENCIAS DE INFORMÁTICA"  
REFERENCIA: CGR-LPN-002-2015"  
CRN: PR\_Entren\_C\_IM-030060  
27/2015-04-010

MULTICOMPUTOS S<sup>A</sup> SOL  
SANTO DOMINGO, D. R.  
SANTO DOMINGO, D. R.



# MULTICOMPUTOS

optimizando el futuro juntos

Abraham Lincoln No. 1007  
Piso No. 4, Ensanche Piantini

809-540-2846  
809-540-2847

**Cotizado a:**

Contralora General de la Republica Dominicana

Carmen Matilde Mejia Vasquez

Av. Mexico, #45, 3er piso

Ministerio de Hacienda

Republica Dominicana

Teléfono (809) 582-1677 Fax 809-882-1677

cmj@contralora.gob.do

**Favor enviar a:**

Contraloria General de la Republica Dominicana

Carmen Matilde Mejia Vasquez

Av. Mexico, #45, 3er piso.

Ministerio de Hacienda

Republica Dominicana

(809) 582-1677 809-662 1677

cmj@contralora.gob.do

## Reporte de Servicio

No.	2015-04-010
Fecha	Apr 28, 2017
O/C No.	OR-2015-527
Orden Ventas	2015-04-010
Pre-Ventas	Oracle Systems
Fabricante	Oracle Systems
Fecha O/V	Oct 7, 2015
No. Cuota	201509-75181
Fecha Estim. Entrega	4 Nov 4, 2015

Division de Soporte y Servicios

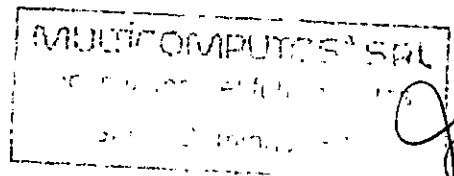
ADQUISICION DE EQUIPOS ACCESORIOS Y LICENCIAS DE INFORMÁTICA  
REFERENCIA UGR-PN-02-2015

Ser.	Cant.	Descripcion	INST. (MSS)	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#	
1		Servidor			XXX
2	1	HP DL60 Gen9 4LFF CTO Server	XXX	727403-B21	XXX
3	1	HP DL60 Gen9 E5-2640v3 FIO Kit	XXX	765542-L21	XXX
4	1	HP DL60 Gen9 E5-2640v3 Kit	XXX	765542-B21	XXX
5	3	HP 32GB 2Rx4 PC4-2133P R Kit	XXX	728629-B21	XXX
6	3	HP 300GB 12G SAS 15K 3.5in SCC ENT HDD	XXX	737261-B21	XXX
7	1	HP 300GB 12G SAS 15K 3.5in SCC ENT HDD	XXX	737261-B21	XXX
8	1	HP 6.5mm SATA DVD-ROM for Gen9 Kit	XXX	726516-B21	XXX
9	1	HP DL60/120 Gen9 CPU1 Riser FIO Kit	XXX	765508-B21	XXX

MULTICOMPUTOS S.R.L.  
 Calle 100 No. 1007  
 Ensanche Piantini, Santo Domingo, D.R.  
 Tel: (809) 540-2846 Fax: (809) 540-2847  
 Email: info@multicomputos.com

Seq.	Cant.	Descripcion	(INST.)	(MSS)	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part No.		
10	1	HP DL60/80/120 Gen6 ALFF Cbl FIO Kit	XXX	Z77331-B21		XXX
11	2	HP 1.83m 10A C13-UL US Pwr Cord	XXX	AF555A		XXX
12	1	HP 1U Security Bezel Kit	XXX	664918-B21		XXX
13	1	HP 1U SFF Easy Install Rail Kit	HP_EIS_EM	734807-B21		HP_EIS
14	2	HP 800W/900W Gold AC Pwr Input FIO Mdl	XXX	813534-B21		XXX
15	1	HP Server RPS Backplane FIO Kit	XXX	813535-B21		XXX
16	1	HP DL60 Gen6 Quick Release Ear FIO Kit	XXX	777324-B21		XXX
17	1	HP 3y Nbd DL60 Gen6 FC Service	XXX	UZVX4E		XXX
18		SubTotal	XXX			XXX
19		<i>Dim de Memoria DL380 G6</i>				XXX
20	24	HP 8GB 2Rx4 PC3-10600R-9 K:	XXX	500662-B21		XXX
21		SubTotal	XXX			XXX
22		Running SubTotal				
23		<i>Plataforma CITRIX</i>				XXX
24		<i>Citrix XenDesktop/ Xenapp Trade Up 430 licencias</i>				

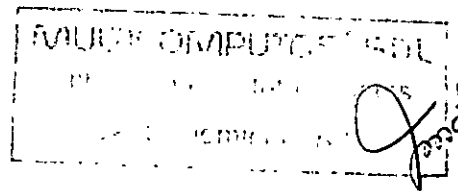
Sec	Cant	Descripcion	[INST.]	[MSS]	Pre-Ventas	Fabricante
		Vendor Part No.			Manuf. Part#	
25	430	Citrix XenDesktop Trade Up Usuario Concurrente Citrix XenDesktop Platinum Edition Trade-up from XenApp Platinum with Expired SA Concurrent User License with SA	XXX		3003:12:E2	XXX
26						XXX
27		SubTotal				
28		<i>Windows Remote Desktop Cal</i>				XXX
29	430	WinRmtDsktpSrvcCAL 2012 OLP NL Gov UsrCAL	XXX		6VC-02077	XXX
30		<i>Cal Windows Server 2012</i>				XXX
31	430	WinSvrCAL 2012 OLP NL Gov DcrCAL	XXX		R18-04290	XXX
32		<i>Nota. De parte del licenciamiento MS, solo seran las Cals de Remote Desktop y Cals de Winserver pues el cliente cuenta con licencias de WinServer</i>				XXX
33		SubTotal				
34		<i>Netscaler Gateway</i>				XXX
35	1	ELA2 NETSCALER MPX 5550 ENT ED 6X 10/100/1000	XXX		3005424:EZ	XXX
36		SubTotal				
37	1	Soporte Ex5 local	XXX		4013929:E2	XXX
38		<i>Instalacion Solucion Citrix</i>				XXX





Sac	Cant.	Descripción	[INST.]	[MSS]	Pro-Ventas	Fabricante
			Vendor Part No.			Manuf-Part#

39		Implementación para Xenapp				XXX
40	1	<p>Instalación, configuración y puesta a punto de solución de virtualización de aplicaciones (Hosted Shared Desktop) Citrix Xenapp Detalles</p> <p>PARA LICENCIAS XENAPP</p> <ul style="list-style-type: none"> <li>- Creación de máquina virtual Template (Golden Image) para Citrix Xenapp 7.6</li> <li>- Instalación de Sistema Operativo sobre servidores físicos en caso de no existir virtualización de servidores               <ul style="list-style-type: none"> <li>- instalación de parchos y hotfix sobre Template (Golden Image)</li> <li>- Instalación de binarios de Citrix Xenapp 7.6 sobre Golden Image</li> <li>- Instalación de pre-requisitos sobre Golden Image</li> </ul> </li> <li>o Rol de Terminal Server               <ul style="list-style-type: none"> <li>o Terminal Server License Server</li> <li>- instalación de aplicaciones a ser virtualizadas (responsabilidad del cliente)</li> <li>- Creación de catálogo de servidores de Xenapp (Windows Server 2012 R2)</li> </ul> </li> <li>o Despliegue de 5 servidores virtuales               <ul style="list-style-type: none"> <li>- Creación de Desktop Group para asignación de aplicaciones</li> <li>- Configuración de políticas de Xenapp</li> <li>- Configuración de impresión</li> <li>- Despliegue de agentes de Citrix Receiver (15 agentes - Cliente es responsable de resto de agentes)</li> <li>- Pruebas de acceso a aplicaciones virtuales</li> <li>- Pruebas de impresión</li> <li>- Pase de conocimiento de la solución de xenapp 7.6</li> <li>- Documentación del proyecto</li> </ul> </li> </ul>			Citrix_EIS	Citrix_EIS_GS Citrix_EIS
41		Implementación del Netscaler				XXX
42	1	<p>Instalación, configuración y puesta a punto de solución Citrix Netscaler Gateway Detalles</p> <ol style="list-style-type: none"> <li>1. Instalación física sobre Rack</li> <li>2. Configuración inicial de red</li> <li>3. Generación e instalación de licencias de Netscaler Gateway</li> <li>4. Configuración inicial del appliance de Netscaler Gateway</li> <li>5. Creación de políticas de Netscaler Gateway para acceso a escritorios virtuales (Reverse Proxy)               <ol style="list-style-type: none"> <li>a. Configuración de políticas sobre Citrix XenDesktop / XenApp</li> <li>5. Creación de políticas de Netscaler Gateway para acceso a recursos del LAN de forma Segura.</li> <li>7. Afinamiento de la plataforma</li> <li>8. Pruebas de acceso desde LAN / WAN</li> <li>9. Documentación de implementación</li> <li>10. Pase de conocimiento de la solución</li> </ol> </li> </ol>			Citrix_EIS_VR	Citrix_EIS
43						XXX
44		Entrenamiento Citrix				XXX
45	3	<p>CXD-263 Managing App and Desktop Solutions with XUI</p> <p>Duración: 40 horas</p> <p>Incluye materiales originales del fabricante, Certificado de participación, Laboratorios y guía mediante instructor</p>				XXX





viernes, 24 de marzo de 2017  
Santo Domingo, Rep. Dom.

Señores:  
Despacho de la Primera Dama  
Ciudad.

**ATENCION :**

**Sr. Radhy J. Diaz Peña, Analista de Redes y Servidores**

**ASUNTO:**

**Documentación de cierre "ADQUISICIÓN, INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y GARANTÍA DE LOS COMPONENTES DE TECNOLOGIA DE INFORMACION Y SEGURIDAD PARA EL CENTRO DE ATENCIÓN INTEGRAL PARA LA DISCAPACIDAD-CAID EN LA CIUDAD DE SANTIAGO DE LOS CABALLEROS, PROVINCIA DE SANTIAGO. DPD-CCC-PU-2015-08**

Estimado Señor,

Con relación a nuestra propuesta 201508-72572 "ADQUISICIÓN, INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y GARANTÍA DE LOS COMPONENTES DE TECNOLOGIA DE INFORMACION Y SEGURIDAD PARA EL CENTRO DE ATENCIÓN INTEGRAL PARA LA DISCAPACIDAD-CAID EN LA CIUDAD DE SANTIAGO DE LOS CABALLEROS, PROVINCIA DE SANTIAGO. DPD-CCC-PU-2015-08

", sirva la presente comunicación como certificación de cierre de la implementación de la misma.

Le informamos que las actividades correspondientes a la instalación de la referida solución fueron completadas de forma satisfactoria por el personal técnico de **Multicómputos S.R.L.** Las mismas fueron ejecutadas por nuestros ingenieros y fueron aprobadas por parte del equipo técnico asignado al proyecto por parte de **Despacho de la Primera Dama.**

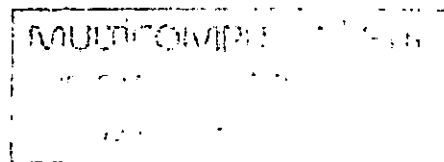
Sirva la presente también para dejar constancia de los puntos pendientes para completar en coordinación con la parte técnica de **Despacho de la Primera Dama** según disponibilidad de ambas partes y del cumplimiento de los requerimientos necesarios.

Puntos Pendientes:

- **Entrenamientos formales:**
  - ✓ Fortigate Multithreat Security Systemas I & II - 2 personas.
  - ✓ Backup Exec Administration - 2 personas.

Entrega Proyecto "ADQUISICIÓN, INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y GARANTÍA DE LOS COMPONENTES DE TECNOLOGIA DE INFORMACION Y SEGURIDAD PARA EL CENTRO DE ATENCIÓN INTEGRAL PARA LA DISCAPACIDAD-CAID EN LA CIUDAD DE SANTIAGO DE LOS CABALLEROS, PROVINCIA DE SANTIAGO. DPD-CCC-PU-2015-08

CRN: PR\_S9438  
CV: 2015-03-138

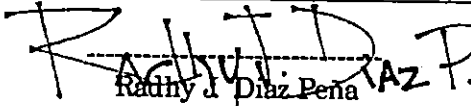
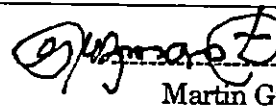




A partir de la fecha de emisión de este documento inicia un periodo de quince (15) días de Garantía de la solución implementada.

Agradecemos de ustedes el apoyo autorizando el cierre del proyecto.

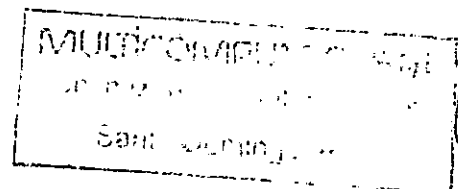
Nos reiteramos a sus órdenes y agradecemos la oportunidad de servirles.

Para constancia, suscriben la presente acta:

 Radhy J. Diaz Peña Analista de Redes y Servidores Despacho de la Primera Dama	 Martín Guzmán Director de Operaciones y Servicios MULTICOMPUTOS
 Laura Delgado Ejecutivo de Cuentas MULTICOMPUTOS	 Daniela Comarazamy Coordinadora de Proyectos MULTICOMPUTOS

Entrega Proyecto "ADQUISICIÓN, INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y GARANTÍA DE LOS COMPONENTES DE TECNOLOGÍA DE INFORMACIÓN Y SEGURIDAD PARA EL CENTRO DE ATENCIÓN INTEGRAL PARA LA DISCAPACIDAD-CAID EN LA CIUDAD DE SANTIAGO DE LOS CABALLEROS, PROVINCIA DE SANTIAGO. DPD-CC-PU-2015-08

CRN: PR\_S9438  
CV: 2015-03-138



# MULTICOMPUTOS<sup>®</sup>

optimizando el futuro juntos

Abraham Lincoln No. 1007,  
Piso No. 4, Ensanche Piantini

809-540-2846  
809-540-2847

## Reporte de Servicio

No. : 2015-03-138-1

Fecha Sep 10, 2015

O/G No. 1,383

Orden Ventas 2015-03-138

Pre-Ventas Oracle Systems

Fabricante Oracle Systems

Fecha O/V Sep 10, 2015

No.Quote 201508-72572

Fecha Estim. Entrega  Oct 15, 2015

### Division de Soporte y Servicios

#### Cotizado a:

Despacho de la Primera Dama

Radhy J. Diaz Peña  
Ave. Mexico esq. 30 de Marzo  
Oficinas Gubernamentales, Bloque D  
Republica Dominicana  
Teléfono : (809) 686-3262 Fax :  
r.diaz@primeradama.gob.do

#### Favor enviar a :

Despacho de la Primera Dama

Radhy J. Diaz Peña  
Ave. Mexico esq. 30 de Marzo  
Oficinas Gubernamentales, Bloque D  
Republica Dominicana  
(809) 686-3262  
r.diaz@primeradama.gob.do

ADQUISICIÓN, INSTALACIÓN, PUESTA EN FUNCIONAMIENTO Y GARANTÍA DE LOS COMPONENTES DE TECNOLOGIA DE INFORMACION Y SEGURIDAD PARA EL CENTRO DE ATENCIÓN INTEGRAL PARA LA DISCAPACIDAD-CAID EN LA CIUDAD DE SANTIAGO DE LOS CABALLEROS. PROVINCIA DE SANTIAGO. DPD-CCC-PU-2015-08

Sec	Cant.	Descripcion	*[_INST.]   * [MSS]	Pre-Ventas	Fabricante
			Vendor Part No.	Mánuf. Part#	

1 **2.8.1.1 - INFRAESTRUCTURA Y CENTRO DE DATOS**

Tecnoredes, S.  
R. L.

2 **1.1 - Cableado Estructurado**

3 **Item 1.1.2 - Racks de dos torres**

4 1 RACK DE 7' 42U DE RACK PANDUIT

PAND\_CMR19X84

5 2 ORGANIZADOR DE CABLE VERTICAL

PAND\_PREP

6 **Item 1.1.3 - Gabinete**

7 1 GABINETE UNIMAX DE 42U COLOR NEGRO CON PUERTAS RANURADAS METALICAS

UNIM\_UMSSG6842

8 4 ABANICOS PARA GABINETE 115V UNIMAX

UNIM\_UMSWEAN110V

9 **Item 1.1.4 - Gabinete**

*[Handwritten Signature]*

Sec	Cant.	Descripción	*[_INST.]   * [MSS]	Pre-Ventas	Fabricante
			Vendor Part No.		Manuf. Part#

10	3	GABINETE UNIMAX DE 12U			UNIM_UMSMB6512
11		<i>Item 1.1.5 - Bandeja Sencilla</i>			
12	2	BANDEJA UNIMAX DE 1U 19X15			UNIM_UM19X15
13		<i>Item 1.1.6- Organizador de Cables</i>			
14	10	ORGANIZADOR HORIZONTAL UNIMAX DE 2U			UNIM_UMOH2
15		SubTotal			
16		<i>Item 1.1.7- Solucion de fibra optica desde MDF</i>			
17	1,800	PIES DE FO MM OM2 DE 6 HILOS			UNIM_UMGYTY53-12A/P
18	4	FDP CON 3 PUERTOS PARA MINIPANELES DE 12 PUERTOS LC 1U			SIE_FCP3BACK
19	10	MINIPANELES LC DE 12 PUERTOS (SI VIENEN DE 6 ES MEJOR)			SIE_RIC-F-LCU12-01C
20	2	BLANKINGPANELS PARA LOS HUECOS VACIO DE LOS FDPs			SIE_RIC-F-BLNK-01
21	60	PIGTAILS LC OM2 SIEMON			
22	10	PATCH CORD LC/LC MM OM2 DE 2 MTRS			SIE_J2-LCLC5-03
23	1	MANO DE OBRA INSTALACIÓN DE ANILLO DE FO MM OM2 PARA INTERCONECTAR MDF CON TRES IDFs Y UNA ENTRE LOS TRES IDFs PARA CONSTRUIR UN ANILLO. INCLUYE TIRADA DE LA FO, TERMINACION POR FUSION EN AMBOS LADOS, IDENTIFICACION Y CERTIFICACION, TRANSPORTE, VIATICOS Y HOTEL LA INFRAESTRUCTURA PARA LA TIRADA DE LA FO EXISTE EN SU TOTALIDAD. COTIZACION DE MANO DE OBRA PARA TRABAJAR EN HORARIO REGULAR DE TRABAJO. ESTA LABOR SE REALIZA EN DOS DIAS LABORABLES.			

MULTIMEDIA 2009

Página: 2

Santa Carolina

*[Handwritten signature]*

Sec	Cant.	Descripcion	[ _ INST.]	[ * ] MSS	Pre-Ventas	Fabricante
			Vendor Part No.			Manuf. Part#

24		SubTotal Solucion de fibra optica desde MDF				MANO DE OBRA
25		<b>Item 1.1.8- Usuarios</b>				
26	35	CAJAS DE CABLE				SIE 9C6M4-E3
27	10	PATCH PANELS MODULARES DE 24 PUERTOS CAT.6				SIE Z-PNL-24E
28	350	JACK RECTOS BLANCO				SIE MX6-02
29	65	BLANKINGPANEL				SIE MX-BL01
30	185	PATCH CORDS DE 3 PIES BLANCO				SIE MC6-8-T-03-02
31	175	PATCH CORDS DE 7 PIES BLANCO				SIE MC6-8-T-07-02
32	175	FACE PLATE SENCILLOS BLANCO				SIE MX-HFP-01-02
33	1	MANO DE OBRA INSTALACION DE 175 SALIDAS PARA DATA. INCLUYE TIRADA DEL CABLEADO, TERMINACION EN AMBOS EXTREMOS (USUARIOS Y PATCH PANELS), IDENTIFICACION Y CERTIFICACION. LA INFRAESTRUCTURA PARA LA TIRADA DE LA FO EXISTE EN SU TOTALIDAD. COTIZACION DE MANO DE OBRA PARA TRABAJAR EN HORARIO REGULAR DE TRABAJO. ESTA LABOR SE REALIZA EN DIEZ DIAS LABORABLES				MANO DE OBRA
34		SubTotal Solucion de Cableado para 175 usuarios				
35		<b>Item 1.1.9 - Solucion Integral de Punto de Acceso (Access Point)</b>				
36	10	FortiAP-221c				EAP-221c-N

MULTIEMPRESA S.A.S.  
 Operadora de Servicios de Telecomunicaciones  
 Calle 100 No. 100-100

*[Handwritten Signature]*

Sec	Cant.	Descripción	*[_INST.]	*[MSS]	Pre-Ventas	Fabricante	
			Vendor Part No.	Manuf. Part#			

37 10 FortiAP-221B 3 years 8x5 FortiCare Contract

EC-10-P0225-311-02-36

38 1 Instalacion solucion wireless

Redes\_EIS

Redes\_EIS\_ER Redes\_EIS

39 **Cableado**

40 2 CAJAS DE CABLE

SIE\_9C6M4-E3

41 1 PATCH PANELS MODULARES DE 24 PUERTOS CAT.6

SIE 7-PNL-24E

42 20 JACK RECTOS BLANCO

SIE\_MX6-02

43 10 BLANKINGPANEL

SIE\_MX-BL01

44 20 PATCH CORDS DE 3 PIES BLANCO

SIE\_MC6-B-T-03-02

45 1 FACE PLATE SENCILLOS BLANCO

SIE\_MX-HFP-01-02

46 19 FACE PLATE SENCILLOS BLANCO

SIE\_MX-HFP-01-02

47 1 MANO DE OBRA INSTALACION DE 10 SALIDAS PARA APs.  
 INCLUYE TIRADA DEL CABLEADO, TERMINACION EN  
 AMBOS EXTREMOS (USUARIOS Y PATCH PANELS),  
 IDENTIFICACION Y CERTIFICACION.  
 TRANSPORTE, VIATICOS Y HOTEL  
 LA INFRAESTRUCTURA PARA LA TIRADA DE LA FO  
 EXISTE EN SU TOTALIDAD.  
 MANO DE OBRA PARA TRABAJAR EN  
 HORARIO REGULAR DE TRABAJO.  
 ESTA LABOR SE REALIZA EN DIEZ DIAS LABORABLES.

48 SubTotal - Solucion integral de Punto de Acceso (Access Point)

49 **1.2 - Seguridad Lógica**

50 **1.2.1 - Firewall**

*[Handwritten signature]*



Sec	Cant.	Descripcion	* [ _ INST.]   * [ M5S]	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#	

51	1	FortiGate-60D Hardware plus 8x5 FortiCare and FortiGuard Bundle			EG-60D-BDL-900-36
52	1	Instalacion solucion wireless			Redes_EIS
				Redes_EIS_IS	Redes_EIS
53		SubTotal Firewall			
54		Running SubTotal			
55		<b>1.3 - Switches</b>			
56		<b>1.3.1 - Switch de 48 Puertos</b>			
57	7	HP 2920-48G-POE+ Switch			J9729A
58	7	HP 3y NBD Exch 2900-48G FC SVC			U3LR5E
59	28	HP X121 1G SFP LC SX Transceiver			J4858C
60	7	HP 2920 2-port Stacking Module			J9733A
61	7	HP X410 1U Univ 4-post Rack Mnt Kit			J9583A
62	7	HP 2920-48G-POE+ Switch US en		J9729A	J9729A
63	7	Instalacion			Redes_EIS
				Redes_EIS_IS	Redes_EIS
64		SubTotal Switch de 48 Puertos			
65		<b>1.3.2 - Switch de 24 Puertos</b>			

AUTENTICACION  
 03/24/2017 11:20:09  
 Santo Domingo

*Handwritten signature*

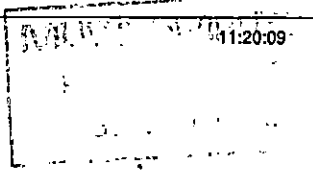
Sec	Cant.	Descripcion	* [ INST ]	* [ MSS ]	Pre-Ventas	Fabricante
			Vendor Part No.			Manuf. Part#

66	3	HP 2920-24G-POE+ Switch				J9727A
67	3	HP 3y NBD Exch 2900-24G FC SVC				U3LQZE
68	6	HP X121 1G SFP LC SX Transceiver				J4858C
69	3	HP 2920 2-port Stacking Module				J9733A
70	15	HP 2920 0.5m Stacking Cable				J9734A
71	3	HP X410 1U Univ 4-post Rack Mnt Kit				J9583A
72	3	HP 2920-48G-POE+ Switch US en			J9729A	J9729A
73	3	Instalacion				Redes_EIS
					Redes_EIS_IS	Redes_EIS
74		SubTotal Switch de 24 Puertos				
75		<b>1.4.1 Servidor procesador de 8 cores</b>				
76	3	HP DL60 Gen9 4LFF CTO Server				777403-B21
77	3	HP DL60 Gen9_E5-2640v3 FIO Kit				765542-L21
78	6	HP 32GB 2Rx4 PC4-2133P-R Kit				728629-B21
79	6	HP 2TB 6G SATA 7.2k 3.5in SC MDL HDD				658079-B21
80	3	HP 9.5mm SATA DVD-ROM Jb Gen9 Kit				

*Handwritten signature*

Sec	Cant.	Descripción	[ INST.]   [ MSS]	Pre-Ventas	Fabricante
			Vendor Part.No.	Manuf. Part#	

81	3	HP DL60/120 Gen9 CPU1 Riser FIO Kit			765508-B21
82	3	HP DL60/80/120 Gen9 4LFF Cbl FIO Kit			777331-B21
83	3	HP Ethernet 1Gb 4-port 331T Adapter			647594-B21
84	3	HP 1U Security Bezel Kit			664918-B21
85	3	HP 1U SFF Easy Install Rail Kit			734807-B21
86	6	HP 800W/900W Gold AC Pwr Input FIO Mdl			813534-B21
87	3	HP Server RPS Backplane FIO Kit			813535-B21
88	3	HP DL60 Gen9 Quick Release Ear FIO Kit			777324-B21
89	3	HP Install DL60/DL80 SVC			U7WZ5E
90	3	WinSvrDataCtr 2012R2 OLP NL Gov 2Proc Qlfd			P71-07845
91	3	HP 3y Nbd DL60 Gen9 FC Service			U7VX4E
92		SubTotal 1.4 - Servidor de Storage			
93		<b>1.4.2 - Servidor de Storage 8 cores y cuatro discos de 2TB</b>			
94	1	HP StoreEasy 1450 8TB SATA Strg			K2R13A
95	1				XX



*Handwritten signature*

Sec	Cant.	Descripcion	* [ _ INST.]   * [ MSS]	Pre-Ventas	Fabricante
			Vendor Part No.		Manuf. Part#
96	4	7 Unit of HP 8GB 1Rx4 PC4-2133P-R Kit			726718-B21
97	4	--			XX
98	1	HP 9.5mm SATA DVD-ROM Jb Gen9 Kit			726536-B21
99	1	HP DL160 Gen9 E5-2603v3 Kit			763235-B21
100	1	HP DL60/80/120 Gen9 4LFF Cbl FIO Kit			--
101	1	HP Ethernet 1Gb 4-port 331T Adapter			--
102	1	HP 1U Security Bezel Kit			--
103	1	HP 1U SFF Easy Install Rail Kit			--
104	2	HP 800W/900W Gold AC Pwr Input FIO Mdl			813534-B21
105	1	--			--
106	1	--			--
107	1	HP Install DL320e/DL120 Service			U6E51E
108	1	--			--
109	1	HP 3y Nbd DL120 Gen9 FC Service			U7VNZE
110		SubTotal Servidor de 8cores y cuatro discos de 2TB			

*Handwritten signature*

Sec	Cant.	Descripcion	*[_INST.]	*[MSS]	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#		
111		<b>1.4.3 - Servidor de procesador 8 cores 2.5</b>				
112	1	HP DL60 Gen9 4LFF CTO Server				777403-B21
113	1	HP DL60 Gen9 E5-2640v3 FIO Kit				765542-L21
114	2	HP 32GB 2Rx4 PC4-2133P-R Kit				726719-B21
115	2	HP 1TB 6G SATA 7.2k 3.5in SC MDL HDD				657750-B21
116	1	HP 9.5mm SATA DVD-ROM Jb Gen9 Kit				726536-B21
117	1	HP DL60/120 Gen9 CPU1 Riser FIO Kit				765508-B21
118	1	HP DL60/80/120 Gen9 4LFF Cbl FIO Kit				777331-B21
119	1	HP Ethernet 1Gb 4-port 331T Adapter				647594-B21
120	1	HP 1U Security Bezel Kit				664918-B21
121	1	HP 1U SFF Easy Install Rail Kit				734807-B21
122	2	HP 800W/900W Gold AC Pwr Input FIO Mdl				813534-B21
123	1	HP Server RPS Backplane FIO Kit				813535-B21
124	1	HP DL60 Gen9 Quick Release Ear FIO Kit				777324-B21
125	1	MS WS12 R2 Std ROK E/F/I/G/S SW				748921-B21

Sec	Cant.	Descripción	[ _ INST.]   [ MSS]	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#	

126	1	HP Install DL60/DL80 SVC			
					U7WZ5E

127	1	HP 3y Nbd DL60 Gen9 FC Service			
					U7VX4E

128		SubTotal 1.4.3 - Servidor de procesador 8 cores 2.5			
-----	--	---	--	--	--

129		<b>1.4.4 KVM</b>			
-----	--	------------------	--	--	--

130	1	8PT KVM 2G ALOG 1 LOC U			
					KVM0108A

131	8	LA KVM 2G SVR MOD USB W/ VIRTUAL MEDIA			
					KVM-USBVM2LA

132	1	LA 19IN RACK LCD CONS KVM			
					AP57192LA

133		SubTotal KVM			
-----	--	--------------	--	--	--

134		<b>1.5 - Central Telefónica</b>			
-----	--	---------------------------------	--	--	--

135		<b>1.5.1 Central Telefonica</b>			
-----	--	---------------------------------	--	--	--

136	1	Sangoma Vega 400 1T1/E1 Digital Gateway			
					INT95011

137	1	Elastix Standard Suscripción de Soporte por 3 años			
					INT94000

138	1	Sangoma Garantia Golden por 3 años 8x5			
					INT95098

139	1	Implementation and Project Management			
					Intouch
			Intouch_EIS	Intouch_EIS	

140	1	Sangoma Garantia Platinum por 3 Años 8x5			
					INT95099

Sec	Cant.	Descripcion	*[_INST.]	*[MSS]	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#		

141 SubTotal Central Telefonica Elastix OS Software Only

142 **1.5.2 Telefono IP Sencillo**

143 70 SoundPoint IP 331, 2-line SIP desktop phone with integrated 2-port 10/100 Ethernet switch and PoE support. Compatible Partner platform: 20. Does not include AC power supply  
2200-12365-025

144 70 Soporte por 3 años  
2200-12365-025

145 **1.5.3 - Telefono IP Ejecutivos**

146 75 VVX 310 6-line Desktop Phone Gigabit Ethernet with HD Voice. Compatible Partner platforms: 20. POE. Ships without power supply.  
2200-46161-025

147 15 Soporte por 3 años  
2200-12365-025

148 **1.5.4 - Modulo de expansión**

149 3 Polycom VVX Expansion Module (paper directory)for VVX 300/310/400/410/500/600 [ does not support Microsoft® Lync® ]  
2200-46300-025

150 3 Soporte por 3 años  
2200-12365-025

151 SubTotal

152 **1.6 hasta el 1.6.7 - Balanceadores de carga**

153 2 Citrix NetScaler MPX 5650 Enterprise Edition (6x 10/100/1000)  
3006527-E2

154 2 3 Years Gold Maintenance Citrix NetScaler MPX 5650 Enterprise Edition (6x 10/100/1000)  
4013997-E2

155 1 Servicios de Implementación  
Redes\_EIS  
Redes\_EIS\_IS Redes\_EIS

Sec	Cant.	Descripcion	*[_INST.]   * [MSS]	Pre-Ventas	Fabricante
			Vendor Part No.	Manuf. Part#	

156 SubTotal

157 **1.7 -Solucion de Respaldo de Datos (Backup)**

158 **1.7.1 Software de Backup Exec**

159 5 SYMC BACKUP EXEC 15 CAPACITY  
EDITION WIN 2 TO 5 TB PER FRONT END  
TB BNDL STD LIC GOV BAND S  
ESSENTIAL 12 MONTHS W7KQWZF9-EI1.GS

160 5 SYMC BACKUP EXEC 15 CAPACITY  
EDITION WIN 2 TO 5 TB PER FRONT END  
TB INITIAL ESSENTIAL 12 MONTHS GOV  
BAND S W7KQWZZ9-EI1.GS

161 5 SYMC BACKUP EXEC 15 CAPACITY  
EDITION WIN 2 TO 5 TB PER FRONT END  
TB INITIAL ESSENTIAL 12 MONTHS GOV  
BAND S W7KQWZZ9-EI1.GS

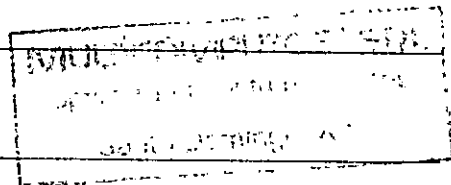
162 SubTotal

163 1 Descripción: Instalación, configuración y puesta de Backup Exec 15 Citrix\_EIS

Detalles:

- Instalación física de servidor Citrix\_EIS\_AR Citrix\_EIS
- Creación de máquina virtual sobre plataforma de Vmware vsphere versión gratuita.
- Instalación de servidor virtual de Windows Server 2008 R2 / 2012 R2
- Configuración de red.
- Instalación de binarios de backup Exec
- Instalación de librería en Backup Exec.
- Realización de Inventario de Cintas en Backup Exec.
- Configuración del Storage en Backup Exec para realización de backup a disco deduplicado.
- Creación de la Política de Backup para el Catalogo de Backup Exec.
- Definición y creación de estrategia de backup
- Configuración de las credenciales a ser utilizadas para sacar backups a máquinas virtuales (no se realizara backup por medio de vmware - versión gratuita)
- Envío de agentes para los servidores de Windows (8 servidores)
- Creación de las políticas de Backup para Windows / Vmware / Microsoft Hyper-V
- 1. Creación de política para dos servidor de Active Directory
- 2. Creación de política para un servidor de SQL
- 3. Creación de política para un servidor de File Server.
- 4. Creación de política para un servidor de Exchange.
- 5. Creación de política para un servidor de Oracle.
- 6. Creación de política para un File Server.
- 7. Creación de políticas para un servidor de Linux.
- 8. Creación de política de backup para Vmware / Microsoft Hyper-V.
  - Pruebas de backup de las políticas Configuradas.
  - Pruebas de restore de las políticas Configuradas (Un máximo de 3 servicios a ser seleccionados por el cliente).
  - Hands On Training de la solución.
  - Documentación del proyecto.

164 SubTotal





Séc	Cant.	Descripción	[ INST. ]	[ MSS ]	Pre-Ventas	Fabricante	
			Vendor Part No.	Manuf. Part#			

165		<b>Servidor de Backup</b>				
166	1	HP DL60 Gen9 4LFF CTO Server				777403-B21
167	1	HP DL60 Gen9 E5-2640v3 FIO Kit				765542-L21
168	2	HP 32GB 2Rx4 PC4-2133P-R Kit				726719-B21
169	2	HP 1TB 6G SATA 7.2k 3.5In SC MDL HDD				657750-B21
170	1	HP 9.5mm SATA DVD-ROM Jb Gen9 Kit				726536-B21
171	1	HP DL60/120 Gen9 CPU1 Riser FIO Kit				765508-B21
172	1	HP DL60/80/120 Gen9 4LFF Cbl FIO Kit				777331-B21
173	1	HP Ethernet 1Gb 4-port 331T Adapter				647594-B21
174	1	HP 1U Security Bezel Kit				664918-B21
175	1	HP 1U SFF Easy Install Rail Kit				734807-B21
176	2	HP 800W/900W Gold AC Pwr Input FIO Mdl				813534-B21
177	1	HP Server RPS Backplane FIO Kit				813535-B21
178	1	HP DL60 Gen9 Quick Release Ear FIO Kit				777324-B21
179	1	WinSvrDataCtr 2012R2 OLP NL Gov 2Proc Qlfd				P71-07845

MULTICOMPUTOS S.A.  
 Optimo Plan. al 11:20:09  
 Santo Domingo

*J. J. J.*

Sec	Cant.	Descripcion	*[_INST.]   *[_MSS]	Pre-Ventas	Fabricante
			Vendor Part No.		Manuf. Part#

180	1	HP Install DL60/DL80 SVC			U7WZ5E
181	1	HP 3y Nbd DL60 Gen9 FC Service			U7VX4E
182		SubTotal			
183		<b>Libreria</b>			
184	1	HP MSL2024 0-Drive Tape Library			AK379A
185	1	HP 3Yr Foundation Care NBD Service			H7J32A3
186	1	MSL2024 Library Support			H7J32A3_80N
187	2	HP MSL LTO-5 Ultrium 3000 SAS Drive Kit			BL540B
188	1	HP Installation Service			HA113A1
189	1	HP Install for 1 MSL5U Lib SVC			HP_EIS HP_EIS_EM HA113A1_5DS
190	2	HP StoreEver Driv PwrSup Crd Install SVC			HA113A1_5DU
191	8	HP LTO5 Ultrium 3TB RW Data Tape			C7975A
192	2	HP Ultrium Universal Cleaning Cartridge			C7978A
193		SubTotal			

194 **1.8 -Dispositivo de Almacenamiento en Red (NAS)**

MULTICOMPUTO S.A.  
Optimizando el tiempo de tu negocio  
Santo Domingo, R.D.

Sec	Cant.	Descripción	*[_INST.]	*[MSS]	Pre-Ventas	Fabricante
			Vendor Part No.			Manuf. Part#

195	1	HP StoreEasy 1450 4TB SATA Strg				K2R12A
196	1	HP 800W/900W Gold AC Power Input Module				Z44689-B21
197	1	HP Installation NAS/Proliant StorSvr SVC				U7986E
198	1	HP 3y Nbd Store 1450 FC SVC				U8JT4E
199		SubTotal 1.8.1 HP StoreEasy 1450 4TB (NAS)				
200		<b>1.9 -Licenciamiento y capacitación</b>				
201		<b>1.9.1 Software de Ofimatica</b>				
202	80	OfficeStd 2013 OLP NL Gov				021-10271
203		<b>1.9.2 Software de Exchange CAL</b>				
204	80	ExchgStdCAL 2013 OLP NL Gov UsrCAL				381-04335
205		SubTotal				
206		<b>1.9.3 Software de Administracion para virtualizacion</b>				
207	1	VMw vCntr Srv Std 1yr E-LTU/S-Buy				G6E84AAE
208	4	VMw vSphere Std 1P 1yr E-LTU				BD710AAE
209	1	VMw vCntr SRM Std 25VM 1yr E-LTU				BD749AAE

MULTICOMPUEROS S.R.L.  
 Santo Domingo

*Janet*

Séc.	Cant.	Descripción	*[_INST.]	*[MSS]	Pre-Ventas	Fabricante	
			Vendor Part No.	Manuf. Part#			

210 SubTotal

211 1 Instalacion y configuración Citrix\_EIS  
Citrix\_EIS\_VR Citrix\_EIS

212 1 Instalacion y configuración Citrix\_EIS  
Citrix\_EIS\_EM Citrix\_EIS

213 SubTotal

214 **1.9.4 Capacitaciones para dos personas**

215 2 VMware vSphere: Install, Configure, Manage V6  
Fecha : Coordinar con el cliente  
Materiales: Manuales originales, Acceso a laboratorios

216 2 Citrix NetScaler 10 Essentials and Networking course  
Key Topics:  
Module 1: Introductions and Course Overview  
Module 2: Basic Networking  
Module 3: Basic Load Balancing  
Module 4: High Availability  
Module 5: Policies and Expressions  
Module 6: Content Switching  
Module 7: Connection Tuning  
Module 8: Global Server Load Balancing  
Module 9: Clustering  
Module 10: Security and Authentication  
Module 11: Rewrite, Responder, and URL Transformation  
Module 12: Optimizing Traffic  
Module 13: Advanced Monitoring  
Module 14: Troubleshooting  
Duración: 40 horas  
Modalidad: virtual y/o Presencial a disponibilidad de Quorum.  
Incluye: materiales originales del fabricante, Certificado de participación, Laboratorios y guía mediante instructor.

217 2 (201 & 301) FortiGate Multi-Threat Security Systems I & II.  
Duración: 40 horas.  
Manuales originales  
Acceso a laboratorios  
Coffee Break (en caso de cursos con modalidad presencial)

218 2 Symantec Backup Exec  
Duracion: 5 días (40 HORAS)  
Incluye: Instructor certificado, Manuales Originales, Material de apoyo, Certificación del fabricante.  
Modalidad: Virtual  
Fecha: Acordar con el Cliente.

MULTI COMPLEJOS S.A.  
Santo Domingo, D.R.  
11:20:09

*g*



Julio 21, de 2017.

Señores  
CONSEJO DEL PODER JUDICIAL (CPJ)

Ref. ADQUISICION DE EQUIPOS TECNOLOGICOS PARA EL CONTROL DE RIESGO Y SEGURIDAD, CORRESPONDIENTE A LA FASE I DEL PROYECTO "MODELO DE ADMINISTRACION DE RIESGO DE LAS REDES DE LA JURISDICCION INMOBILIARIA. Número de Licitación: LPN-CPJ-12-2017

Por este medio queremos hacer de su conocimiento que las políticas de distribución, comercialización y servicio técnico que tenemos en Citrix Systems, Inc. están dirigidas a garantizar el buen nivel y calidad de atención a nuestros clientes.

Por tal razón deseamos comunicarles que la empresa Multicomputos con ORG ID en Citrix # 41338100, basada en República Dominicana quien es revendedor de Citrix desde 11/10/1999, es único canal autorizado con membresía GOLD, para revender los productos de Citrix en República Dominicana. Contando con capacidad para comercializar, implementar y soportar los productos Citrix en el territorio Dominicano.

Validez de esta comunicación 6 meses a partir de la fecha.

Atentamente,

Sandra Gomez Faber  
Senior Partner Account Manager NOLA Region  
Citrix Systems, Inc.

MULTICOMPUTOS S.A.  
[Handwritten signature]

CITRIX AWARDS THE TITLE OF

# Citrix Certified Associate

## Ismael Sosa

is proudly awarded the title of

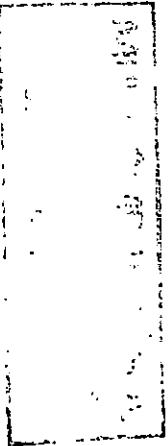
**Citrix Certified Associate**  
**Networking**

*In recognition of successful completion of all the requirements for this certification*

August 15, 2016

DATE CERTIFIED

Certification is valid for three years from the date certified



Kirill Tatarinov, President and CEO  
Citrix Systems, Inc.



CITRIX AWARDS THE TITLE OF

# Citrix Certified Professional

## Ismael Sosa Martinez

is proudly awarded the title of

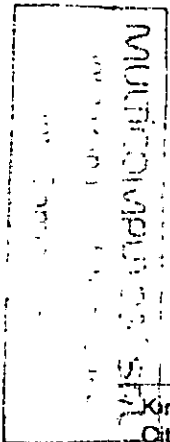
**Citrix Certified Professional  
Networking**

*In recognition of successful completion of all the requirements for this certification*

April 22, 2016

DATE CERTIFIED

Certification is valid for three years from the date certified



Kirill Tatarinov, President and CEO  
Citrix Systems, Inc



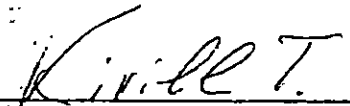
CITRIX AWARDS THE TITLE OF

# Citrix Certified

## Ismael Sosa

has successfully completed all requirements for  
**Citrix NetScaler SD-WAN Certified**

April 27, 2017



Kirill Tatarinov, President and CEO  
Citrix Systems, Inc.







## Luis Ariel Molina Miranda

---

### Información Personal

Dirección: C/ camino central #25, Arroyo Hondo Viejo, D.N.

Fecha y Lugar de Nacimiento: 20-11-1991, Sto. Dgo., Dom Rep.

Cédula: 402-2014407-1

Celular: 809-605-2514

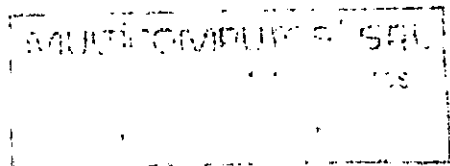
E-mail: [luis.molina@multicomputos.com](mailto:luis.molina@multicomputos.com)

---

### Sinopsis

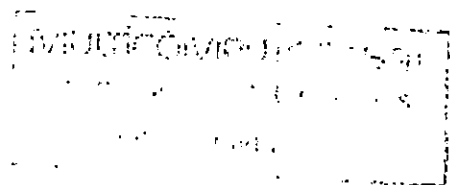
Tomando el papel como futuro profesional en el ambiente de tecnología desde mediados del 2005 de manera informal. Dándole soporte a diferentes familiares, conocidos y demás persona cuando se fue regando la voz de mis servicios de soporte. De manera presencial, remota ya sea vía telefónica o con conexión de directa a la computadora. Durante este periodo fui tomando capacitándome en CENTU, ITLA, FCLD (fundación Código libre Dominicano) e INTEC. Tomando una gran diversidad de cursos: reparación de computadoras, diseño y programación web, parte de CCNA, GNU Linux, asterisk y algunos más.

Dichos conocimientos los fui utilizando durante mis servicios de soporte. Hoy en día ya como profesional formado, trabajo como soporte técnico dándole todo el soporte, mantenimiento y reparación y demás a toda la infraestructura tecnológica donde laboro actualmente. Siempre buscando poder desarrollarme al máximo ya como profesional formado, y a su vez adquiriendo conocimiento en el área de TI.



## **Capacitación**

- Programa de inglés, UNAPEC-2005.
- Reparación de computadora, CENTU-2006.
- Diseño de páginas web, CENTU-2007.
- Programación Web, CENTU- 2008.
- IT Essentials, ITLA-2008.
- CCNA, INTEC (hasta el módulo 3)-2009.
- Programa de inglés, UNAPEC-2010.
- Diplomado de Sistemas GNU/Linux, FCLD (Fundación Código Libre Dominicano)-2012.
- GNU Certified Asterisk Professional, FCLD (Fundación Código Libre Dominicano)-2013.
- Juniper Networks Sales Associate Enterprise Routing, Juniper Networks Learning Academy-2014.
- Junos Operating System highlights, Juniper Networks Learning Academy-2014.
- The Junos Software Advantage, Juniper Networks Learning Academy-2014.
- Citrix Netscaler 11 Essentials and Networking, Multicomputos- 2015.
- Citrix Netscaler 11 Advanced Implementation, Multicomputos-2015.
- Fortigate Multi-threat Security Systems I & II, Adistec-2016.
- Aruba ClearPass Essentials, HPE Education-2016.
- Aruba Mobility Boot Camp, HPE Education-2016.



*Janet*

---

## Certificaciones

- NSE 4 Security Profesional

Junio-2016

**FORTINET.**

- Citrix Certified Associate Networking

Septiembre-2016

**CITRIX®**

---

## Educación

-Graduado de Ingeniería de Sistemas, Instituto Tecnológico de Santo Domingo (INTEC), 2014.

-Graduado del Colegio Arroyo Hondo, 2009.

---

## Experiencia Laboral

- Soporte técnico

*Cable max*

*Desde Septiembre 2013 - 26-09-2014*

-Mantenimiento, adquisición e implementación de toda la infraestructura tecnológica.

-Soporte a los usuarios internos de la empresa.

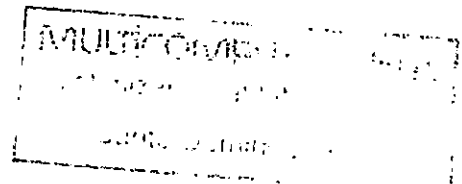
-Cableado UTP.

-Monitoreo de la red, servidores y central telefónica (asterisk).

- Soporte técnico Redes

*Multicomputos*

*Noviembre 2014- Diciembre 2015*



-Brindar apoyo en los proyectos de networking.

-Toma de entrenamientos internos o externos así como sea necesario para mantener el conocimiento de cada uno de los productos de networking.

-Apoyo en la documentación de los proyectos.

- Consultor de Tecnología

### *Multicomputos*

*Enero 2016- Actual*

-Proporcionar servicios profesionales a los clientes que soliciten ayuda con cualquier problema en su red.

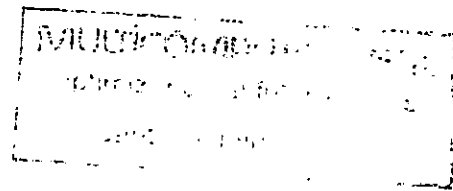
-Manejo de proyectos de networking.

-Elaboración de la documentación técnica de los proyectos.

---

### Referencias

- Ing. José Paredes, Director, Fundación Código Libre Dominicano.  
809-629-59122
- Ing. Ramón Morillo, CEO Morillo, Consulting.  
809-434-1312
- Lic. Enmanuel Bueno, Presidente, Luis Bueno y Asoc S.R.L  
809-771-3417



*Josef*



# Ismael Sosa Martínez

C/ Yolanda Guzmán, # 186, Villa María; Santo Domingo, Rep. Dom.  
Tel: 809-245-1294; Cell: 809-722-8217  
E-mail: ismsosa04@gmail.com

## DATOS PERSONALES

- Cédula : 225-0020434-6
- Fecha de nacimiento : 04 Junio 1988
- Nacionalidad : Dominicana
- Estado civil : Soltero
- Nivel académico : Estudiante Universitario
- Área profesional : Networking/Seguridad

## FORMACION ACADEMICA

- Ingeniería en Sistema. : UNICDA
- Tecnólogo en redes de información : ITLA

## PREPARACION TECNICA & CERTIFICACIONES

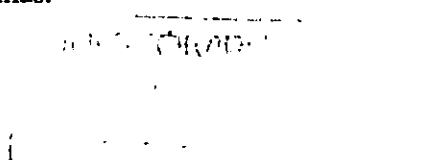
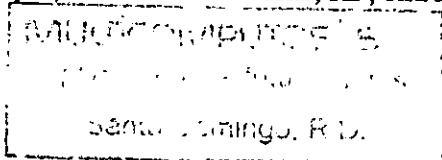
- Citrix CCP-N : MULTICOMPUTOS
- HP FlexNetwork Solutions V3 : MULTICOMPUTOS
- INGLES / Certificación (TOEIC) : UNAPEC/ITLA
- CCNA (CSCO11977388)/CCNP ( BSCI) : ITLA
- Windows Server 2008/2012 : ITLA
- Linux básico : ITLA

## EXPERIENCIA LABORAL

Consultor de Tecnología – Multicomputos (12/2014 - Actual)

### Responsabilidades:

- Implementador de soluciones tecnológicas en el área de redes, instalación y configuración de equipos de comunicación y seguridad, tales como Router, Switches, Firewall, ADC, etc...
- Soporte de las implementaciones realizadas, dando seguimiento y/o resolviendo casos de fallas en los equipos.
- Experiencia trabajando con equipos de las siguientes marcas: Citrix NetScaler, Cisco, Fortinet, Juniper, Palo Alto Networks, HP, entre otras más.



**Analistas de calidad de software – Newtech SRL (08/2013 – 11/2014)**

**Responsabilidades:**

- Probar y verificar el correcto funcionamiento de aplicaciones desarrolladas para Verizon Enterprise.
- Verificar con los clientes los requerimientos de las aplicaciones para en conjunto con los desarrolladores alcanzar las metas deseadas.
- Crear tiques de seguimientos para corregir errores durante el desarrollo de las aplicaciones.

**Soporte Técnico Bilingüe – Amov International Teleservices (02/2010 – 08/2012)**

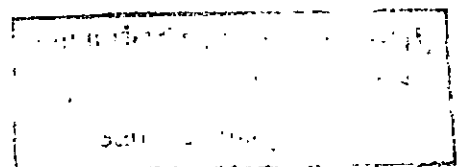
**Responsabilidades:**

- Brindar asistencia y soporte técnico a clientes con conexión a internet para Claro Puerto Rico.
- Configurar la transmisión de señal en los DSLAM de forma remota.
- Crear tiques de seguimiento para corregir fallas en el sistema y reportarlo a los departamentos correspondientes.

**REFERENCIAS PERSONALES**

---

- Bismark Motero : Cel. 829-207-3436
- Dr. Soraya Acosta : Cel. 829-430-2389
- Lic. Richard Mena : Cel. 829-891-0162



*Just*

## Magic Quadrant for Application Delivery Controllers

Published: 29 August 2016 ID: G00292902

Analyst(s): Andrew Lerner, Joe Skorupa, Danilo Piscato

### Summary

Application delivery controllers are a key component within enterprise and cloud data centers to improve application availability, performance and security. However, the market is in a state of flux, with a growing divergence between the needs of traditional I&O and application-centric personnel.

### Strategic Planning Assumptions

By the end of 2018, more than 30% of enterprises will use containerized ADC form factors in their environments, up from less than 5% today.

By the end of 2017, enterprises will be able to obtain lightweight "container friendly" ADC instances from 90% of the vendors included in this research, up from less than 30% today.

By the end of 2017, three of the top six ADC vendors will support third-party ADC software in their management suites, including open source, up from zero today.

### Market Definition/Description

Application delivery controllers (ADCs) provide functions that optimize delivery of enterprise applications across the enterprise network. ADCs provide functionality for both user-to-application and application-to-application traffic, and effectively bridge the gap between the application and underlying protocols and traditional packet-based networks. ADC was a \$2 billion market in 2015, which grew 6.7% and was primarily driven by refresh and new application deployments.

ADCs are also often referred to as "load balancers," as the ADC market evolved from load balancing systems that were developed in the latter half of the 1990s (primarily to ensure the availability and scalability of websites). Historically, ADCs were purchased, deployed and managed by traditional infrastructure and operations (I&O) personnel, but today, application-centric personnel are increasingly making or heavily influencing ADC decisions.

This divergence of ADC buying requirements is driving change and innovation in the market. This change and bifurcation is a microcosm of what Gartner refers to as "bimodal" work style, which combines the conventional capabilities of IT alongside a capability to respond to the level of uncertainty and the need for agility required for a digital transformation.

### Bimodal

Bimodal is a critical work style capability that combines the rock-solid conventional capabilities of IT alongside a capability to respond to the level of uncertainty and the need for agility required for a digital transformation (see "Predicts 2015: Bimodal IT Is a Critical Capability for CIOs"):

- Mode 1 focuses on predictability and has a goal of stability. It is best used where requirements are well-understood in advance, and can be identified by a process of analysis. It includes the necessary investment in renovating and opening up the legacy environment.
- Mode 2 is exploratory. In this case, the requirements are not well-understood in advance. Mode 2 is best-suited for areas where an organization cannot make an accurate, detailed, predefined plan because not enough is known about the area. Mode 2 efforts don't presume to predict the future, but allow the future to reveal itself in small pieces. This work often begins with a hypothesis that is proven, disproven or evolves during a process typically involving short iterations/projects.

In the ADC market, bimodal is exemplified by very distinct buying requirements, including:

- Traditional I&O buyers that use ADCs to improve availability, scale, performance and/or security for enterprise applications primarily supporting Mode 1 initiatives.
- Application-centric buyers that use basic, low-cost, easy-to-acquire load balancers primarily intended to provide high availability and scale for cloud-native applications, primarily supporting Mode 2 initiatives.

This year, Gartner is publishing a companion "Critical Capabilities for Application Delivery Controllers." Enterprise clients can use that research to identify the vendors with the strongest alignment to their relevant use case(s).

Enterprises use ADCs today to improve the following aspects of their applications (see Note 1 for a more detailed listing of ADC capabilities):

- Availability
- Scalability
- End-user performance
- Data center resource utilization

**Security**

**Application visibility and analytics**

The following ADC deployment models are commonly found in the market:

Single-instance hardware appliance

Multi-instance hardware appliance (one hardware device that supports multiple ADC instances)

Software-based instance, which can be run on a bare-metal server, a virtual appliance or within a container, or as an image within an infrastructure as a service (IaaS) provider's platform

A cloud-based as-a-service (aaS) offering, which can be referred to as (over-the-top [OTT]) or "ADCaaS"

**ADC Buyers**

From the buying perspective, we can broadly categorize enterprise ADC buyers into the following types:

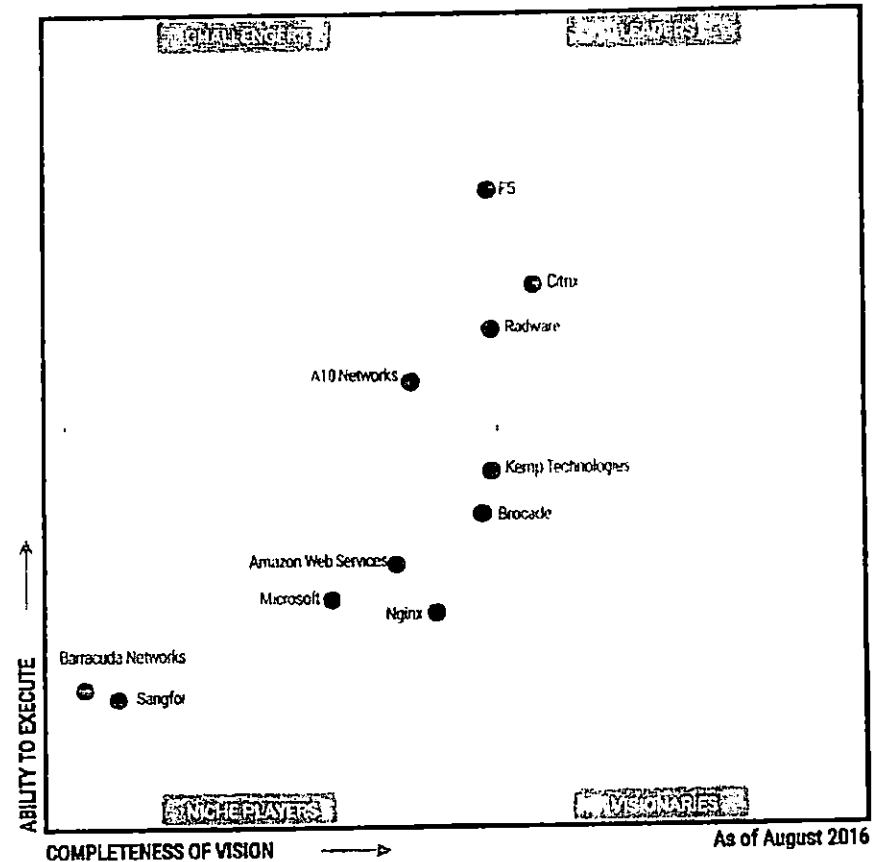
**Standard I&O** – Traditional I&O buyer looking primarily for basic load-balancing functionality to provide high availability for applications (Mode 1 initiatives). This is typically a buyer from the networking organization. Most of these buyers purchase fully capable ADCs that are not fully exploited in their implementation.

**Advanced I&O** – Traditional I&O buyer looking for standard functionality and beyond. These buyers are looking to leverage more of the advanced ADC features, such as performance (for example, asymmetric front-end optimization [FEO], dynamic compression and caching), security (for example, web application firewall [WAF] and distributed denial of service [DDoS]), or geographic load balancing (primarily Mode 1 initiatives). A subset of these buyers is looking for very advanced integration/orchestration with virtualization, containers, cloud management platforms and software-defined networking (SDN) architectures. This is typically a multidisciplinary effort, including architecture, cloud, networking, security and system/application personnel.

**Application-Centric** – Often an application developer, DevOps team or enterprise/cloud architect looking for a lightweight and low-cost load balancer that is easy to acquire, and that will be deployed on a per-application, scale-out basis (often Mode 2 initiatives).

**Magic Quadrant**

Figure 1. Magic Quadrant for Application Delivery Controllers



Source: Gartner (August 2016)

**Vendor Strengths and Cautions**

**A10 Networks**

A10 Networks is a publicly held company based in San Jose, California, and is the fourth-largest ADC vendor when measured by revenue with approximately 7% overall share and 4,900 ADC customers. A10 has a well-established footprint in large-scale environments, including e-commerce and service providers. The vendor's Harmony platform includes ADC capabilities that are delivered as hardware (Thunder appliances) and software (virtual machine [VM] and bare metal). A10 provides strong ADC price/performance and has increased its enterprise business over the past two years, moving beyond just large-scale environments. In the past year, A10 has launched a new platform of ADC appliances, added bare-metal support and enhanced its security portfolio, enhancing WAF functionality. Also, in June 2016, the vendor completed an

MULTICLOUD & SD-WAN SOLUTIONS  
 800.875.8888 | www.gartner.com



acquisition of an ADC startup vendor, Appcito. Organizations looking for leading price/performance and/or those with experience serving large-scale environments should consider A10 for their Mode 1 initiatives.

#### STRENGTHS

A10 has an established footprint and track record for success in large-scale environments, including service providers within North America and Japan, particularly in environments where Internet Protocol version 6 (IPv6) transition, carrier-grade network address translation (CGNAT) and/or Secure Sockets Layer (SSL) inspection are important.

A10 delivers strong value based upon price/performance, small form factors (200 Gbps of Layer 7 throughput in a one-rack unit [1RU] device) and broad programmability.

Compared to leading competitors, A10's all-inclusive licensing SKUs lower product costs, simplify ordering and remove a common concern from enterprise buyers that "Someday I might need that feature."

The acquisition of Appcito will allow A10 to offer both lightweight ADC instances and OTT deployment for ADC features.

#### CAUTIONS

A10 has a smaller installed base and less expertise in mainstream enterprise environments, compared with leading competitors.

A10 lacks SSL VPN capability, which is required by buyers looking to consolidate remote access capabilities into their ADC platform. A joint go to market with Pulse Secure will satisfy some prospects.

Surveyed customers report issues with A10 documentation, which can lead to difficulty in configuring or upgrading the vendor's ADC products.

The vendor grew below market rates in 2015, which Gartner believes is due to difficulty displacing F5/Citrix, combined with a lack of capability to address emerging requirements for Mode 2 initiatives.

#### Amazon Web Services

Based out of Seattle, Washington, Amazon Web Services (AWS) is a subsidiary of Amazon and delivers ADC capability as a feature within its cloud service offering. The vendor's suite of ADC services grew well beyond market rates and is now the No. 3 overall ADC vendor in the market when measured by revenue, with nearly 9% share. The vendor's primary ADC services include Elastic Load Balancing (ELB) for Layer 4 through Layer 7 (L4-7) load balancing, Amazon CloudFront for content delivery and caching, Amazon Route 53 for DNS and global load balancing, and AWS WAF. AWS both competes and partners in the market, as it offers nearly all of its competitors' ADC products in the AWS Marketplace, and customers can choose to bring their own ADC

software to run in Amazon EC2 virtual machines. Over the past year, AWS added several enterprise functions, including basic WAF, improved certificate management and support for additional TCP ports. While the vendor continues to add enterprise-relevant features to its offering, the ADC suite remains available only within the AWS cloud. Organizations deploying applications within AWS should consider this vendor's suite of ADC services.

#### STRENGTHS

The vendor's suite of ADC services is highly integrated with the AWS cloud offering, which enables functionalities (such as autoscaling) to address changing application requirements, and can save money via the ability to scale down back-end services when they aren't needed.

AWS has fostered a large community of developers that are very familiar with its API and suite of functionalities, making it the de facto choice for developing applications within the AWS cloud.

AWS is the fastest-growing major vendor in the market, and accounted for more than half of the total market growth in 2015. We estimate there are now more than 1 million instances of ELB deployed.

The vendor has shown an increasing commitment to developing and delivering enterprise-centric features, including a basic WAF, certificate management, ADC management and regulatory requirements.

#### CAUTIONS

The AWS suite cannot fully address ADC requirements for workloads not deployed within the AWS cloud. For example, ELB cannot be deployed in other clouds or within an organization's on-premises data center.

AWS lacks several key Level 7 enterprise features compared to other ADC vendors — for example, it lacks HTTP 2.0 and DNS Security Extensions (DNSSEC) for Route 53 — and offers a limited set of load-balancing algorithms.

In volatile usage scenarios that entail a sudden and massive burst of traffic, customers may need to contact AWS prior to the burst so the vendor can perform "prewarming" of additional ELB instances.

While the AWS suite resonates well with developers, I&O personnel comment that managing the different functions of the ADC suite can be cumbersome, compared to other ADC vendors. This is reiterated in the customer reference survey as AWS's scores for support are lower than most ADC competitor scores.

#### Barracuda Networks

Barracuda Networks is a publicly traded company based in Campbell, California, with over 11,000 paying ADC customers. The company offers a broad portfolio of products, including security, storage and networking, targeted primarily at small or midsize

businesses (SMBs). Barracuda seeks to provide products that are simple to use and cost-effective, have embedded security functionality and are backed by subscription-based support. Such features are particularly suitable for SMB clients. Barracuda offers hardware and software ADC options, but has more limited deployment options and consumption models than those of some other competitors. Over the past year, Barracuda has enhanced support for virtual desktop infrastructure (VDI) deployments, improved the performance/scale of its hardware platforms, and enhanced its global server load balancing (GSLB) and reporting functions. Small and midmarket organizations should consider this vendor for basic Mode 1 initiatives, particularly if security is a priority and/or other Barracuda products exist in the environment.

#### STRENGTHS

Barracuda delivers a cost-effective solution that is well-aligned with its target customers in SMBs and the midmarket.

Clients report that Barracuda ADC products are easy to set up and manage, and that the vendor provides strong support.

Barracuda offers the option for customers to receive free hardware upgrades every four years, if customers purchase premium maintenance.

Barracuda offers products in several adjacent markets, which can help SMBs limit the number of network suppliers they have to manage.

#### CAUTIONS

Barracuda has a limited set of deployment options, lacking multi-instance appliances, bare-metal or container form factors, and does not offer ADC features via an OTT service.

Barracuda lacks a sizable enterprise installed base, and the vendor does not yet have well-established channels outside of North America and Europe.

Barracuda can meet basic ADC requirements, but lags competitors with respect to enterprise features such as centralized role-based access control (RBAC) for multiple devices, application templates and wizards, and was late to market with support for HTTP 2.0.

Gartner believes that the vendor's roadmap lags those of most competitors in terms of addressing Mode 2 initiatives.

#### Brocade

Brocade is a publicly traded company based in San Jose, California, with over 3,500 ADC customers that we estimate accounted for 1.6% revenue market share in 2015. Over the past year, Brocade completed the acquisition of Riverbed's SteelApp ADC and officially announced the end of life for its legacy ADC product, the ADX. The vendor's ADC suite is now branded as vADC and encompasses its flagship product, Virtual Traffic Manager (vTM), which provides Layer 4 and Layer 7 services; Services Director,

which provides licensing, metering and visibility; and Virtual Web Application Firewall (vWAF). In addition to integration efforts resulting from the Riverbed acquisition, over the past year Brocade has added support for a bare-metal deployment option and improved performance of its platform to support 80 Gbps throughput per x86 node. Organizations looking for a software-only solution and/or that desire consumption-based pricing should consider this vendor for Mode 1 and/or Mode 2 initiatives.

#### STRENGTHS

Brocade's features, licensing options and roadmap are well-aligned with organizations looking to deploy ADC within their virtual or cloud environments.

Brocade provides a no-cost, license-free developer edition that is fully featured and can be acquired with one click.

Brocade offers an advanced pricing model that provides consumption-based billing in addition to traditional capital expenditure (capex)-centric pricing.

Brocade has had a containerized ADC form factor in the market for several years, well ahead of other ADC competitors, which is of increasing importance as containers gain adoption in the enterprise.

The Brocade vADC offers a high degree of programmability and extensibility.

#### CAUTIONS

The vendor does not offer a turnkey hardware appliance, in which hardware/software support is sourced from Brocade.

Brocade lacks visibility in the market, and was not cited as a top six vendor based on unaided end-user client mentions. Similarly, the vendor was not identified as a top three current/future competitor by any other vendors in this research.

Although the vendor offers transition assistance, customers have cited concern over the discontinuation of Brocade's legacy ADC product line, the ADX.

Brocade's perpetual-license pricing can be expensive versus competitors in specific usage scenarios.

Brocade's vADC lacks several features that other ADC vendors have, including SSL VPN, Security Assertion Markup Language (SAML) and deployment templates/wizards for common enterprise applications.

#### Citrix

Citrix is a publicly held company based in Fort Lauderdale, Florida, and its NetScaler ADC business unit is based in Santa Clara, California. Based on revenue, Citrix grew above market rates in 2015 and holds the No. 2 market share position (20%) with 22,000 customers. Citrix provides a comprehensive set of deployment options, including hardware (dedicated and virtualized) and software (VM and container), and is deployed globally in enterprises of all sizes. In the midmarket, we often observe

NetScaler deployed as a gateway in front of Citrix XenDesktop/XenApp products. Over the past year, Citrix announced support for a containerized form factor, and launched a new management and analytics platform. Of the traditional ADC incumbents, Citrix has been the most aggressive in laying out a strategy to address Mode 2 initiatives. Citrix should be considered for all ADC opportunities globally.

#### STRENGTHS

Citrix provides a cost-effective offering with a broad range of deployment options and feature capabilities, which is well-aligned for most enterprise environments and scales to support large environments as well.

Citrix is aggressively pursuing capabilities that address Mode 2 initiatives, with a solid roadmap of product features and licensing options.

NetScaler is deeply integrated with the Citrix suite of products, including XenApp, XenMobile and XenDesktop, which simplifies deployment in those usage scenarios.

Citrix and Cisco have a strong corporate partnership that includes close integration between the NetScaler ADC and Cisco Nexus switch offerings, which can simplify deployments.

#### CAUTIONS

Gartner clients and survey respondents report more problems with Citrix implementation and support when compared with other vendors in this research, although this has improved over the past year.

Citrix has been slow to roll out ADC features as a cloud-based OTT offering, most notably DDoS protection.

Citrix currently lacks a bare-metal deployment option, although the vendor has this on its roadmap.

The Citrix channel lags F5 in demonstrating expertise within complex enterprise application environments.

environments remain primary differentiators. All enterprises globally should consider F5 for their Mode 1 initiatives, especially when support for complex or custom application environments is a requirement.

#### STRENGTHS

F5 has a solid and long-standing understanding of the ADC market, and has the capability to address complex and customized application environments better than other vendors in this research.

The vendor possesses a broad product portfolio that includes physical, virtual and cloud deployments to support a range of use cases from enterprise to service provider.

F5 provides multiple security, remote access, performance and application delivery capabilities, including ADC, WAF, DDoS, FEO and secure web gateway (SWG) that can be integrated on a single platform.

F5's Silverline cloud-based services provide ADC functionality for on-premises and cloud-resident applications.

The vendor has the strongest brand awareness in the market, and appears in nearly all client shortlists on a global basis.

#### CAUTIONS

Based on client feedback and deals that Gartner reviews, F5 is the most expensive ADC vendor in the market.

F5 has not adequately addressed the requirements associated with Mode 2 initiatives, such as low-friction acquisition and lightweight instances, and Gartner believes this has resulted in customers looking to alternative solutions.

Gartner clients and survey results confirm that the complexity of managing F5 ADC functions is a primary concern, particularly in environments with basic requirements.

F5 relies heavily on selling redundant ADC pairs, which drives up customer's total cost of ownership (TCO), instead of leading with alternative platforms (such as virtualized appliances or multitenant hardware). Additionally, clients rarely mention the vendor's ADC-as-a-service offering (Silverline).

The F5 platform is not well-aligned with midmarket and SMB organizations' ADC requirements from feature and price perspectives.

#### Kemp Technologies

Kemp Technologies is a privately held company based in New York, New York, focused exclusively on the ADC market. Kemp has 1.9% revenue share and over 17,000 paying customers worldwide, but grew below market rates in 2015. Kemp provides ADC solutions with flexible deployment models (from bare metal to cloud instances) as well as flexible consumption models (including pay-per-use and per-seat options), with

#### F5

F5 is a publicly traded company based in Seattle, Washington, with over 25,000 ADC customers. F5 continues as the market share leader, although its revenue share decreased from 49% in 2014 to 47% in 2015. While F5 understands the market evolution toward bimodal work styles, public cloud and containers, its focus is largely on its Mode 1 initiatives, such as operations and security. Over the past year, F5 updated its popular iRules with support for Node.js-based development, enhanced management and orchestration capabilities, and added turnkey integration for several popular cloud and networking platforms such as OpenStack, Cisco Application Centric Infrastructure (ACI) and VMware NSX. Gartner sees clients increasingly deploying F5's security capabilities in conjunction with their ADC deployments. F5's in-depth knowledge and features to support applications deployed in complex enterprise

mainstream enterprise. Over the past 12 months, Nginx has announced several new capabilities to better address a more mainstream audience, including UDP load balancing, WAF and a SaaS-based management platform (Nginx Amplify). Nginx should be considered by organizations with Linux expertise when a per-app, software-based ADC is desired, or when commercial support for the raw Nginx open-source software is needed.

#### STRENGTHS

Based on interactions with Nginx Plus customers, the vendor's ADC software is extremely cost-effective, often 50% to 75% less than its competitors.

Nginx open-source software is popular and well-known with application developers, well-suited for containers, and widely deployed globally as a reverse proxy and high-performance web server.

Nginx has a feature set, pricing model and roadmap well-aligned to the needs of developers and application architects, particularly in microservice environments.

The Nginx Plus product is highly extensible, with support for Ruby, Lua, Perl and Linux-based automation tools like Ansible, Chef and Puppet.

Nginx software is available as open source, which reduces capital costs and friction to get started with its product.

#### CAUTIONS

Nginx does not provide a turnkey hardware appliance.

Nginx lacks expertise with, and has a limited installed base within, traditional mainstream enterprise environments.

Nginx Plus lacks several generally available features of established ADC players, including global load balancing (GLB), SSL VPN and enterprise app optimizations.

Currently, Nginx Plus lacks centralized capability to manage multiple ADC instances. This makes it difficult for organizations without Linux expertise to support the product.

Some Nginx Plus customers have cited issues with commercial support, when used for traditional or legacy enterprise applications.

#### Radware

Radware is a publicly traded company headquartered in Tel Aviv, Israel, and Mahwah, New Jersey, with a comprehensive ADC portfolio. The vendor has over 7,500 ADC customers globally and is the No. 4 vendor measured by revenue with 8% share, but fell below market growth rates in 2015. Radware provides flexible deployment options, with a complete set of physical, virtualized and software appliances. Radware also offers ADC functionality OTT, including cloud WAF, cloud DDoS protection and cloud web acceleration. Over the past year, Radware has invested in the programmability,

automation and performance of its platforms, while shifting its corporate messaging more toward security use cases. Enterprises that require full-featured ADC products should consider Radware for their Mode 1 initiatives.

#### STRENGTHS

Radware offers a deep and broad set of security capabilities (DDoS protection, WAF) and performance features (APM, FEO) integrated with its ADC solutions, and is historically early to market with new functionalities.

Radware provides very flexible deployment and delivery options, including capex and operating expenditure (opex) models and managed services, and offers both appliance-based and cloud-based OTT delivery.

Radware provides out-of-the box integration with leading orchestration solutions (Cisco's ACI, VMware NSX, OpenStack, Ansible, Chef and Puppet).

Radware supports high virtualization densities on all of its appliances (including entry level).

Radware provides investment protection through a five-year longevity guarantee on its ADC platforms (guaranteed ability to run the latest software versions).

#### CAUTIONS

Radware customers cite the GUI as an area for improvement, based on inquiry and research surveys.

Gartner believes that Radware underperforms in marketing and brand recognition. Radware has low visibility on Gartner client ADC shortlists and gets fewer mentions in Gartner client inquiries than several of its direct competitors.

Radware does not currently support SSL VPN functionality or provide a containerized ADC instance form factor.

Although Radware operates globally, its coverage and routes to market are not as comprehensive as some of its leading competitors. Enterprises should ensure that local resources with appropriate levels of expertise are available.

Radware was very late to market to support Microsoft Azure, which was concerning for organizations migrating workloads to the public cloud.

#### Sangfor

Sangfor is a privately held company based in Shenzhen, China. It grew above market rates in 2015 and now has a 1.6% revenue share. Sangfor is both a cloud provider and network vendor with multiple networking products, including an ADC branded as Sangfor AD. Sangfor has about 5,700 paying customers for AD, including public sector, finance and telecom verticals primarily within China, but is expanding its channel further into Asia/Pacific (APAC). Over the past year, the vendor launched a new product

called aBOS, which converges several distinct network functions — including ADC — onto a single hardware appliance. Organizations looking for a cost-effective ADC solution in the APAC region should evaluate Sangfor for Mode 1 initiatives.

#### STRENGTHS

Sangfor has products that are tailored to meet specific needs in the Chinese market, such as language localization and support for government security certifications. Similarly, the vendor continues to gain experience in the enterprise by winning deals in larger-scale environments within APAC.

Sangfor can meet common ADC requirements in terms of functionality and performance at an attractive price point.

Sangfor offers an integrated solution, with the most relevant ADC features (load balancing, optimization, global server load balancing [GSLB] and SSL acceleration) packaged in a single-license, cost-effective solution, both appliance-based and virtual.

The vendor has shown consistent investment in its ADC products, improving security and GSLB features while expanding the capacity of its hardware portfolio.

#### CAUTIONS

Gartner believes that the vendor's roadmap lags behind most competitors in terms of addressing Mode 2 initiatives.

Sangfor has a small footprint and limited channel reach outside of China and Southeast Asia; thus, clients should evaluate their local sales and technical support coverage.

The vendor does not offer low-friction lightweight versions of its ADC software, and has not yet integrated its software into the marketplace of popular cloud providers such as AWS, Azure or Tencent.

Sangfor lacks the deployment options of leading ADC competitors, as it does not offer bare-metal, containerized or OTT options.

#### Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

#### Added

Nginx was added as it now meets inclusion criteria.

Microsoft was added due to its collection of ADC features within Azure that now meet inclusion criteria.

#### Dropped

Array Networks was dropped as it no longer meets inclusion criteria.

#### Inclusion and Exclusion Criteria

Criteria for inclusion in the ADC Magic Quadrant include the vendor's ability to:

Provide enterprise ADC products for general availability as of 15 May 2016. ADC product components must be generally available and included on the vendors' published price list.

The vendor must be able to demonstrate at least 100 *enterprise* customers that use its ADC products in production environments as of 15 May 2016.

The vendor must support ADC deployments for both internal and external applications, including support for both front-end and back-end services.

The vendor's product offering must include at least four of these six basic ADC capabilities in general availability as of 15 May 2016:

Dynamic L4 redirection, load balancing and failover

Dynamic L7 redirection, load balancing and failover

Centralized management that includes role-based administrator access for ADC instances/services

Global load balancing

SSL offloading/termination

Protocol optimization (including TCP, HTTP and/or application-specific optimizations)

The vendor's product offering must include at least one of the following four advanced ADC capabilities in general availability as of 15 May 2016:

Web application firewall

IPv6 to IPv4 gateway functions

Content caching

Distributed-denial-of-service protection

Demonstrate relevance to Gartner clients via achieving any one of the following three criteria:

\$25 million in ADC product revenue during 2015, or \$6 million in ADC product subscription revenue during 2015.

\$5 million in ADC support and/or maintenance revenue, which can be associated with commercialized open-source offerings.

Over 5,000 current enterprise and/or midmarket users who have deployed its ADC products as of 15 May 2016.

The vendor must provide evidence to support meeting the above inclusion requirements.

ADC vendors may be excluded from this research for one or more of the following reasons:

The vendor cannot provide ADC capabilities for applications that are not publicly exposed to the internet.

The vendor is not actively providing ADC products to enterprise customers, or has minimal continued investments in the enterprise ADC market.

The company is not the original manufacturer of the ADC product or, in the cases of commercially supported open-source software (OSS), is not the direct provider of that support (including Tier 2 and Tier 3). This includes hardware OEMs, resellers that repackage products that would qualify from their original manufacturers, as well as carriers and ISPs that provide managed services.

#### Open-Source Software Considerations

Magic Quadrants are used to evaluate the commercial offering, sales execution, vision, marketing and support of products within markets, which excludes evaluation of raw open-source software (OSS). The ADC Magic Quadrant includes only commercial-vendor-based offerings, and it does not include individual positions and evaluations for noncommercialized OSS projects, such as Nginx, HAProxy, Maglev, Varnish or Zen Load Balancer. However, vendors that provide commercial support and differentiation for OSS such as Nginx, HAProxy Technologies, SofIntel IT Engineering SL (Zen Load Balancer) and Varnish Software are eligible for this Magic Quadrant, provided they meet inclusion criteria.

#### Other Players

There are several additional vendors that garner interest from Gartner clients within this market and/or that we anticipate will impact this market over time. These vendors do not currently meet our inclusion criteria, but can address application delivery requirements in certain usage scenarios. Some of these vendors address specific usage scenarios or sell to customers outside the traditional IT organization – the so-called "shadow IT."

Specific additional ADC vendors we track include: AppViewX (ADC orchestration), Array Networks, Avi Networks, Fortinet, JetNEXUS, Loadbalancer.org, ScaleArc (database load balancing), Soha Systems, VMware (NSX Load Balancing), Webscale (formerly Lagrange Systems) and embedded functionalities from leading public cloud providers.

#### Evaluation Criteria

##### Ability to Execute

We analyze the vendor's capabilities across broad business functions. Vendors that have expanded their ADC products across a wider range of protocols and applications, improved their service and support capabilities, and focused on improving enterprise applications will be more highly rated in the Magic Quadrant analysis.

**Product or Service** evaluates the capabilities of the products or solutions offered to the market. This includes the vendor's ability to address both Mode 1 and Mode 2 requirements. Key items to consider for the application delivery market are how well the products address enterprise application and scale requirements. This includes the breadth of the products (in terms of different functional capabilities) and how well they scale – from entry-level and/or lightweight products to high-end products and features. The ability to integrate within public and private cloud architectures, including management, orchestration and elasticity, is increasingly important. Key aspects that demonstrate continued execution in this area are flexibility to deploy the ADC in different form factors and deployment architectures.

**Overall Viability** includes an assessment of the organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue to invest in the product, offer the product, and advance the state of the art in the organization's product portfolio.

**Sales Execution/Pricing** looks at the vendor's ability to get the product into the market efficiently. In this market, we evaluate vendors' channels to reach both Mode 1 and Mode 2 IT personnel. In this market, pricing has become a more important criterion during the past two years. As the market matures and expands to include SMBs and DevOps buyers, customer pricing and flexible licensing approaches will become even more important. Additionally, we expect global distribution and support to serve large-enterprise accounts.

**Market Responsiveness/Record** focuses on the vendor's capability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the provider's history of responsiveness.

**Marketing Execution** measures the clarity, quality, creativity and efficacy of programs that are designed to deliver the organization's message to influence the market, including both Mode 1 and Mode 2 IT. This includes the ability to promote the brand

and business, increase awareness of the products, and establish a positive identification of the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotions, thought leadership, word of mouth and sales activities.

**Customer Experience** looks at a vendor's capability to deal with postsales issues. Because of the specialized nature of the application delivery market and the mission-critical nature of many of the application environments supported by the ADC, vendors are expected to escalate and respond to issues in a timely fashion with dedicated and specialized resources, and to have detailed expertise in many specific application environments. Another consideration is a vendor's ability to deal with increasing global demands. Additional support tools and programs are indications of a maturing approach to the market.

Ability to Execute reflects the market conditions and, to a large degree, it is our analysis and interpretation of what we hear from the market. Our assessment focuses on how a vendor participates in the day-to-day activities of the market.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	High
Operations	Not Rated

Source: Gartner (August 2016)

#### Completeness of Vision

**Market Understanding** looks at the vendor's capability to understand buyers' current and future needs, and to translate those needs into an evolving roadmap of products and services. Vendors that show the highest degree of vision listen to, understand, and anticipate Mode 1 and Mode 2 buyers' wants and needs, and can shape or enhance

those wants and needs with their added vision. An example of the expectations in this category is how vendors are enhancing their offerings to address emerging Mode 2 application environments.

**Marketing Strategy** examines the messages and methods that vendors use to disseminate their messages. Are they clear and differentiated? Are they consistently communicated throughout the organization, and communicated externally through the website, advertising, customer programs and positioning statements? A key attribute of a market leader is the ability to shape and direct the key discussion points in a market to help shift a market in new or expanded directions.

**Sales Strategy** looks at how the vendor is positioned to take advantage of different business models, packaging and routes to market to address the requirements for both Mode 1 and Mode 2 applications. Specific items we consider here are pricing models, including perpetual, subscription, consumption-based, freemium and charge for support of open-source software.

**Offering (Product) Strategy** looks at a vendor's product roadmap and architecture, which we map against our view of enterprise requirements. We expect product direction to focus on optimizing enterprise application performance across a variety of deployment models (hardware, software and cloud/OTT). Specific functional capabilities may include application enhancements, security features, analytics, heterogeneous management and orchestration. The timely incorporation of new application architectures, including OTT delivery, SDN, containers and microservices, contributes to this ranking.

**Business Model** assesses a vendor's approach to the market. Does the vendor have an approach that enables it to scale the elements of its business (for example, development, sales/distribution and manufacturing) cost-effectively, from startup to maturity? Does the vendor understand how to leverage key assets to grow? Can it gain additional revenue by charging separately for optional, high-value features or by changing the business model for delivering ADC functionality in different ways? How is the vendor addressing both Mode 1 and Mode 2 requirements? Other key attributes in this market would be reflected in how the vendor uses partnerships and bundling/integration to increase sales. The ability to build strong partnerships with a broad range of application vendors and associated system integrators demonstrates leadership.

**Innovation** measures a vendor's ability to move the market into new solution areas, and to define and deliver new technologies or business models. In the application delivery market, innovation is key to simultaneously addressing rapidly expanding Mode 1 and Mode 2 requirements, and keeping ahead of new (and often more agile) competitors.

Completeness of Vision distills a vendor's view of the future, the direction of the market and the vendor's role in shaping that market. We expect the vendor's vision to be compatible with our view of the market's evolution. A vendor's vision of the evolution of

the data center and the expanding role of ADCs in an increasingly distributed cloud and mobile environment are important criteria. In contrast with how we measure Ability to Execute criteria, more of the rating for Completeness of Vision is based on direct vendor interactions, and on our analysis of the vendor's view of the future.

**Table 2. Completeness of Vision Evaluation Criteria**

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Low
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Not Rated
Innovation	High
Geographic Strategy	Not Rated

Source: Gartner (August 2016)

**Quadrant Descriptions**

**Leaders**

A Leader exhibits the ability to shape the market by introducing capabilities in its product offerings and by raising awareness of the importance of these features. Key capabilities for a Leader in this market revolve around enterprise application functionality. We expect a Leader to have strong or growing market share and to have solutions that resonate with an increasing number of enterprises. We expect Leaders to release ADC capabilities (deployment models, features, pricing models and so on) that support Mode 1 and Mode 2 requirements well in advance of mainstream enterprise demand. A Leader must exhibit expertise in complex enterprise application environments and offer a range of deployment models.

**Challengers**

A Challenger in this market is a follower from a product or innovation perspective, but has demonstrated the capability to take its products into the market and show their relevance to a wide audience. Compared to Leaders, Challengers typically have not yet shown a comprehensive vision to address emerging ADC requirements far in advance of mainstream enterprise demand.

**Visionaries**

Visionaries are vendors that have provided key innovative elements that illustrate the future of the market, and they have an ability to influence the direction of the market toward new approaches. Like Leaders, we expect Visionaries to release ADC capabilities (deployment models, features, pricing models and so on) for both Mode 1 and Mode 2 well in advance of mainstream enterprise demand. However, they lack the capability to reach a large portion of the market; they haven't expanded their sales and support capabilities on a global basis; or they lack the funding to execute with the same capabilities as a vendor in the Leaders quadrant. Examples of technical innovation include the integration of ADCs into cloud and SDN architectures, facilitating the deployment of ADCs into ADC cloud offerings, or addressing emerging Mode 2 IT requirements. Visionary status is not a matter of deploying certain features, but rather requires a vendor to be early enough to demonstrate new approaches while having an ability to change key aspects of the market.

**Niche Players**

Niche Players provide more limited capabilities or focus on specific geographies, verticals or specific deployment scenarios. Niche Players haven't demonstrated enough vision or focused execution to warrant a stronger position in our analysis.

**Context**

The key criterion in this Magic Quadrant focuses on the vendor's ability to provide products and services that solve complex and/or emerging application deployment challenges. Success in this market goes beyond features. It involves a deep understanding of how the elements of applications perform across the network and how emerging network and application deployment options, such as network fabrics, cloud services, microservices and containers will change ADC requirements in the enterprise.

**Market Overview**

The ADC market provides asymmetrical solutions to improve the reliability, performance, efficiency and security of a wide range of applications. Based on the customer research survey (which aligns with Gartner inquiry), the most common applications deployed in association with ADCs include:

Internal websites — 69% of respondents



- Customer internal applications — 66%
- Public websites — 62%
- Customer portal — 56%
- E-commerce external websites — 42%
- Partner portal — 31%
- Microsoft Exchange — 28%
- Internal ERP systems — 23%
- Microsoft Lync or other real-time applications — 21%
- Microsoft SharePoint — 20%
- CRM application — 15%
- Other — 7%

#### Market Drivers

The ADC market is driven primarily by several factors, most prominently:

Refresh of existing ADC and load balancer deployments (primarily for Mode 1 initiatives).

New applications that require ADC capacity, including public/private cloud deployments. In many cases, the buyer is not traditional infrastructure and operations personnel (Mode 1 and 2 initiatives).

Extension of ADC capabilities into nonproduction environments, such as development/test/quality assurance (QA; Mode 1 and 2 initiatives).

Expansion of ADC to include additional features such as security (WAF, remote access) and global load balancing (Mode 1 initiatives).

Net-new expenditure in the midmarket as organizations upgrade from nonexistent or rudimentary load-balancing solutions (Mode 1 initiatives, primarily).

#### ADC Use Cases

We observe ADCs deployed within a varying set of use cases, and the most common we observe in the enterprise include:

**Infrastructure Load Balancing** — This includes basic Layer 4 traffic spraying to provide scale and reliability to infrastructure software services such as DNS, logging and software distribution servers.

**Standard Enterprise Applications** — This use case focuses on the ability to support standard commercial applications commonly deployed by the enterprise.

**Customized Enterprise Applications** — This use case focuses on the ability to support customized and nonstandard application deployment scenarios.

**Midmarket Environments** — This addresses the fact that midmarket organizations have similar functionality requirements to the above standard and customized use cases, but often prioritize simplified management much higher than product scalability.

**Mode 2 Initiatives** — This use case is driven by application-centric personnel that are looking for ADCs to provide basic functionality, at a reduced cost and with low acquisition friction.

#### Revenue and Vendor Landscape

The market drivers identified above are diverse. As a result, the ADC market — including the vendor landscape — remains dynamic. For example, despite F5 and Citrix accounting for more than 67% of total revenue in the market, AWS accounted for more than half of the total revenue *growth* in the market. AWS, Radware and A10 combined to account for roughly 23% of market revenue, and remaining vendors account for roughly 10% (see "Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q15 and 2015").

#### Key ADC Features

Load balancing and SSL termination continue to be the primary functions required in ADC platforms, from more than 99% of clients, based on inquiry. However, we continue to see clients use a broad set of features in their ADCs, including WAF, global load balancing, IPv6/IPv4 and content acceleration. Based on the customer research survey (which aligns with Gartner inquiry, except for WAF), the most common ADC features used by respondents include:

Server Load Balancing — 100%

SSL Offload — 70%

TCP Multiplexing — 34%

Web Content Optimization — 32%

Global Load Balancing — 31%

Application-Specific Configuration — 30%

WAF — 25% (however, we observe 30% to 50% of clients are interested in WAF on their ADCs, based on inquiry)

Customized Programmatic Scripting — 24%

SSL VPN — 21%

IPv6 Gateway Services — 4%

Other -- 7%

### What Has Changed?

For several years, changes in the ADC market centered on adding features and improving price/performance. While there is still technological innovation in these areas over the past year, with support for HTTP 2.0 being the most notable, we now see changes beyond just additional features, including:

- Continued influence of application-centric "buyers" to support Mode 2 initiatives
- The cloud making load balancers "cool" again
- Increasing desire for software-based deployment options
- Increasing security interest
- Increasing importance of management and orchestration (MANO)

### Proliferation of Application-Centric Influence

Over the past year, the biggest impact to the ADC market has been continued proliferation to address requirements for Mode 2 initiatives, which typically require a very different set of requirements versus traditional I&O:

- Low-friction software acquisition (such as open-source downloads, freemium or direct access from cloud provider service catalogs)
- Per-application instances of ADC/load balancing (versus per environment)
- Scale-out resiliency and scalability versus scale-up
- Limited usage of advanced ADC capabilities
- Very low-cost and/or usage-based pricing
- API control and integration with DevOps processes and tooling

### The Result: The Cloud Makes Load Balancers "Cool" Again

As a result of increasing influence from application-centric personnel, we are seeing renewed interest in basic load-balancing functionality (see "How I&O Teams Can Survive the Return of the Zombie Load Balancers"). Development teams supporting Mode 2 initiatives have application delivery requirements that cannot be met with traditional ADCs. Thus, application-centric personnel typically prefer to use nontraditional ADC vendor offerings such as Amazon Web Services, Microsoft Azure, HAProxy or Nginx. Further, traditional vendors have been slow to release products that address Mode 2 initiatives.

Longer term, this will create challenges for enterprises as traditional I&O has limited management, control and visibility for applications built with nontraditional ADC products. To address this, we anticipate traditional ADC vendors will respond via several mechanisms (see "Predicts 2016: Enterprise Networks and Network Services"), including:

- Providing open-source or freemium lightweight versions of their software that can run inside a container
- Providing support for open-source software within their management suites
- Updating pricing and packaging models to provide consumption-based and/or freemium offerings

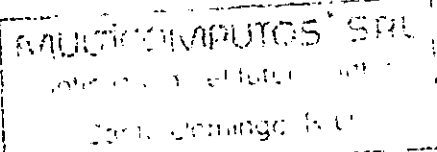
### Shifting From Hardware to Software

ADCs have always been rooted in software, but traditionally packaged as hardware appliances. While hardware-based ADC appliances are still widely deployed today, ADCs are becoming much less hardware-centric as the market evolves. Software-based ADC deployment now comes up in more than half of our client discussions, and can address a much larger percentage of ADC requirements than in prior years. In 2014, there was only one vendor in the ADC Magic Quadrant that didn't provide a turnkey hardware appliance (Riverbed), which has quadrupled to four this year (Brocade, AWS, Nginx, Microsoft). This is the result of several factors, including:

- Applications being developed and run in a cloud provider's environment, where only software-based ADCs can be used
- Increased viability of x86 platforms from a scale and performance perspective, and increased confidence from I&O personnel in the stability and availability of virtual infrastructure
- Increasing use of per-application ADC instances versus per-environment ADC instances, reducing the scale/performance/functionality requirement on a per-ADC instance
- Increasing use of microservice-based architectures and containers (Note: 35% of respondents to the Magic Quadrant reference survey are running containers in their environments)
- Increasing influence on ADC decisions from application teams versus only I&O personnel
- Availability of over-the-top offerings from traditional and newer ADC vendors

### Continued Security Interest

Of the ADC deals that Gartner reviews, between 30% and 50% now include security functionality. This is due to several factors, including:



The continuing string of widely publicized security breaches

The relatively low incremental cost and effort to derive security functionality (like WAF) from an ADC deployment (versus a dedicated separate security product/purchase)

Lingering concerns over vulnerabilities such as Heartbleed and Shellshock

Continued DDoS attacks

Concern over governmental spying

This is accelerated by the fact that many ADC vendors have heavily pivoted their marketing and messaging toward a security-centric focus and are increasingly targeting buyers from the chief information security officer (CISO) organization. Gartner also publishes a "Magic Quadrant for Web Application Firewalls," which includes four vendors from this research (Barracuda, Citrix, F5, Radware).

### Management and Orchestration Matters

Nearly all enterprise are aiming to improve agility within their data center environments to deliver services to their business faster, and this is often associated with cloud initiatives. This aim has trickled down to the ADC market since it is a key component within most enterprise data centers. As a result, we've seen increasing desire from end users for improved ADC MANO, along with corresponding investment from vendors in the following areas:

Tying ADCs in with application life cycle workflow processes

Tying ADCs in with infrastructure orchestration and provisioning tools, including precanned integration with leading cloud, virtualization and network solutions such as VMware vRealize, VMware NSX, Cisco ACI, OpenStack and Docker

Improved programmability with APIs and support for common automation tools like Puppet, Chef and Ansible

Increasing investment in improved ADC device management and provisioning capabilities

Further, we anticipate MANO to gain increasing importance since it will help to bridge the gap between ADCs supporting Mode 1 and Mode 2 initiatives. Currently, no vendor evaluated in this research has strong capability to bridge Mode 1 and Mode 2 initiatives in its management suite.

### The Result: Change, Innovation, and Simultaneous Aggregation and Disaggregation

Ultimately, the byproduct of these changes has led to conflicting evolutionary trends – consolidation and disaggregation of ADC functionality:

Consolidation is being led by traditional I&O buyers who are aggregating security,

optimizing and...

<https://www.gartner.com/doc/reprints?id=1-3GDIRPU&ct=160829&st=sb>

8/7/2017

performance and availability while deploying ADCs between users and applications.

Disaggregation is being led by application-centric personnel deploying lightweight, software-based ADCs primarily for load balancing and closer to the application logic.

As the market continues to develop, our expectations increase with each iteration of this Magic Quadrant. As a result, the Magic Quadrant axis depicts a shift up and to the right with each revision. Consequently, vendors must progress to maintain their positions in each new Magic Quadrant.

### Evidence

Gartner analysts conducted more than 400 interactions with current and prospective clients on the topic of ADCs between January 2015 and June 2016.

Through the course of client interactions and the research process, Gartner has specific insight into ADC global deals tallying more than \$70 million in expenditure over the past year.

All the vendors evaluated in this research were asked to respond to a questionnaire that describes current and future strategies, representative customer wins, and so on. All vendors in the research responded to the questionnaire.

Customer reference surveys were conducted for this research (n = 71). All included vendors were asked to submit 10 references that generally represented the inclusion criteria. The vendors provided reference contact information that was used to invite the reference to complete a 15-minute online survey. A total of 71 references from 11 vendors completed the survey between 23 May 2016 and 6 June 2016. The 71 references represent the select customers the 11 vendors chose to share with Gartner that ultimately elected to participate as a reference check, and may not represent customers in the overall application delivery controller (end-user) market.

Gartner analysts reviewed vendors' technical specification sheets, configuration guides, marketing materials, blogs, webinars and publicly available financial statements for vendors in this research.

Gartner enterprise network equipment Market Share research.

Gartner "Magic Quadrant for Web Application Firewalls."

### Note 1 ADC Capabilities

The range of functionality offered by ADCs continues to grow and can include some, or all, of the following:

Reliability

Dynamic L4-7 redirection, load balancing and failover

<https://www.gartner.com/doc/reprints?id=1-3GDIRPU&ct=160829&st=sb>

8/7/2017

- Transaction assurance
- Load balancing for database and big data use cases
- High availability and clustering for ADC platforms
- Data center resource efficiency
  - TCP connection multiplexing
  - SSL termination
  - Proxy caching
  - XML validation and transformation
- Performance
  - Data compression and dynamic/adaptive compression
  - Protocol optimization
  - Caching
  - Content transformation and rewrite
  - HTML (and other application protocol) optimizations – prefetching and selective encoding
  - Object reordering and consolidation
  - Application-specific acceleration
  - HTTP 2.0 gateway
- Security
  - WAF
  - Network-level security functions, DDoS protection and server cloaking
  - Access control, identity management and single sign-on
- Platform capabilities
  - Rules and programmatic interfaces (rule-based extensibility), including open APIs
  - Application configuration templates and wizards to ease deployment
  - Role-based management
  - Virtualized appliance, software and containerized form factors
  - Application performance management capabilities
  - Cloud deployment and control
  - Back-end server monitoring

- Network-address translation (NAT)
- Bidirectional and stateful application proxy
- IPv6 to IPv4 gateway functions
- Global load balancing
- Integration with other IT systems (via APIs and protocols)

**Evaluation Criteria Definitions**

**Ability to Execute**

**Product/Service:** Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

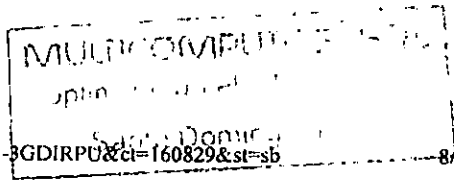
**Overall Viability:** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

**Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

**Market Responsiveness/Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

**Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.



**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

#### Completeness of Vision

**Market Understanding:** Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor's underlying business proposition.

**Vertical/Industry Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

**Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services

(/technology/about/policies/usage\_guidelines.jsp) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and

shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity. (/technology/about/ombudsman/omb\_guide2.jsp)"

About (<http://www.gartner.com/technology/about.jsp>)

Careers (<http://www.gartner.com/technology/careers/>)

Newsroom (<http://www.gartner.com/newsroom/>)

Policies ([http://www.gartner.com/technology/about/policies/guidelines\\_ov.jsp](http://www.gartner.com/technology/about/policies/guidelines_ov.jsp))

Privacy (<https://www.gartner.com/privacy>)

Site Index (<http://www.gartner.com/technology/site-index.jsp>)

IT Glossary (<http://www.gartner.com/it-glossary/>)

Contact Gartner ([http://www.gartner.com/technology/contact/contact\\_gartner.jsp](http://www.gartner.com/technology/contact/contact_gartner.jsp))

VALIDE IMPRIMOS SUU

https://www.gartner.com/doc/reprints?id=1-3GDIRPU&ct=160829&st=sb

8/7/2017

https://www.gartner.com/doc/reprints?id=1-3GDIRPU&ct=160829&st=sb

8/7/2017

Page 2

NetScaler

The world's most advanced cloud network platform

NetScaler is the industry's leading web and application delivery controller that maximizes the performance and availability of all applications and data, and also provides secure remote access to any application from any device.



Application availability

Application availability	
Load balancing and L7 content switching	
Microsoft SQL, MySQL	
Application rate control	
IPv6 support	
Traffic domains	
Subscriber-aware traffic steering	
Global server load balancing (GSLB)	
Carrier-Grade Network Address Translation (CGNAT)	
Dynamic routing protocol	
Staged protection and priority queuing	
MQTT support	
Fireplace clustering	
Application acceleration	
Client and server TCP optimizations	
AppCompass	
Application security	
L7 DDoS defenses	
L7 remote and responder	
Extensible NetScaler connector	
AAA for traffic management	
NetScaler Approval with XDR security	
IP Reputation	
Webinar integration	
NetScaler Cloud Connector	
Front-end optimization	
Content bypass	
Domain sharing	
Image optimization	
Sign sheets and JavaScript optimization	
TCP protocol optimization	
Multi-path TCP	
Big and small TCP	

NetScaler

Send us your feedback

Send us your feedback	
NetScaler Insight Center Web Insight	
Application virtual policy builder	
Application service catalogs, templates and wizards	
Configuration wizards	
Role-based administration and AAA for administration	
Native CLI for web interface	
Configure Management Pack for NetScaler	
Cloud Command Center	
Unified Gateway	
Federated Identity	
One URL / SSD using SAML 2.0	
Centralized Policy Management (SmartControl)	
Stateless TCP proxy	
Microsoft Exchange support	
PGOP support	
Monitoring of XenApp/XenDesktop traffic (Real Time)	
Monitoring of XenApp/XenDesktop traffic (Historical)	
Monitoring of Gateway traffic (Real Time)	
Monitoring of Gateway traffic (Historical)	
NetScaler Gateway	
Broad client support for plug-ins	
Customizable web portal	
SSL VPN remote access	
ICA proxy to XenApp and XenDesktop	
Contextual policies for XenApp/XenDesktop (SmartAccess)	
End Point Analysis	
Secure browser-only access (LVPN)	
Always-On	
Integration with StackStorm	

© 2019 Citrix. All rights reserved. Citrix, NetScaler, and the NetScaler logo are trademarks of Citrix. All other trademarks are the property of their respective owners.

	MPX 25100T4	MPX 25100T4	MPX 25100T4	MPX 25100T4
<b>Platform attributes</b>				
Memory	128	128	128	128
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3- 2002/2005/2008/2012)	32x10G SFP+	32x10G SFP+	8x 40GE QSFP+	8x 40GE QSFP+
Transceivers support	10GE SFP+, 1G SFP - Cu	10GE SFP+, 1G SFP - Cu	40GE QSFP+, SR	40GE QSFP+, SR
Raid support	Yes	Yes	Yes	Yes
Pay as you grow and BurstPack license upgrades		Upgrade option to MPX 25160T		Upgrade option to MPX 25200T
<b>Platform performance</b>				
System throughput, Gbps (L7 throughput)	160	100	200	160
L7 HTTP requests/sec	4,600,000	3,700,000	5,200,000	4,600,000
SSL transactions/sec (2K key certificates)*	2,000	1,400	2,000	2,000
ECDFE transactions/sec**	N/A	N/A	N/A	N/A
SSL throughput, Gbps	21	15	30	21
Compression throughput, Gbps	14	10	17	14
ICA Proxy/SSL VPN concurrent users	35,000	35,000	35,000	35,000
Number of instances included/ Maximum number of instances (on SDX models)	N/A	N/A	N/A	N/A
<b>Platform mechanical, environmental and regulatory</b>				
Power supplies	2	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 50-60 Hz	100-240VAC full range, 50-60 Hz	100-240VAC full range, 50-60 Hz	100-240VAC full range, 50-60 Hz
Optional DC power supply	Yes	Yes	Yes	Yes
Max power supply	1000W	1000W	1000W	1000W
Typical/max power consumption	594W/717W	594W/717W	594W/717W	594W/717W
Weight, lbs	60	60	60	60
Height	2U	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets
Depth	28 1/4"/72 cm	28 1/4"/72 cm	28 1/4"/72 cm	28 1/4"/72 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	20%-80%, non-condensing	20%-80%, non-condensing	20%-80%, non-condensing	20%-80%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Critix compliance regulatory model	ZU1P1D	ZU1P1D	ZU1P1D	ZU1P1D

\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
\*\* Hybrid SSL optimization (TLS1-ECDFE-RSA-AES128-SHA 256)

	MPX 25100T4	MPX 25160T4	MPX 25160T4	MPX 25160T4
<b>Platform attributes</b>				
Memory	128	256 GB	256 GB	256 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3- 2002/2005/2008/2012)	8x 40GE QSFP+	8x 40GE QSFP+	8x 40GE QSFP+	8x 40GE QSFP+
Transceivers support	40GE QSFP+, SR	40GE QSFP+, SR	40GE QSFP+, SR	40GE QSFP+, SR
Raid support	Yes	Yes	Yes	Yes
Pay as you grow and BurstPack license upgrades*		Upgrade option to MPX 25160TA, 25200TA	Upgrade option to MPX/SDX 25200A	Upgrade option to MPX/SDX 25160A, 25200A
<b>Platform performance</b>				
System throughput, Gbps (L7 throughput)	100	200	160	100
L7 HTTP requests/sec	3,200,000	5,200,000	4,000,000	3,000,000
SSL transactions/sec (2K key certificates)*	1,400	69,000	69,000	43,000
ECDFE transactions/sec**	N/A	56,000	47,000	29,000
SSL throughput, Gbps	15	46	42	34
Compression throughput, Gbps	10	17	14	10
ICA Proxy/SSL VPN concurrent users	35,000	35,000	20,000	20,000
Number of instances included/ Maximum number of instances (on SDX models)	N/A	115/115	70/115	70/115
<b>Platform mechanical, environmental and regulatory</b>				
Power supplies	2	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 50-60 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes	Yes
Max power supply	1000W	822W	822W	822W
Typical/max power consumption	594W/717W	300W 1024 BTU/Hr	300W 1024 BTU/Hr	300W 1024 BTU/Hr
Weight, lbs	60	60	60	60
Height	2U	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets
Depth	28 1/4"/72 cm	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	20%-80%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Critix compliance regulatory model	ZU1P1D	ZU1P1D	ZU1P1D	ZU1P1D

\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
\*\* Hybrid SSL optimization (TLS1-ECDFE-RSA-AES128-SHA 256)

MULTICOMPUTER SALES  
SANTO DOMINGO, DOMINICAN REPUBLIC  
Santo Domingo, D.R.







NetScaler

Data Sheet

Platform attributes	64 GB	64 GB	64 GB	64 GB
Memory	64 GB	64 GB	64 GB	64 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE 802.3- 2002/2005/2008/2012)	4x 40GE QSFP+, 4x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 4x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 4x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 4x 10GE SFP+, 4x 10GBase-T
Transceivers support	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR
Raid support	Yes	Yes	Yes	Yes
Pay as you grow and Burst- Pack license upgrades	Upgrade option to MPX 14100- 40C	Upgrade option to MPX 14100- 40C	Upgrade option to MPX 14080- 40C, 14100-40C	Upgrade option to MPX 14040- 40C, 14080-40C, 14100-40C, 14100-40C
<b>Platform performance</b>				
System throughput, Gbps (L7 throughput)	100	80	60	40
L7 HTTP requests/sec (MPX/SDX)	2,800,000	2,400,000	2,400,000	2,400,000
SSL transactions/sec (2K key certificates)*	69,000	69,000	69,000	42,000
ECDSA transactions/sec**	33,500	32,000	31,500	25,500
SSL throughput, Gbps	45	43	40	34
Compression throughput, Gbps	8.6	8.5	7.7	6
ICA Proxy/SSL VPN concurrent users	20,000	20,000	20,000	20,000
Number of instances included (for SDX models)	N/A	N/A	N/A	N/A
<b>Platform mechanical, environmental and regulatory</b>				
Power supplies	2	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes	Yes
Max power supply	528W	528W	528W	528W
Typical/max power consumption	300W/1024 BTU/Hr	300W/1024 BTU/Hr	300W/1024 BTU/Hr	300W/1024 BTU/Hr
Weight, lbs	60	60	60	60
Height	2U	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 A1 G30 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 A1 G30 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets
Depth	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	ZUP18	ZUP18	ZUP18	ZUP18

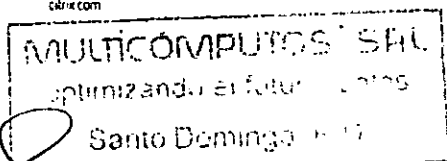
\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
\*\* Hybrid SSL optimization (TLS1-ECDSA-RSA-AES128-SHA 256)

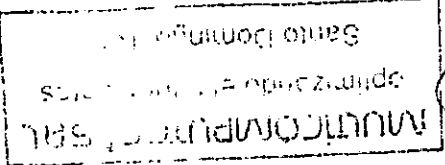
NetScaler

Data Sheet

Platform attributes	64 GB	64 GB	64 GB	64 GB
Memory	64 GB	64 GB	64 GB	64 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE 802.3- 2002/2005/2008/2012)	4x 40GE QSFP+, 4x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 16x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 16x 10GE SFP+, 4x 10GBase-T	4x 40GE QSFP+, 16x 10GE SFP+, 4x 10GBase-T
Transceivers support	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR	40GE QSFP+, SR, 10GE SFP+, SR, LR
Raid support	Yes	Yes	Yes	Yes
Pay as you grow and Burst- Pack license upgrades	Upgrade option to MPX 14040- 40C, 14080-40C, 14100-40C, 14100-40C	Upgrade option to MPX/SDX 14100-40G	Upgrade option to MPX/SDX 14080-40G, 14100-40G	Upgrade option to MPX/SDX 14080-40G, 14100-40G
<b>Platform performance</b>				
System throughput, Gbps (L7 throughput)	20	100	80	60
L7 HTTP requests/sec (MPX/SDX)	2,400,000	2,800,000	2,800,000	2,400,000
SSL transactions/sec (2K key certificates)*	42,000	69,000	69,000	69,000
ECDSA transactions/sec**	20,000	33,500	32,000	31,500
SSL throughput, Gbps	34	45	43	40
Compression throughput, Gbps	6	8.6	8.5	7.7
ICA Proxy/SSL VPN concurrent users	20,000	20,000	20,000	20,000
Number of instances included (for SDX models)	N/A	25/25	25/25	25/25
<b>Platform mechanical, environmental and regulatory</b>				
Power supplies	2	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes	Yes
Max power supply	528W	528W	528W	528W
Typical/max power consumption	300W/1024 BTU/Hr	300W/1024 BTU/Hr	300W/1024 BTU/Hr	300W/1024 BTU/Hr
Weight, lbs	60	60	60	60
Height	2U	2U	2U	2U
Width	EIA 310-D, IEC 60297, DIN 41494 A1 G30 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 A1 G30 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 A1 G30 rack width with mount- ing brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mount- ing brackets
Depth	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	ZUP18	ZUP18	ZUP18	ZUP18

\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
\*\* Hybrid SSL optimization (TLS1-ECDSA-RSA-AES128-SHA 256)





Sheet 8

Performance varies depending on options deployed, contact your Client sales representative for details

Table with columns: Platform attributes, Memory, Ethernet ports, Transmitters support, Red support, Pay as you grow and Buy-It-Now, Platform performance, System throughput, L7 HTTP requests/sec, L7 HTTP requests/sec (MFX/SDX), SSL transactions/sec, E2E transactions/sec, SSL Throughput, Compression Throughput, KPI Throughput, Number of instances, Platform mechanical, environmental and regulatory, Power supplies, Input voltage and frequency ranges, Output DC power supply, Max power supply, Typical/max power consumption, Weight, Height, Width, Depth, Operating temperature, Allowed relative humidity, Safety certifications, Electromagnetic emissions, Regulatory compliance, Model.

Networker Data Sheet

Performance varies depending on options deployed, contact your Client sales representative for details

Table with columns: Platform attributes, Memory, Ethernet ports, Transmitters support, Red support, Pay as you grow and Buy-It-Now, Platform performance, System throughput, L7 HTTP requests/sec, L7 HTTP requests/sec (MFX/SDX), SSL transactions/sec, E2E transactions/sec, SSL Throughput, Compression Throughput, KPI Throughput, Number of instances, Platform mechanical, environmental and regulatory, Power supplies, Input voltage and frequency ranges, Output DC power supply, Max power supply, Typical/max power consumption, Weight, Height, Width, Depth, Operating temperature, Allowed relative humidity, Safety certifications, Electromagnetic emissions, Regulatory compliance, Model.

Networker Data Sheet

NetScaler Data Sheet

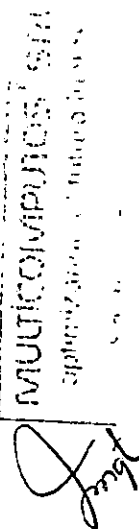
Platform attributes	48 GB	64 GB	80 GB
Memory	48 GB	64 GB	80 GB
Ethernet ports (Published Ethernet interfaces compatible per IEEE802.3-2002/7005/7009/2012)	8x 10GbASE-X SFP, AND 4x 10GbASE-X SFP (fiber or copper)	16x 10GbASE-X SFP, AND 4x 10GbASE-X SFP (fiber or copper)	16x 10GbASE-X SFP, AND 8x 10GbASE-X SFP (fiber or copper)
Transceivers support	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu
Raid support	No	Yes	No
Pay as you grow and BurstPeak license upgrades	Upgrade option to MPV/SDX 10540 and TIS42	Upgrade option to MPV/SDX 14060 FPS	Upgrade option to MPV/SDX 14060 FPS, 14080 FPS
Platform performance			
System throughput, Gbps (L7 throughput)	30	30	35
L7 HTTP requests/sec (MPV/SDX)	2,000,000/2,000,000	1,600,000	1,200,000
SSL transactions/sec (ZK key encryption)	30,000	25,000	6,000
ECDFE transactions/sec**	N/A	N/A	N/A
SSL throughput, Gbps	17	18	4.5
Compression throughput, Gbps	6.5	5	6.5
CA Proxy/SSL VPN concurrent users	20,000	20,000	10,000
Number of instances included/Maximum number of instances (on SDX models)	20/20	25/25	N/A
Platform mechanical, environmental and regulatory			
Power supplies	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes
Max power supply	650W 2219 BTU/Hr	528W	450W 1536 BTU/Hr
Typical/max power consumption	500W 1706 BTU/Hr	300W 1024 BTU/Hr	360W 1228 BTU/Hr
Weight, lbs	45	60	30
Height	2U	2U	2U
Width	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets
Depth	28" / 712 cm	28" / 712 cm	28" / 712 cm
Operating temperature	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance standard	RoHS, WEEE, IEC 60950-1, Level 2	RoHS, WEEE, IEC 60950-1, Level 2	RoHS, WEEE, IEC 60950-1, Level 2
Other compliance regulatory model	RoHS, WEEE	RoHS, WEEE	MPV INRGE BUSFP+ FPS

\* Performance varies depending on options deployed, contact your Citrix sales representative for details  
 \*\* Hybrid SSL optimization (TIS1-ECDFE-45A-AL0276-SHA-256)

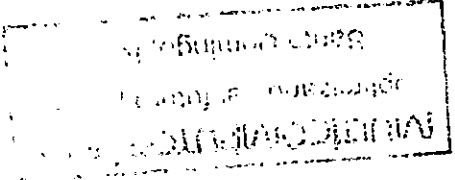
NetScaler Data Sheet

Platform attributes	48 GB	64 GB	80 GB
Memory	48 GB	64 GB	80 GB
Ethernet ports (Published Ethernet interfaces compatible per IEEE802.3-2002/7005/7009/2012)	8x 10GbASE-X SFP, AND 4x 10GbASE-X SFP (fiber or copper)	16x 10GbASE-X SFP, AND 4x 10GbASE-X SFP (fiber or copper)	16x 10GbASE-X SFP, AND 8x 10GbASE-X SFP (fiber or copper)
Transceivers support	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu	10Gb SFP+, SR, LR, 16 cu 1Gb SFP+, SR, LR, 16 cu
Raid support	No	Yes	No
Pay as you grow and BurstPeak license upgrades	Upgrade option to MPV/SDX 10540 and TIS42	Upgrade option to MPV/SDX 14060 FPS	Upgrade option to MPV/SDX 14060 FPS, 14080 FPS
Platform performance			
System throughput, Gbps (L7 throughput)	30	30	35
L7 HTTP requests/sec (MPV/SDX)	2,000,000/2,000,000	1,600,000	1,200,000
SSL transactions/sec (ZK key encryption)	30,000	25,000	6,000
ECDFE transactions/sec**	N/A	N/A	N/A
SSL throughput, Gbps	17	18	4.5
Compression throughput, Gbps	6.5	5	6.5
CA Proxy/SSL VPN concurrent users	20,000	20,000	10,000
Number of instances included/Maximum number of instances (on SDX models)	20/20	25/25	N/A
Platform mechanical, environmental and regulatory			
Power supplies	2	2	2
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	Yes
Max power supply	650W 2219 BTU/Hr	528W	450W 1536 BTU/Hr
Typical/max power consumption	500W 1706 BTU/Hr	300W 1024 BTU/Hr	360W 1228 BTU/Hr
Weight, lbs	45	60	30
Height	2U	2U	2U
Width	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets	EIA 310-D, EC 60297, DIN 41894, SEC80 rack width with mounting brackets
Depth	28" / 712 cm	28" / 712 cm	28" / 712 cm
Operating temperature	0-40C	0-40C	0-40C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standard	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance standard	RoHS, WEEE, IEC 60950-1, Level 2	RoHS, WEEE, IEC 60950-1, Level 2	RoHS, WEEE, IEC 60950-1, Level 2
Other compliance regulatory model	RoHS, WEEE	RoHS, WEEE	MPV INRGE BUSFP+ FPS

\* Performance varies depending on options deployed, contact your Citrix sales representative for details  
 \*\* Hybrid SSL optimization (TIS1-ECDFE-45A-AL0276-SHA-256)



face



Performance varies depending on clients deployed, contact your Citrix sales representative for details

Performance varies depending on clients deployed, contact your Citrix sales representative for details

Platform architecture	Memory	Ethernet ports	Platform performance	System throughput, Gbps	[L7 throughput]	[L7 HTTP requests/sec (MFX/SDX)]	SSL transactions/sec	SSL transactions/sec (key certificates)	ECHE transactions/sec	SSL throughput, Gbps	Compression throughput, Gbps	CA Proxy/SSL VPN concurrent users	Number of instances included/Maximum number of instances (on SDX models)	Platform mechanical, environmental and regulatory	Power supplies	Input voltage and frequency ranges	Optional DC power supply	Max power supply	Typical power consumption	Weight, lbs	Height	Width	Depth	Operating temperature	Allowed relative humidity	Safety certifications	Electromagnetic emissions certifications and susceptibility standards	Regulatory compliance	Citrix compliance regulatory model
16 GB	2x 10GbASE-X SFP, AND 8x 1000BASE-X SFP (fiber or copper)	2x 10GbASE-X SFP, AND 8x 1000BASE-X SFP (fiber or copper)	1000 SFP, SR LR	10	10	700,000	500,000	4,000	N/A	3.6	2.0	360W 12.29 BTU/Hr	N/A	EIA 310-D, EC 60292, DIN 4194, SC480	2	100-240VAC full range, 47-63 Hz	Yes	450W 153.6 BTU/Hr	30	2U	28" / 71.2 cm	0-40C	5%-95%, non-condensing	CSA	FCC Part 15 Class A, FCC CE, VCCI, CNS, AN/NES	Regulatory compliance	MFX 2X10GE 8xSFP+ SFPs		
16 GB	2x 10GbASE-X SFP, AND 8x 1000BASE-X SFP (fiber or copper)	1000 SFP, SR LR	1000 SFP, SR LR	6	6	500,000	10,000	4,000	N/A	3.6	2.0	360W 12.29 BTU/Hr	N/A	EIA 310-D, EC 60292, DIN 4194, SC480	2	100-240VAC full range, 47-63 Hz	Yes	450W 153.6 BTU/Hr	30	2U	28" / 71.2 cm	0-40C	5%-95%, non-condensing	CSA	FCC Part 15 Class A, FCC CE, VCCI, CNS, AN/NES	Regulatory compliance	MFX 2X10GE 8xSFP+ SFPs		
16 GB	2x 10GbASE-X SFP, AND 8x 1000BASE-X SFP (fiber or copper)	1000 SFP, SR LR	1000 SFP, SR LR	3	3	200,000	10,000	2,000	N/A	3.6	2.0	360W 12.29 BTU/Hr	N/A	EIA 310-D for 19-inch racks	2	100-240VAC full range, 50-60 Hz	Yes	450W 153.6 BTU/Hr	30	2U	28" / 71.2 cm	0-45C	5%-95%, non-condensing	CSA	FCC Part 15 Class A, FCC CE, VCCI, CNS, AN/NES	Citrix compliance regulatory model	MFX 2X10GE 8xSFP+ SFPs		

Performance varies depending on clients deployed, contact your Citrix sales representative for details

Performance varies depending on clients deployed, contact your Citrix sales representative for details

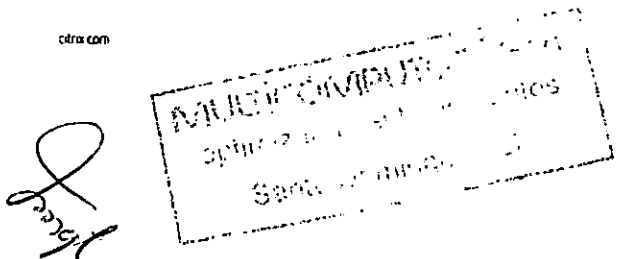
Platform architecture	Memory	Ethernet ports	Platform performance	System throughput, Gbps	[L7 throughput]	[L7 HTTP requests/sec (MFX/SDX)]	SSL transactions/sec	SSL transactions/sec (key certificates)	ECHE transactions/sec	SSL throughput, Gbps	Compression throughput, Gbps	CA Proxy/SSL VPN concurrent users	Number of instances included/Maximum number of instances (on SDX models)	Platform mechanical, environmental and regulatory	Power supplies	Input voltage and frequency ranges	Optional DC power supply	Max power consumption	Weight, lbs	Height	Width	Depth	Operating temperature	Allowed relative humidity	Safety certifications	Electromagnetic emissions certifications and susceptibility standards	Regulatory compliance	Citrix compliance regulatory model
22 GB	4x 10Gb SFP, 6x 10/100/1000 (4x 10Gb SFP, 6x 10/100/1000 CU)	4x 10Gb SFP, 6x 10/100/1000 (4x 10Gb SFP, 6x 10/100/1000 CU)	1000 SFP, SR LR	20	20	1,700,000	40,000	16,000	10,000	4,000	5	330W	2/2	EIA 310-D for 19-inch racks	1 (2nd optional)	100-240VAC full range, 50-60 Hz	Yes	300W 81.0 BTU/Hr	25	2U	28" / 61 cm	0-45C	5%-95%, non-condensing	CSA	FCC (CE), FCCA, FCCB, FCCC, FCCD, FCS, AN/NES	Regulatory compliance	MFX 2X10GE 8xSFP+ SFPs	
22 GB	4x 10Gb SFP, 6x 10/100/1000 (4x 10Gb SFP, 6x 10/100/1000 CU)	1000 SFP, SR LR	1000 SFP, SR LR	4	4	1,000,000	40,000	16,000	10,000	4,000	5	330W	2/2	EIA 310-D for 19-inch racks	1 (2nd optional)	100-240VAC full range, 50-60 Hz	Yes	300W 81.0 BTU/Hr	25	2U	28" / 61 cm	0-45C	5%-95%, non-condensing	CSA	FCC (CE), FCCA, FCCB, FCCC, FCCD, FCS, AN/NES	Regulatory compliance	MFX 2X10GE 8xSFP+ SFPs	
22 GB	4x 10Gb SFP, 6x 10/100/1000 (4x 10Gb SFP, 6x 10/100/1000 CU)	1000 SFP, SR LR	1000 SFP, SR LR	10	10	700,000	10,000	22,000	10,000	4,000	5	330W	N/A	EIA 310-D for 19-inch racks	1 (2nd optional)	100-240VAC full range, 50-60 Hz	Yes	300W 81.0 BTU/Hr	25	2U	28" / 61 cm	0-45C	5%-95%, non-condensing	CSA	FCC (CE), FCCA, FCCB, FCCC, FCCD, FCS, AN/NES	Citrix compliance regulatory model	MFX 2X10GE 8xSFP+ SFPs	

Platform attributes			
Memory	16 GB	16 GB	16 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3-2002/2003/2008/2012)	2x10GE SFP+, 6x10/100/1000 CU	2x10GE SFP+, 6x10/100/1000 CU	2x10GE SFP+, 6x10/100/1000 CU
Transceivers support	10GE SFP+, SR, LR, 1G CU	10GE SFP+, SR, LR, 1G CU	10GE SFP+, SR, LR, 1G CU
Raid support	No	No	No
Pay as you grow and BurstPack license upgrades		Upgrade option to MPX 5910	Upgrade option to MPX 5905 and 5910
Platform performance			
System throughput, Gbps (L7 throughput)	10	5	1
L7 HTTP requests/sec (MPX/SDX)	900,000	700,000	450,000
SSL transactions/sec (2K key certificates)*	12,000	6,000	4,000
ECDSA transactions/sec	6,000	3,000	1,700
SSL throughput, Gbps	8	5	1
Compression throughput, Gbps	2.5	1.5	1
ICA Proxy/SSL VPN concurrent users	5,000	5,000	5,000
Number of instances included/Maximum number of instances (on SDX models)	N/A	N/A	N/A
Platform mechanical, environmental and regulatory			
Power supplies	1 (2nd optional)	1 (2nd optional)	1 (2nd optional)
Input voltage and frequency ranges	100-240VAC full range	100-240VAC full range	100-240VAC full range
Optional DC power supply	Yes	Yes	Yes
Max power consumption	336W	336W	336W
Typical power consumption	300W 840 BTU/hr	300W 840 BTU/hr	300W 840 BTU/hr
Weight, lbs	25	25	25
Height	1U	1U	1U
Width	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks	EIA 310-D for 19-inch racks
Depth	24" / 61 cm	24" / 61 cm	24" / 61 cm
Operating temperature	0-45C	0-45C	0-45C
Allowed relative humidity	5%-95%, non-condensing	5%-95%, non-condensing	5%-95%, non-condensing
Safety certifications	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standards	FCC, CE, (VCCI), (RCM), (CECC), (KCC), (BSI), (NOM), (CETC)	FCC, CE, (VCCI), (RCM), (CECC), (KCC), (BSI), (NOM), (CETC)	FCC, CE, (VCCI), (RCM), (CECC), (KCC), (BSI), (NOM), (CETC)
Regulatory compliance	RoHS, WEEE, REACH	RoHS, WEEE, REACH	RoHS, WEEE, REACH
CE compliance regulatory model	TUPTA	TUPTA	TUPTA

\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
 Platforms shown above are only supported on the firmware version installed from manufacturing

Platform attributes				
Memory	32 GB	32 GB	8 GB	8 GB
Ethernet ports (Published Ethernet interfaces compliant per IEEE802.3-2002/2003/2008/2012)	6x10/100/1000 BASE-T AND 6x1000BASE-X SFP (fiber or copper) OR 6x10/100/1000 BASE-T AND 2x10G BASE-X SFP+	6x10/100/1000 BASE-T AND 6x1000BASE-X SFP (fiber or copper) OR 6x10/100/1000 BASE-T AND 2x10G BASE-X SFP+	6x10/100/1000 BASE-T	6x10/100/1000 BASE-T
Transceivers support	10GE SFP+, SR, LR, 1GE SFP, SX, LX	10GE SFP+, SR, LR, 1GE SFP, SX, LX	No	No
Raid support	No	No	No	No
Pay as you grow and BurstPack license upgrades		Upgrade option to MPX/SDX 60T5		Upgrade option to MPX 5650
Platform performance				
System throughput, Gbps (L7 throughput)	15	5	5	0.5
L7 HTTP requests/sec (MPX/SDX)	1,200,000	375,000	350,000	175,000
SSL transactions/sec (2K key certificates)*	11,000	6,500	2,800	1,500
ECDSA transactions/sec**	N/A	N/A	N/A	N/A
SSL throughput, Gbps	6	4	2	0.5
Compression throughput, Gbps	3.5	2.3	3	0.5
ICA Proxy/SSL VPN concurrent users	10,000	10,000	5,000	5,000
Number of instances included/Maximum number of instances (on SDX models)	2/5	N/A	N/A	N/A
Platform mechanical, environmental and regulatory				
Power supplies	1 (2nd optional)	1 (2nd optional)	1	1
Input voltage and frequency ranges	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz	100-240VAC full range, 47-63 Hz
Optional DC power supply	Yes	Yes	No	No
Max power consumption	250W 853 BTU/hr	250W 853 BTU/hr	180W 614 BTU/hr	180W 614 BTU/hr
Typical power consumption	185W 631 BTU/hr	185W 631 BTU/hr	135W 461 BTU/hr	135W 461 BTU/hr
Weight, lbs	32	32	32	32
Height	1U	1U	1U	1U
Width	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mounting brackets	EIA 310-D, IEC 60297, DIN 41494 SC480 rack width with mounting brackets
Depth	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm	28" / 71.2 cm
Operating temperature	0-40C	0-40C	0-40C	0-40C
Allowed relative humidity	10%-90%, non-condensing	10%-90%, non-condensing	10%-90%, non-condensing	10%-90%, non-condensing
Safety certifications	CSA	CSA	CSA	CSA
Electromagnetic emissions certifications and susceptibility standards	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES	FCC (Part 15 Class A), DoC, CE, VCCI, CNS, AN/NES
Regulatory compliance	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE	RoHS, WEEE
Citrix compliance regulatory model	NS 2x10GE SFP+ 6XCU	NS 2x10GE SFP+ 6XCU	NS 6xCu	NS 6xCu

\* Performance varies depending on ciphers deployed, contact your Citrix sales representative for details  
 \*\* Hybrid SSL optimization (TLS1-ECDSA-RSA-AES128-SHA 256)  
 For information on VPX, please refer to the VPX datasheet



## Technical aspects

### Unified Gateway

- Provides consolidation of secure remote access infrastructure with One URL
- Provides SAML 2.0 Federated identity to provide Single Sign-On across all applications whether in a datacenter or in a cloud
- One URL to access any application
- Always-On allows auto reconnection of SSL VPN session when users are moving between networks
- Integration with StoreFront allows single URL changes from StoreFront to Gateway portal and vice versa
- Gateway through for monitoring and troubleshooting all Gateway traffic for issues like authentication and CPA failures, single sign-on failures etc.
- Refactor authentication for all applications
- Stillness RDP proxy
- Support for Linux (Ubuntu 14.04, 12.04, Ubuntu 12.04, 32bit / 64bit)
- Support for Mac (OS X 10.9 Mavericks, OS X 10.10 Yosemite)
- Support for Windows 7, 8, and 8.1 (32bit / 64bit)
- Support for iOS 7.1 or later. Compatible with iPhone, iPad and iPod touch
- Support for Android 4.1 & 4.2 (every brand), 4.4 & 4.4 KitKat, & 5.0 (all ops)

### Secure access

- KAX/SD-WAN integration
- Device certificate scanning
- Single sign-on using HTML5/JavaScript/SAML etc.
- SmartAccess: Adaptive application and action control enforced on XenApp and XenDesktop servers
- SmartControl: Adaptive application and action control enforced on NetScaler Unified Gateway, thereby providing centralized policy management and security at the edge
- Integrated NetScaler Unified Gateway SSL VPN
- Below NetScaler 11.1 Standard and Enterprise Editions include (5) Universal Licenses. Platinum Edition includes (100) Universal Licenses. Starting NetScaler 11.1, Standard includes 500 Universal Licenses, Enterprise Editions include (1000) Universal Licenses and there are no Universal License requirements with Platinum Edition Universal License entitlements as a per MA per or per cluster depending on how you deploy NetScaler.

- Endpoint analysis of user device
- SAML 2.0 and refactor, passwords for single sign-on to applications running behind NetScaler Unified Gateway
- AAA traffic management
- AAA traffic management
- SAML 2.0 and HTML5/JavaScript support for configuring NetScaler with single sign-on (SSO)
- Support for Active Directory, LDAP, RADIUS, TACACS+, OCS, Diameter etc.

### 16-7 traffic management

#### Layer 4 load balancing (LB)

- Protocols supported: TCP, UDP, FTP, HTTP, HTTPS, DNS (TCP and UDP), SIP (over UDP), RTP, RADIUS, DIAMETER, SQL, RDP, IS-IS, SNMP
- Algorithms: Round Robin, Least Packets, Least Bandwidth, Least Connections, Response Time, Hashing (URL, Domain, Source IP, Destination IP, and CustomID), SHMP-provided metric, Server Application State Protocol (SASP)
- Session persistence: Source IP, cookie, server, group,

- SSL session, SIP CALLER, token based, SESSIONID, Diameter AVP
- Session protocols: TCP, UDP, SSL\_TCP, Multi-path TCP, SPDY
- Server monitoring: Ping, TCP, URL, FQDN, scriptable health checks, Dynamic Server Response Time
- Link load balancing
- CloudEdge load balancing

#### Layer 7 content switching

- Policies: URL, URL Query, URL, Wildcard, Domain, Source/Destination IP, HTTP Header, Custom, HTTP and TCP Payload Values, UDP, Diameter AVP
- Switch requests based on protocol of incoming packets

#### Database load balancing

- Support for: Microsoft SQL Server and MySQL
- Switching algorithms include SQL query parameters such as token and database names and command parameters
- Token-based load balancing provides advanced configuration for persistence and fault tolerant deployments

#### TrScale Clustering

- "Scale-Out" with clustering up to 32 NetScaler appliances into single system image and up to 3 Tbps throughput
- Configuration Coordinator node for centralized management and synchronization
- Compatible with Pay-As-You-Grow and Burst Face performance upgrades
- Traffic distribution mechanisms include Equal Cost Multiple Path (ECMP), Link sets, and Cluster Link Aggregation Group (CLAG)
- Available on NetScaler MPX, SDX and VPX and with NetScaler EE and PE editions
- Modules may be configured on all nodes in a cluster or using "spooled VPS" they are added only to a select subset of nodes

#### Rate-based policy enforcement

- Trigger NetScaler policies based upon connections per second, packets per second, or bandwidth used
- Source or destination based upon header or payload information

#### Traffic domains

- Allows overlapping IP addresses
- Promotes separate routing flows within a single appliance
- Enables basic multi-tenancy implementations

#### Admin Partitioning

- Independent instances that share resources on the appliance
- Maximum number of 512 admin partitions per appliance

#### Global server load balancing (GSLB)

- Algorithms: site health, geographic proximity, network proximity, connections, bandwidth, AG-ESSL VPN users
- Site health checking on status, connection load, packet loss, SHMP-provided metrics

#### Surge protection and priority queuing

- Adaptive rate control for TCP connections and HTTP requests
- Prioritized transaction dispatchs for critical application requests

#### Carrier-grade Network Address Translation

- Support for: Full-cone NAT, Deterministic NAT,

- Endpoint Independent Mapping and Filtering, Hair-pinning
- Application Layer Gateways: FTP, FTPS, ICMP, SIP, RTPS, PPTP, GRE

#### Subscriber-aware traffic steering

- Policy control interface: Gx, RADIUS

#### Application acceleration

- TCP optimization
- Multiplexing, buffering, connection keep alive, window scaling, selective acknowledge, fast ramp, TCP Westwood

#### AppCompress

- GUI-based compression for HTTP traffic, AppCache?
- Caching for static and dynamic application content
- HTTP GET and POST method support
- Policies defined based upon HTTP header and body values

#### Application security

- DoS attack defense
- Continue service to legitimate users when protecting against attacks such as SYN Flood, HTTP DoS, and Ping of Death
- ICMP and UDP rate control

#### Content rewriting and response control

- Policy-based bidirectional rewriting of HTTP header and payload elements
- Policy-based redirection of incoming requests
- Body URL rewrite
- Responder module
- Custom responses and redirects
- Policy-based routing
- Network aware policies

#### SSL Encryption

- Supports Thales nShield and SafeNet HSM integration
- DNSEC
- DNS proxy
- Authoritative DNS
- DNS signing

#### Packet filtering

- Layer 3 and 4 Access Control Lists (ACL)
- Network Address Translation (NAT)
- IPv4/IPv6 Network Address Translation (NAT)

#### NetScaler AppFirewall with hybrid security model

- Positive security model protects against: Buffer Overflow, CGI-HTTP Parameter Manipulation, Form/Hidden Field Manipulation, Forward Briversion, Cookie or Session Poisoning, Broken ACLs, Cross-Site Scripting (XSS), Command Injection, SQL Injection, Error Triggering, Sensitive Information Leak, Insecure Use of Cryptography, Server Misconfigurations, Back Doors and Denial of Service, Rate-based Policy Enforcement, Well known Platform Vulnerabilities, Zero-day Exploits, Cross Site Request Forgery (CSRF), credit card and other sensitive data leakage prevention
- Negative security model with dynamically updated signatures to protect against L7 and HTTP application vulnerabilities
- Integrates with third party scanning tools
- Common event format (CEF) logs
- XML security: XML, Denial of Service (DoS)

- XML, SQL injection and cross site scripting, XML message validation, format checks, WS basic profile compliance, XML API/JSON injection attachment check, iQuery injection protection

#### IP Reputation service

- Enhanced service that provides a continuously updated list of malicious IP addresses in near real time

#### NetScaler Cloud Connector

- Network connectivity protection via IPSec security
- Datacenter extension through GRE based network bridging

#### Support for XenMobile MDM

- First end optimization scalable to over 100,000 concurrent users

#### NetScaler Cloud Connector

- Network connectivity protection via IPSec security
- Datacenter extension through GRE based network bridging

#### Support for XenMobile MDM

- First end optimization scalable to over 100,000 concurrent users

#### Network integration

- Static routes, managed static routes, weighted static routes
- OSPF, RIPv2, BGP2
- VLAN 802.1Q
- Link Aggregation (LACP)
- Stateful IPv6 to IPv4 network address translation and DNS64
- Static and dynamic network address translation from IPv4 to IPv6

#### High availability

- Active/Passive
- Active/Active
- VRRP
- ECMP
- Conversion mirroring

#### Simplified Installation and management

- User interface
- Graphical application visualizer
- Secure web-based GUI
- CLI Telet, SSH, Console
- Real-time performance dashboard
- URL, SSLB Application Firewall, and EdgeSign™ for NetScaler configuration wizards
- XenApp configuration wizards

#### Policy management

- AppExpert Visual Policy Builder
- Policy enforceability via HTTP service catalogs
- AppExpert templates
- AppExpert Visualizers

#### Client Command Center

- Centralized configuration and management of over 200 NetScaler appliances

#### NetScaler Insight Center and AppFloor

- NetScaler Insight Center is a software solution enabling traffic visibility, it includes HTTP Insight, and Web Insight

NetScaler  
 Unified Gateway  
 16-7 traffic management  
 Layer 4 load balancing (LB)  
 Layer 7 content switching  
 Database load balancing  
 TrScale Clustering  
 Rate-based policy enforcement  
 Traffic domains  
 Admin Partitioning  
 Global server load balancing (GSLB)  
 Surge protection and priority queuing  
 Carrier-grade Network Address Translation

Citrix.com  
 NetScaler  
 Unified Gateway  
 16-7 traffic management  
 Layer 4 load balancing (LB)  
 Layer 7 content switching  
 Database load balancing  
 TrScale Clustering  
 Rate-based policy enforcement  
 Traffic domains  
 Admin Partitioning  
 Global server load balancing (GSLB)  
 Surge protection and priority queuing  
 Carrier-grade Network Address Translation





**MULTICOMPUTOS, S.R.L.**  
**Capital Social Suscrito y Pagado: RD\$6,545,300.00**  
**Domicilio Social: Ave. Abraham Lincoln No. 1007, Ensanche Piantini, D. N.**  
**Santo Domingo, República Dominicana**

Quienes suscriben, señores: **VIRGILIO SALVADOR ALBERT FIORINELLI**, dominicano, mayor de edad, casado, ingeniero, portador de la cédula de identidad y electoral número 001-0201987-7, domiciliado y residente en la Calle Transversal No. 5, Arroyo Hondo, de esta ciudad de Santo Domingo, Distrito Nacional y **RAQUEL MARIA MENICUCCI DE ALBERT**, dominicana, mayor de edad, casada, licenciada en administración, portadora de la cédula de identidad y electoral número 001-0202854-5, domiciliada y residente en la Calle Transversal No. 5, Arroyo Hondo, de esta ciudad de Santo Domingo, Distrito Nacional; han acordado constituir una Sociedad de Responsabilidad Limitada y con tal propósito han formulado, para regir la misma, los siguientes estatutos:

**TRANSFORMACION Y CONSTITUCIÓN DE LA SOCIEDAD  
MULTICOMPUTOS, S. R. L.**

**ESTATUTOS**

**CAPÍTULO 1**

**DE LA FORMA, RÉGIMEN JURÍDICO, DENOMINACIÓN, OBJETO, DOMICILIO Y  
DURACIÓN**

**Artículo 1. Forma y Régimen Jurídico.** Ha quedado constituida, entre quienes suscriben el presente acto, una Sociedad de Responsabilidad Limitada, la cual se regirá por las leyes de la República Dominicana, especialmente por la Ley General de Sociedades Comerciales y Empresas Individuales de Responsabilidad Limitada, No. 479-08, (en lo adelante, "la Ley"), así como por las disposiciones contractuales contenidas en estos estatutos y sus modificaciones posteriores.

**Artículo 2. Denominación.** La sociedad se denominará "MULTICOMPUTOS, S.R.L."

**Artículo 3. Objeto Social.** La sociedad tiene por objeto principal dedicarse al negocio de soluciones de tecnología de información a través del desarrollo, consultoría, implementación, soporte, importación, fabricación, distribución, exportación, representación de casa nacionales y extranjeras de equipos (Hardware), programas (Software) de computadoras, redes, comunicación, telefonía, seguridad, aplicaciones, gestión y monitoreo entre otros; inversión en valores o acciones de otras empresas y entidades, así como realizar cualquier otra actividad de lícito comercio. La empresa podrá llevar a cabo también cualquier actividad relacionada directamente o indirectamente de acuerdo con las disposiciones de la Gerencia. De manera general, la sociedad podrá realizar todas las operaciones civiles, comerciales, industriales, financieras, mobiliarias e inmobiliarias, o de cualquier otra naturaleza, que se relacionen directa o indirectamente con dicho objeto o que sean susceptibles de facilitar su continuidad y expansión.

**Párrafo.** Las actividades referidas podrán también ser desarrolladas por la sociedad, total o parcialmente, de manera directa o indirecta, mediante su participación en otras sociedades con objeto análogo.

**Artículo 4. Domicilio Social.** El domicilio de la sociedad se establece en la Ave. Abraham Lincoln No. 1007, Ensanche Piantini, D. N., Santo Domingo, D. N., República Dominicana. La gerencia de la sociedad podrá trasladar el domicilio social a otro lugar dentro del mismo municipio o a otra provincia, al igual que establecer, suprimir o trasladar sucursales, agencias o delegaciones, dentro y fuera del territorio nacional.

**Artículo 5. Duración.** La sociedad será de duración indefinida. Podrá disolverse en los casos y con las formalidades establecidas en la Ley y en estos estatutos.

## CAPÍTULO II DE LOS APORTES, CAPITAL SOCIAL Y PRESTACIONES ACCESORIAS

**Artículo 6. Aportes.** Los socios, conforme al número de acciones que poseían con anterioridad a los presentes estatutos, tienen como aportes en la presente sociedad, los que se indican a continuación:

sesenta y cinco mil trescientos veintisiete (65,327)

- 1) **VIRGILIO SALVADOR ALBERT FIORINELLI**, tiene un aporte de seis millones quinientos treinta y dos mil setecientos pesos dominicanos con 00/100 (RD\$6,532,700.00);
- 2) **RAQUEL MARIA MENICUCCI DE ALBERT**, tiene un aporte de doce mil seiscientos pesos dominicanos con 00/100 (RD\$12,600.00);

Total de aportes: **SEIS MILLONES QUINIENTOS CUARENTA Y CINCO MIL TRESCIENTOS PESOS DOMINICANOS CON 00/100 (RD\$6,545,300.00).**

**Artículo 7. Capital Social:** Como consecuencia de los aportes realizados conforme al número de acciones que posee cada socio en la sociedad, el capital social se fija en la suma de **SEIS MILLONES QUINIENTOS CUARENTA Y CINCO MIL TRESCIENTOS PESOS DOMINICANOS CON 00/100 (RD\$6,545,300.00)**, íntegramente aportado y pagado, según consta en el artículo precedente, dividido en **SESENTA Y CINCO MIL CUATROCIENTOS CINCUENTA Y TRES (65,453)** cuotas sociales, iguales, acumulables e indivisibles, enteramente suscritas y pagadas, cada una con un valor nominal de **CIEN PESOS DOMINICANOS CON 00/100 (RD\$100.00)** numeradas consecutivamente del uno (1) hasta el sesenta y cinco mil cuatrocientos cincuenta y tres (65,453), ambos inclusive. Todas las cuotas sociales han sido atribuidas a los socios en proporción a sus aportes de la siguiente manera:

- 1) A **VIRGILIO SALVADOR ALBERT FIORINELLI**: sesenta y cinco mil trescientos veintisiete (65,327) cuotas sociales, numeradas del uno (1) al sesenta y cinco mil trescientos veintisiete (65,327) ambos inclusive;
- 2) A **RAQUEL MARIA MENICUCCI DE ALBERT**: ciento veintiséis (126) cuotas sociales, numeradas del sesenta y cinco mil trescientos veintiocho (65,328) al sesenta y cinco mil cuatrocientos cincuenta y tres (65,453), ambos inclusive;

Los socios que suscriben estos estatutos declaran de manera expresa que dichas cuotas sociales han sido totalmente pagadas y distribuidas en la forma arriba indicada.

**Artículo 8. Aumento del Capital Social.** El capital social podrá ser aumentado en todas las formas previstas por la ley, una o varias veces, ya sea por creación de nuevas cuotas sociales o por elevación del valor nominal de las ya existentes, sea como consecuencia de nuevos aportes en dinero o en naturaleza, incluida la aportación de créditos contra la sociedad, como de la transformación de reservas o beneficios, o de la reevaluación de activos.

**Párrafo I.** En los aumentos del capital con creación de nuevas cuotas sociales cada socio tendrá un derecho preferente a asumir un número de cuotas proporcional a las que posea. Cualquier socio podrá ceder el derecho de preferencia inherente a su cuota social a otro socio. No habrá lugar a derecho de preferencia cuando el aumento se deba a la absorción de otra sociedad o a la absorción, total o parcial, del patrimonio escindido de otra sociedad.

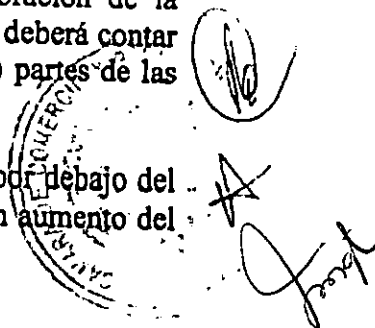
**Párrafo II.** El aumento del capital social podrá ser decidido por los socios reunidos en asamblea general extraordinaria o mediante consulta escrita o por acuerdo unánime contenido en un acta con o sin necesidad de reunión presencial. Sin embargo, en ningún caso podrá la mayoría obligar a un socio a aumentar su compromiso social.

**Párrafo III.** En los casos de que el aumento de capital se produzca por decisión de la asamblea general extraordinaria o por consulta escrita, dicha decisión deberá contar con la autorización de socios que representen, por lo menos, las tres cuartas (3/4) partes de las cuotas sociales, salvo en el caso de que el aumento de capital se realizare por incorporación de los beneficios o de las reservas, en el cual bastará una mayoría de la mitad (1/2) de las cuotas sociales. Sin embargo, si el aumento del capital se realizare por incremento del valor nominal de las partes, la decisión deberá ser siempre unánime, menos en el caso de que se haga íntegramente con cargo a las reservas o a los beneficios de la sociedad.

**Párrafo IV.** Si el aumento del capital se realizare total o parcialmente por aportes en naturaleza, será preciso que al tiempo de la convocatoria de la asamblea general o de la consulta escrita o del acuerdo unánime de todos los socios, se ponga a disposición de estos un informe de la gerencia en el que se describan con detalle las aportaciones proyectadas, su valoración, las personas que hayan de efectuarlas, el número de cuotas sociales que hayan de crearse, la cuantía del aumento del capital y las garantías adoptadas para la efectividad del aumento según la naturaleza de los bienes aportados. Además, la decisión de los socios deberá contener la evaluación de cada aporte en naturaleza, de conformidad con la Ley.

**Artículo 9. Reducción del Capital Social.** La reducción del capital social podrá ser decidida por los socios reunidos en asamblea general extraordinaria o mediante consulta escrita o por acuerdo unánime contenido en un acta con o sin necesidad de reunión presencial, con arreglo a la ley. Cuando la reducción del capital social se produzca mediante la celebración de la asamblea general extraordinaria o por consulta escrita, la decisión que la autorice deberá contar con la aprobación de socios que representen, por lo menos, las tres cuartas (3/4) partes de las cuotas sociales. En ningún caso se podrá atentar contra la igualdad de los socios.

**Párrafo I.** Los socios podrán acordar excepcionalmente la reducción del capital por debajo del mínimo legal, siempre y cuando dicha decisión sea inmediatamente seguida de un aumento del



SECRETARÍA DE ECONOMÍA  
ESTADO DE QUERÉTARO  
SECRETARÍA DE COMERCIO Y INDUSTRIA

*[Handwritten signature]*

capital hasta una cantidad igual o superior al mínimo legal. La eficacia de la decisión que acuerde esta reducción quedará condicionada a la ejecución de la decisión que apruebe el aumento de capital. En todo caso, habrá de respetarse el derecho de preferencia de los socios, sin que en este supuesto haya lugar a su supresión. En caso de que haya un comisario de cuentas, se le comunicará el proyecto de reducción del capital, por lo menos cuarenta y cinco (45) días antes de la fecha en que se deba decidir sobre la reducción de capital. El comisario dará a conocer a los socios su opinión sobre las causas y condiciones de la reducción.

**Párrafo II.** Estará prohibida a la sociedad la compra de las cuotas sociales de su propio capital. Sin embargo, la decisión que haya autorizado una reducción de capital no motivada por pérdidas, podrá autorizar a la gerencia a comprar un número determinado de cuotas sociales para anularlas.

### CAPÍTULO III DE LAS CUOTAS SOCIALES.

**Artículo 10. Naturaleza de las Cuotas Sociales.** Las cuotas sociales representan los aportes en dinero y en especie hechos por los socios. No tendrán el carácter de valores ni podrán representarse por medio de títulos negociables o anotaciones en cuenta, ni denominarse acciones o intereses.

**Artículo 11. Derechos Inherentes a las Cuotas Sociales.** Cada cuota social dará a su titular los derechos siguientes: a) El derecho a una parte proporcional en la distribución de los beneficios y en el activo social en caso de disolución de la sociedad; b) El derecho a voz y a un (1) voto en todas las deliberaciones de la sociedad; c) Los derechos de información y comunicación que le otorga la Ley; y d) Los demás derechos previstos en la Ley y en los presentes estatutos.

**Artículo 12. Obligaciones Inherentes a las Cuotas Sociales. No Intervención.** La propiedad o titularidad de una o más cuotas sociales supone la conformidad del propietario o titular con estos estatutos, así como también su conformidad con las decisiones colectivas que hayan sido adoptadas regularmente. Los titulares de las cuotas sociales no tendrán más derechos que los establecidos en estos estatutos y en la Ley; en consecuencia, ni ellos ni sus herederos, cónyuges, acreedores u otros causahabientes podrán por ninguna causa inmiscuirse en la administración de la sociedad, ni provocar la colocación de sellos u oposiciones sobre sus bienes y valores ni pedir su partición o licitación.

**Artículo 13. Responsabilidad Limitada de los Socios.** Los socios serán responsables solamente hasta la concurrencia del monto de las cuotas sociales que les pertenecen. En consecuencia, no podrán ser compelidos por ningún motivo ni a realizar aportes adicionales a la sociedad ni a restituir beneficios u otros fondos regularmente percibidos.

**Artículo 14. Indivisibilidad de las Cuotas Sociales.** Las cuotas sociales serán indivisibles frente a la sociedad, la cual no reconocerá más que un solo titular por cada cuota. Para ejercer los derechos inherentes a sus cuotas sociales, los copropietarios indivisos deberán designar uno de ellos para que los represente ante la sociedad. A falta de entendimiento, el copropietario indiviso más diligente podrá solicitar la designación de un mandatario mediante instancia elevada al juez presidente de la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial correspondiente al domicilio social.

**Párrafo I.** En caso de desmembración del derecho de propiedad sobre una cuota social, el derecho al voto pertenecerá al nudo propietario para todos los asuntos que sean competencia de las asambleas extraordinarias, y al usufructuario para aquellos de la competencia de las asambleas ordinarias.

**Art. 15. Transmisión de las Cuotas Sociales.** Las cuotas sociales serán libremente transmisibles entre socios; en cuanto a la transmisión entre ascendientes y descendientes, por vía de sucesión o en caso de liquidación de comunidad de bienes entre esposos, estará sujeta a la aprobación de socios que representen, por lo menos, las dos terceras (2/3) partes de las cuotas sociales; pero no podrán ser cedidas a terceros extraños a la sociedad sin el consentimiento de la mayoría de los socios que representen, por lo menos, las tres cuartas (3/4) partes de las cuotas sociales, conforme al procedimiento establecido por la Ley.

**Párrafo I.** Si la sociedad no hiciera conocer su decisión en el plazo de quince (15) días contado desde la notificación del proyecto de cesión, se reputará obtenido el consentimiento para la cesión.

**Artículo 16. Formalidades de la Transmisión de Cuotas Sociales.** La cesión de las partes sociales deberá ser constatada por escrito. Se hará oponible a la sociedad por el depósito de un original del acto de cesión en el domicilio social contra entrega de una certificación del depósito por parte de la gerencia.

**Párrafo I.** En los casos de transferencia de cuotas sociales por sucesión o liquidación de comunidad, la parte interesada deberá depositar en la sociedad los documentos que comprueben, de manera definitiva, su calidad de sucesor o copropietario.

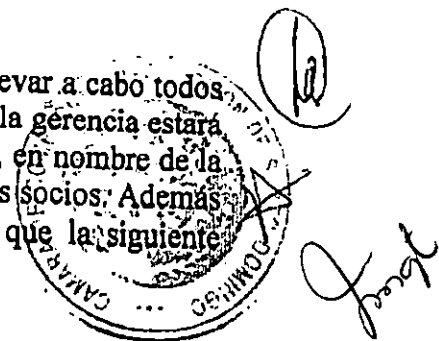
**Párrafo II.** La transmisión de cuotas sociales no se hará oponible a los terceros sino a partir de su inscripción en el Registro Mercantil.

#### **CAPÍTULO IV DE LA GERENCIA DE LA SOCIEDAD.**

**Artículo 17. Nombramiento de la Gerencia.** La sociedad será administrada por un consejo de gerencia o por uno o varios gerentes, socios o no, que deberán ser personas físicas. Su nombramiento podrá ser estatutario o por un acto posterior de la sociedad, y tendrá una duración de un (1) año. El consejo de gerencia o los gerentes podrán ser reelegidos indefinidamente y ejercerán sus funciones mientras no hayan sido sustituidos.

**Párrafo I.** La administración de la sociedad se podrá confiar a un gerente único, o a dos o más gerentes que constituyan un consejo de gerencia. La sociedad tendrá la facultad de optar alternativamente por cualquiera de los modos de organizar la gerencia, sin necesidad de modificación estatutaria.

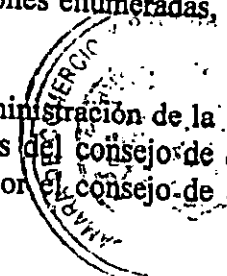
**Artículo 18. Poderes de la Gerencia.** Frente a los socios, la gerencia podrá llevar a cabo todos los actos de gestión necesarios en interés de la sociedad. Frente a los terceros, la gerencia estará investida con los poderes más amplios para actuar, en todas las circunstancias, en nombre de la sociedad, bajo reserva de los poderes que la ley les atribuye expresamente a los socios. Además de las facultades que le confieren otros artículos de estos estatutos y sin que la siguiente



enumeración pueda considerarse como restrictiva de sus poderes, la gerencia tendrá las siguientes atribuciones:

- a) Reglamentar y dirigir las operaciones de la sociedad y el trabajo de su personal;
- b) Nombrar los empleados de la sociedad, acordar sus remuneraciones y disponer la terminación de sus servicios cuando lo estimen conveniente;
- c) Adquirir derechos y bienes de cualquier naturaleza, muebles e inmuebles; aceptar las donaciones hechas a la sociedad;
- d) Obtener los créditos que crea necesarios para los negocios de la sociedad mediante la contratación de préstamos y otros medios;
- e) Recibir los pagos de cualesquiera créditos de la sociedad y otorgar los correspondientes descargos;
- f) Adquirir hipotecas, privilegios y garantías prendarias y de cualquier otra clase, en relación con las operaciones de la sociedad; y cancelar y hacer radiar dichas hipotecas, privilegios y otras garantías;
- g) Vender, ceder, aportar, traspasar o permutar los bienes de la sociedad de cualquier naturaleza, muebles e inmuebles, convenir los precios de dichos bienes, así como las demás condiciones de tales operaciones, recibir el pago de esos precios y dar descargos por los mismos; donar dichos bienes;
- h) Pagar con los fondos sociales toda deuda exigible de la sociedad; conceder créditos y efectuar avances;
- i) Constituir hipotecas, prendas y garantías de cualquier otra clase sobre los bienes de la sociedad;
- j) Tomar y dar en arrendamiento o en subarrendamiento y administrar bienes muebles e inmuebles;
- k) Librar, suscribir, aceptar, adquirir, ceder, descontar, recibir u otorgar el endoso y gestionar el cobro de letras de cambio, giros, pagarés a la orden y otros efectos de comercio y títulos;
- l) determinar la inversión y la colocación de los fondos disponibles;
- m) Disponer respecto de la apertura y funcionamiento de cuentas en bancos y otras instituciones financieras, y el arrendamiento de cajas de seguridad; girar cheques, realizar retiros y cualquier otra operación bancaria o financiera;
- n) Depositar valores, títulos, piezas o documentos cualesquiera en entidades o personas públicas o privadas y retirarlos;
- ñ) Hacer aportes a otras sociedades, constituidas o en proceso de constitución;
- o) Representar la sociedad en justicia, como demandante o demandada, así como otorgar aquiescencias y desistimientos e interponer recursos, en todas las materias y jurisdicciones; y al efecto, designar y revocar abogados y apoderados especiales y convenir sus retribuciones;
- p) Trabajar embargos y medidas conservatorias y ejercer cualesquiera otras vías de derecho, así como suspender y cancelar estos procedimientos;
- q) Perseguir las quiebras de los deudores cuando fuere necesario; autorizar concordatos y tomar cualquier medida conveniente al interés social en esas quiebras y en las tentativas previas de acuerdo amigable;
- r) Celebrar toda clase de contratos, inclusive compromisos y promesas de compromiso para arbitrajes, así como transigir; y
- s) Otorgar poderes específicos para el ejercicio de una o varias de las atribuciones enumeradas, con la facultad de sustituirlos y revocarlos.

**Párrafo I.** Cuando sea nombrado un Consejo de Gerencia, para ejercer la administración de la sociedad, los gerentes deberán haber tomado previamente la decisión a través del consejo de gerencia como órgano colegiado. La oposición formulada por un gerente o por el consejo de



*(Handwritten signature and date)*  
14 MAR 1964

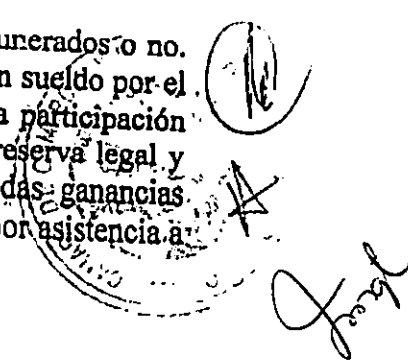
gerencia a los actos o actuaciones de otro gerente no tendrá efectos respecto de los terceros, a menos que se haya probado que estos tuvieron conocimiento de dicha oposición. El consejo de gerencia se regulará por las siguientes normas:

- a) Estará integrado por dos o más gerentes, que podrán o no ser socios;
- b) La convocatoria del Consejo de gerencia se realizará por uno cualquiera de los gerentes siempre que lo estime conveniente.
- c) La convocatoria del consejo se realizará por cualquier procedimiento escrito, incluido por correo electrónico, que permita acreditar su envío al menos con tres (3) días de antelación a la fecha de celebración de la reunión.
- d) El consejo de gerencia quedará válidamente constituido para ejercer cualesquiera de los poderes que les han sido asignados en los presente estatutos, cuando concurran a la reunión, presentes o representados, sus dos miembros, en el caso de que el consejo de gerencia esté compuesto por tres miembros o más, quedará válidamente constituido cuando concurran a la reunión, presentes o representados más de la mitad de sus miembros.
- e) No obstante, el consejo quedará válidamente constituido, sin necesidad de convocatoria previa, cuando estén presentes o representados todos sus miembros y se decida por unanimidad la celebración de la reunión.
- f) Las decisiones emitidas por el consejo se adoptarán por el consentimiento de la mayoría de sus miembros.
- g) Las decisiones del consejo se comprobarán mediante actas que deberán redactarse de cada reunión. Estas actas, que constatarán en un registro especial o en hojas sueltas, deberán ser firmadas por todos los gerentes presentes o representados. Las copias o extractos de las decisiones del consejo deberán estar firmadas por uno de los gerentes del consejo.
- h) Las resoluciones del consejo podrán ser adoptadas en un acta suscrita por todos los gerentes sin necesidad de reunión presencial. Igualmente su voto podrá manifestarse a través de cualquier medio electrónico o digital. Ambas circunstancias deberán expresamente indicarse en el acta que se redacte al efecto.

**Párrafo II.** Cuando sean nombrados varios gerentes, para ejercer uno cualquiera de los poderes previstos en el presente artículo, el gerente actuante deberá obtener el consentimiento por escrito de los demás gerentes. La oposición formulada por un gerente a los actos o actuaciones de otro gerente no tendrá efectos respecto de los terceros, a menos que se haya probado que estos tuvieron conocimiento de dicha oposición.

**Párrafo III:** La sociedad se encontrará comprometida por los actos y actuaciones ejecutados por la gerencia aún si estos no se relacionan con el objeto social, a menos que pruebe que el tercero tenía conocimiento de que el acto o actuación era extraño al objeto social o que no podía ignorarlo dado las circunstancias. Se excluirá que la sola publicación de los estatutos baste para constituir esta prueba.

**Artículo 19. Remuneración de la Gerencia.** El o los Gerentes podrán ser remunerados o no. La remuneración de los gerentes consistirá en una o varias de las siguientes: a) Un sueldo por el desempeño de funciones técnico administrativas de carácter permanente; b) Una participación en las ganancias deducida de los beneficios líquidos y después de cubiertas la reserva legal y estatutaria, la cual no podrá exceder del diez por ciento (10%) de las referidas ganancias aplicadas al conjunto de gerentes; c) Una suma fija anual, a título de honorarios, por asistencia a

Handwritten signatures and stamps at the bottom right of the page. There is a circular stamp with illegible text, a signature that appears to be 'J. José', and another signature that appears to be 'J. José'.

las reuniones; y d) Remuneraciones excepcionales para las misiones o los mandatos confiados a los gerentes por la sociedad; según lo decida la asamblea de socios.

**Artículo 20. Convenciones Celebradas por un Gerente o un Socio con la Sociedad.** La gerencia o el comisario de cuentas, si lo hubiere, presentarán a la asamblea o a los socios un informe sobre las convenciones intervenidas directa o indirectamente entre la sociedad y uno de sus gerentes o uno de sus socios, dentro del mes de celebrada dicha convención. Las disposiciones del presente artículo no serán aplicables a las convenciones relativas a operaciones corrientes concluidas en condiciones normales.

**Párrafo I.** Los socios estatuirán sobre este informe. El gerente o el socio interesado no podrá tomar parte de las deliberaciones y sus cuotas sociales no serán tomadas en cuenta para el cálculo del quórum ni de la mayoría.

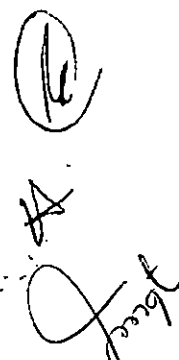
**Párrafo II.** Si no hubiere comisario de cuentas, las convenciones concluidas por un gerente no socio deberán ser sometidas previamente a la aprobación de los socios.

**Párrafo III.** Las convenciones no aprobadas producirán sus efectos para el gerente o para el socio contratante, si hubiere lugar, quienes soportarán individual o solidariamente, según el caso, las consecuencias perjudiciales que produzca el aludido contrato para la sociedad.

**Artículo 21. Prohibiciones a la Gerencia.** La gerencia no podrá, sin autorización expresa y unánime de los socios, realizar ninguno de los actos siguientes:

- a) Tomar en préstamo dinero o bienes de la sociedad;
- b) Usar bienes, servicios o créditos de la sociedad en provecho propio o de parientes, representados o sociedades vinculadas;
- c) Usar en beneficio propio o de terceros relacionados las oportunidades comerciales de que tuvieren conocimiento en razón de su cargo y que a la vez constituya un perjuicio para la sociedad;
- d) Proponer modificaciones de los presentes estatutos sociales o adoptar políticas o decisiones que no tengan por fin el interés social, sino sus propios intereses o de los terceros relacionados;
- e) Impedir u obstaculizar las investigaciones destinadas a establecer su propia responsabilidad o la de otros ejecutivos o gerentes en la gestión de la sociedad;
- f) Inducir a otros gerentes, en caso de que los hubiere, ejecutivos y dependientes o a los comisarios de cuentas o auditores, si los hubiere, a rendir cuentas irregulares, presentar informaciones falsas u ocultar información;
- g) Presentar a los socios cuentas irregulares, informaciones falsas u ocultarles informaciones esenciales;
- h) Practicar actos ilegales o contrarios a los presentes estatutos sociales o al interés social o usar su cargo para obtener ventajas indebidas en su provecho o para terceros relacionados, en perjuicio del interés social;
- i) Participar, por cuenta propia o de terceros, en actividades en competencia con la sociedad, salvo autorización expresa de los socios. Cualquier acto otorgado por la gerencia en violación de lo aquí dispuesto será nulo y los beneficios que pudieren percibirse pertenecerán a la sociedad, la cual además deberá ser indemnizada por cualquier otro perjuicio que hubiere sufrido.

**Párrafo I.** Los gerentes estarán obligados a guardar reserva respecto de los negocios de la sociedad y de la información social a la que tengan acceso en razón de su cargo y que a la vez

A circular stamp is partially visible at the bottom right of the page, containing some illegible text. Overlaid on and around the stamp is a handwritten signature in dark ink.



no haya sido divulgada oficialmente por la sociedad, salvo requerimiento de cualquier autoridad pública o judicial competente.

**Párrafo II.** Estará prohibido a los gerentes, así como a los socios, contratar, bajo la forma que fuere, préstamos con la sociedad o hacerse consentir por la misma un sobregiro, en cuenta corriente o de otro tipo, o avalar por ella sus compromisos con terceros. Esta prohibición se aplicará a los representantes legales de las personas morales que sean socios, al cónyuge y a los ascendientes y descendientes de las personas referidas en este artículo, así como a toda persona interpuesta.

**Artículo 22. Responsabilidad Civil de la Gerencia.** Los gerentes serán responsables, individual o solidariamente, según el caso, frente a la sociedad o frente a los terceros, de las infracciones a las disposiciones legales o reglamentarias aplicables a la sociedad de responsabilidad limitada, así como de las violaciones a los estatutos sociales y de las faltas cometidas en su gestión.

**Párrafo I.** Si varios gerentes han cooperado en tales hechos, el tribunal determinará la parte en que contribuirá cada uno en la reparación del daño.

**Párrafo II.** Además de la acción en reparación del perjuicio personal sufrido por los socios, estos podrán intentar, individual o colectivamente, la acción social en responsabilidad contra los gerentes. Los demandantes podrán perseguir la reparación del perjuicio íntegro sufrido por la sociedad, la cual recibirá el pago de las indemnizaciones correspondientes.

**Párrafo III.** En caso de que exista pluralidad de gerentes, aquellos que no hayan tenido conocimiento del acto o que hayan votado en contra quedarán descargados de responsabilidad.

**Párrafo IV.** Los socios que representen al menos la vigésima parte (1/20) del capital social podrán, en interés común, designar a sus expensas a uno o más de ellos para que los representen a fin de ejercer, como demandantes o demandados, la acción social contra el o los gerentes. El retiro de uno o varios de esos socios de la instancia en curso, sea porque hayan perdido esta calidad o porque hayan desistido voluntariamente, no tendrá efecto sobre la persecución de dicha instancia.

**Párrafo V.** Cuando la acción social sea intentada por uno o varios socios que actúen individualmente o en las condiciones previstas en el párrafo precedente, el tribunal sólo podrá estatuir si la sociedad ha sido regularmente puesta en causa a través de sus representantes legales.

**Párrafo VI.** Las acciones en responsabilidad previstas en este artículo prescribirán a los tres (3) años desde la comisión del hecho perjudicial, o, si estos ha sido disimulado, desde la fecha de su revelación.

**Artículo 23. Revocación del Gerente.** La designación del o de los gerentes será revocable por la decisión de los socios que representen más de la mitad (1/2) de las cuotas sociales. Si la revocación fuere decidida sin justa causa podrá dar lugar a la acción en reparación en daños y perjuicios. Además, el gerente podrá ser revocado a requerimiento de cualquier socio, mediante decisión judicial motivada en causa legítima.

## CAPÍTULO V DEL CONTROL DE LA SOCIEDAD.

**Artículo 24. Nombramiento de un Comisario de Cuentas.** La sociedad podrá nombrar uno o varios comisarios de cuenta si al cierre de su último ejercicio social tuviere un balance igual o superior a cinco (5) veces su capital social o un monto de ganancias igual o superior a las dos terceras partes (2/3) de su capital social, antes de la deducción de los impuestos.

**Párrafo I.** No obstante lo anterior, el o los socios que representen al menos la décima parte (1/10) del capital social podrán siempre demandar en referimiento la designación de un comisario de cuentas.

**Párrafo II.** En los casos en que la sociedad designe comisarios de cuentas, estos serán elegidos por los socios para un período de tres (3) ejercicios sociales y estarán sujetos a las mismas condiciones de calificación profesional, incompatibilidades, poderes, funciones, obligaciones, responsabilidades, suplencias, recusaciones, revocaciones y remuneraciones previstos en la Ley para los comisarios de cuenta de las sociedades anónimas.

**Artículo 25. Derecho Directo de Control de los Socios.** Todo socio no gerente podrá, dos (2) veces por año, plantear a la gerencia las preguntas sobre los hechos que, por su naturaleza, puedan comprometer la continuidad de la explotación social. La gerencia deberá responder por escrito a estas preguntas en el plazo de quince (15) días. En este mismo plazo la gerencia deberá transmitir copia de las preguntas y las respuestas al comisario de cuentas, si lo hubiere.

**Párrafo I.** Uno o más socios que representen por lo menos la vigésima parte (1/20) del capital social, sea individual o colectivamente, podrán demandar en referimiento, habiendo citado previamente al gerente, la designación de uno o más expertos encargados de presentar un informe sobre una o varias gestiones u operaciones.

**Párrafo II.** Si la demanda fuese acogida, la decisión del tribunal determinará el alcance de la gestión y los poderes del o los expertos. Las costas podrán ponerse a cargo de la sociedad.

**Párrafo III.** El informe del experto se depositará en la secretaría del tribunal y el secretario se encargará de comunicarlo al demandante, a los comisarios de cuentas, si los hubiere, ya los gerentes; y será anexado al informe que preparen los comisarios de cuentas, si los hubiere, para la próxima asamblea general.

**Artículo 26. Experticio Contable.** Todo socio cuya participación represente por lo menos el cinco por ciento (5%) del capital social, tendrá el derecho de conocer en cualquier momento la condición económica y las cuentas de la sociedad. Para ejercer este derecho, el socio interesado deberá otorgar mandato a uno o varios contadores públicos autorizados para realizar la investigación correspondiente. El informe rendido por los contadores públicos autorizados sólo tendrá un valor informativo para las personas a cuyo requerimiento se formule y no podrá ser aducido como base jurídica u oficial en ningún caso, salvo el caso de peritaje, en el grado que autorice la ley.

## **CAPÍTULO VI DE LA TOMA DE DECISIONES.**

**Artículo 27. Sobre las Decisiones Colectivas.** Todas las decisiones colectivas de la sociedad serán tomadas por los socios reunidos en asamblea o por consulta escrita o por el consentimiento de todos los socios contenido en un acta con o sin necesidad de reunión presencial. Los acuerdos y resoluciones tomadas regularmente obligarán a todos los socios, incluso a los disidentes, ausentes e incapaces.

**Párrafo I.** Por excepción, las decisiones sobre la gestión y cuentas anuales deberán acordarse obligatoriamente en asamblea de los socios. Igualmente, será obligatoria la celebración de una asamblea cuando así lo requieran el o los socios que sean titulares de la mitad (1/2) o más de las cuotas sociales o que constituyan la cuarta parte (1/4) de los socios y sean propietarios de la cuarta parte (1/4) de las cuotas sociales, por lo menos.

**Párrafo II.** El informe de gestión anual y los estados financieros auditados, más del informe del o de los comisarios de cuentas, si los hubiere, serán sometidos a la aprobación de los socios reunidos en asamblea en el plazo de tres (3) meses contados a partir de la clausura del ejercicio social. Los documentos mencionados con los textos de las resoluciones que sean propuestas, así como, en su caso, el informe del o de los comisarios de cuentas, serán comunicados a los socios y puestos a su disposición en el domicilio social durante los quince (15) días que precedan a la asamblea.

**Párrafo III.** Los socios podrán resolver, reunidos en asamblea o por consulta escrita o por consentimiento unánime de todos los socios contenido en un acta, cualquier asunto que no haya sido previsto en la Ley o en estos estatutos.

**Artículo 28. Consultas Escritas.** En caso de consulta por escrito, la gerencia deberá notificar a todos los socios mediante comunicación física o electrónica con acuse de recibo, o por vía ministerial, el texto de las resoluciones propuestas, los documentos necesarios para la información de los socios y la indicación del plazo que tendrán los mismos para responder. Los socios dispondrán de un plazo mínimo de quince (15) días contados desde la fecha de recepción del proyecto de resolución para emitir su voto por escrito.

**Párrafo I.** El voto emitido por cada socio deberá ser formulado por escrito y remitido a la gerencia en cualquiera de las modalidades establecidas para la comunicación de la consulta escrita. La gerencia levantará un acta a la cual se anexará la respuesta de cada socio.

**Artículo 29. Consentimiento de los Socios Contenido en Actas.** Salvo para el caso de la asamblea que deba conocer del informe de gestión anual y de los estados financieros auditados, los socios podrán tomar cualquier decisión colectiva sin necesidad de reunirse en asamblea si todos estuvieren unánimemente de acuerdo con dicha decisión. El consentimiento unánime se expresará en un acta que deberá ser suscrita por todos los socios con o sin necesidad de reunión presencial.

**Artículo 30. Convocatoria de las Asambleas o Juntas.** Las siguientes personas podrán convocar a los socios a las asambleas generales: a) La gerencia; b) El comisario de cuentas, si lo hubiere, para las asambleas generales extraordinarias, cuando lo juzgue necesario; para las

ordinarias especiales, cuando la gerencia omita hacerlo; y en caso de urgencia, c) El o los socios que sean titulares de la mitad (1/2) o más de las cuotas sociales o que constituyan la cuarta parte (1/4) de los socios y sean propietarios de la cuarta parte (1/4) de las cuotas sociales y d) Cualquier mandatario de uno o varios socios designado por auto del juez de los referimientos correspondiente al domicilio social de la compañía, en virtud de una demanda incoada a tal fin.

**Párrafo I.** Las convocatorias de las asambleas se harán mediante comunicación física o electrónica con acuse de recibo, o por acto de alguacil, quince (15) días por lo menos antes de la fecha de la reunión, salvo para el caso de las asambleas que deban conocer de los proyectos de cesión de las cuotas sociales, en el cual el plazo mínimo de convocatoria será de cinco (5) días. La convocatoria deberá indicar el orden del día y la fecha, hora y lugar en que se celebrará la reunión. Todo socio tendrá derecho a exigir que las convocatorias les sean enviadas por fax o por correo electrónico, en adición a cualquier otro medio de notificación escogido por la o las personas que le hayan convocado.

**Párrafo II.** Las asambleas tendrán lugar en el domicilio social o en cualquier lugar del territorio nacional que se indique en el aviso de convocatoria. Sin embargo, toda asamblea estará válidamente constituida sin necesidad de convocatoria ni de plazo y en cualquier lugar si la totalidad de los socios se encuentran presentes o debidamente representados.

**Artículo 31. Orden del Día.** La agenda u orden del día de la asamblea será redactada por la persona o personas que la convoquen. Toda proposición que fuere una consecuencia directa de la discusión provocada por un punto del orden del día deberá ser sometida a votación. También se deberá incluir en la agenda cualquier tema que sea solicitado por socios que representen por lo menos la cuarta parte (1/4) de las cuotas sociales, siempre y cuando el tema sea compatible con la naturaleza de la asamblea.

**Artículo 32. Informes Previos.** Los socios podrán solicitar por escrito, con anterioridad a la reunión de la asamblea o verbalmente durante la misma, los informes o aclaraciones que estimen precisos acerca de los asuntos comprendidos en el orden del día. La gerencia estará obligado a proporcionárselos, en forma oral o escrita de acuerdo con el momento y la naturaleza de la información solicitada, salvo en los casos en que, ajuicio de la propia gerencia, la publicidad de esta perjudique los intereses sociales. Esta excepción no procederá cuando la solicitud esté apoyada por socios que representen, al menos, la décima parte (1/10) del capital social.

**Artículo 33. Representación y Voto.** Cada socio tendrá derecho a participar en las decisiones y dispondrá de un número de votos igual a la cantidad de cuotas sociales que posea. Todo socio podrá hacerse representar por otro socio o por su cónyuge o por un tercero. El mandato de representación se otorgará para una sola asamblea. Sin embargo, podrá otorgarse para dos asambleas que se celebren el mismo día o en un lapso de siete (7) días. El mandato conferido para una asamblea valdrá para las asambleas sucesivas convocadas con el mismo orden del día.

**Párrafo I.** Tanto en las asamblea como en las consultas escritas, las decisiones se adoptarán con el voto de socio o los socios que representen más de la mitad (1/2) de las cuotas sociales. Si no pudiera obtenerse esta mayoría, los socios serán convocados nuevamente y las decisiones se adoptarán por la mayoría de los votos emitidos, sin importar el número de los votantes, excepto en los casos en que la Ley ordena una mayoría especial.

**Párrafo II.** La modificación de los estatutos podrá ser decidida únicamente con el voto de socios que representen, por lo menos, las tres cuartas (3/4) partes de las cuotas sociales.

**Artículo 34. Tipos de Asamblea.** Las asambleas o juntas podrán ser ordinarias o extraordinarias.

**Párrafo I.** Será competencia de la asamblea o junta general ordinaria deliberar y decidir sobre los siguientes asuntos: a) La aprobación de los estados financieros y la distribución total o parcial de los beneficios acumulados; b) El nombramiento y la revocación de los gerentes, de los comisarios de cuentas, si los hubiere, así como el ejercicio de la acción social de responsabilidad contra cualquiera de ellos; c) La autorización a los gerentes para el ejercicio, por cuenta propia o ajena, de actividades concurrentes con el objeto social o de convenios a través de los cuales obtenga un beneficio personal directo o indirecto; y, d) Cualquier otro asunto que no sea competencia de la asamblea general extraordinaria.

**Párrafo II.** Será competencia de la asamblea o junta general extraordinaria: a) La modificación de los estatutos sociales; b) El aumento y la reducción del capital social; c) La transformación, fisión o escisión de la sociedad; y d) La disolución de la sociedad)

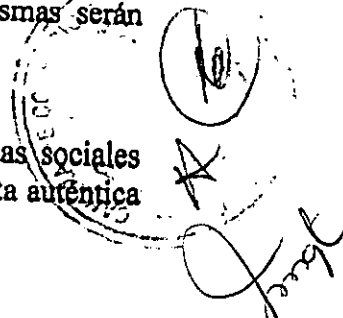
**Párrafo III.** No obstante lo anterior, los socios podrán decidir sobre todos los asuntos atribuidos a las asambleas ordinarias o extraordinarias, sin necesidad de estas, mediante consulta escrita o por el consentimiento de todos los socios contenido en un acta con o sin necesidad de reunión presencial, salvo en los casos señalados en el Párrafo I del Art. 27 de estos estatutos.

**Artículo 35. Mesa de la Asamblea y Actas.** La asamblea de los socios será presidida por el gerente si es socio, o si hay varios, por el gerente de más edad que sea socio. Si ninguno de los gerentes es socio, será presidida por el socio presente y aceptante que posea o represente el mayor número de cuotas sociales. En el caso de que existan dos o más socios aceptantes con igual número de cuotas sociales, la asamblea será presidida por el socio de más edad. En todos los casos que las asambleas sean convocadas por los comisarios de cuentas, serán ellos mismos los que la deberán presidir.

**Párrafo I.** Toda deliberación de la asamblea de los socios será constatada por un acta que indique la fecha, hora y el lugar de la reunión, el nombre, las generales y la calidad del presidente de la sesión, los nombres y generales de los socios presentes o representados, así como de los mandatarios de estos con indicación del número de cuotas sociales pertenecientes a cada uno, los documentos e informes sometidos a la asamblea, un resumen de los debates, los textos de las resoluciones propuestas y el resultado de las votaciones.

**Párrafo II.** Las actas deberán ser aprobadas por la propia asamblea al final de la reunión, ser redactadas en idioma español y asentadas en un registro especial conservado en el domicilio social. Tendrán fuerza ejecutoria a partir de la fecha de su aprobación. Las mismas serán firmadas y certificadas por los gerentes.

**Párrafo III.** Los socios titulares de más de la vigésima (1/20) parte de las cuotas sociales podrán requerir a los gerentes la presencia de un notario público para que levante acta auténtica

A circular stamp with illegible text inside, and a handwritten signature in black ink that appears to be 'J. J. J.' or similar, written over the stamp.

de lo acontecido en la asamblea, siempre y cuando lo soliciten al menos cinco (5) días antes de su celebración. Los gerentes estarán obligados a cumplir con este requerimiento. Los honorarios notariales en este caso estarán á cargo de la sociedad. El acta notarial no será sometida a la aprobación de la asamblea y tendrá la misma fuerza vinculante y ejecutoria que el acta de la asamblea general.

**Párrafo IV.** Las copias o los extractos de las actas de las deliberaciones de los socios serán certificados válidamente por un solo gerente. En caso de liquidación de la sociedad, serán certificados por un solo liquidador.

## **CAPÍTULO VII DEL EJERCICIO SOCIAL, CUENTAS, AFECTACIÓN Y REPARTICIÓN DE LOS BENEFICIOS**

**Artículo 36.** Ejercicio Social. El ejercicio social será anual, iniciará el 1 de enero de cada año y concluirá el 31 de diciembre del mismo año.

**Artículo 37. Cuentas Sociales.** La gerencia deberá, al cierre de cada ejercicio, preparar los estados financieros de la sociedad y el informe de gestión anual para el ejercicio transcurrido.

**Párrafo I.** Los estados financieros deberán reflejar la situación financiera de la sociedad, los resultados de sus operaciones, los cambios en su patrimonio y los flujos de efectivo, de conformidad con los principios y normas contables establecidos por el Instituto de Contadores Públicos Autorizados de la República Dominicana.

**Párrafo II.** El informe de gestión anual deberá contener lo siguiente: a) Los estados financieros auditados de la sociedad; b) La descripción general del negocio y los factores de riesgo que lo afectan; e) Los lugares donde opera la sociedad; d) Los procesos legales en curso; e) Un análisis de la situación financiera y de los resultados de las operaciones; f) Los motivos y las justificaciones de los cambios contables, si los hubiere, y la cuantificación de los mismos; g) La descripción de las inversiones realizadas y la forma en que se hicieron los aportes; h) Los estados financieros auditados de las sociedades subordinadas, si las hubiere, con una descripción de las operaciones relacionadas; i) Los nombres de los gerentes y de los comisarios de cuenta, si los hubiere; y j) La descripción de los hechos ocurridos entre la fecha de cierre del ejercicio y la fecha de preparación del informe de gestión que pudiesen afectar significativamente la situación financiera de la sociedad, los resultados de las operaciones, y los cambios en el patrimonio y en los flujos de efectivo.

**Párrafo III.** Los estados financieros auditados y el informe de gestión anual deberán ser comunicados a los socios y estar en el domicilio social a la disposición de los comisarios de cuentas si los hubiere, por lo menos quince (15) días antes de la asamblea general de los socios llamada a estatuir sobre dichos estados e informe.

**Artículo 38.** Reserva Legal. La sociedad deberá separar anualmente una reserva no menor del cinco por ciento (5%) de las ganancias realizadas y líquidas arrojadas por el estado de resultado del ejercicio anterior. Esta separación anual dejará de ser obligatoria cuando el fondo de reserva alcance el diez por ciento (10%) del capital social.

**Artículo 39. Dividendos.** La asamblea general, después de la aprobación del informe de gestión anual, podrá decidir sobre la distribución de dividendos en efectivo, en especie o en cuotas sociales. Los dividendos deberán provenir de los beneficios acumulados al cierre del ejercicio mostrado en los estados financieros auditados incluidos en el informe de gestión anual. La distribución de los dividendos deberá hacerse en un plazo máximo de nueve (9) meses después de su declaración en la asamblea y basado en un flujo de efectivo que evidencie que con su pago no se violan acuerdos con los socios ni se afectan intereses de los terceros acreedores de la sociedad.

**Párrafo I.** Salvo el caso de reducción de capital, no se podrá hacer ninguna distribución a los socios cuando los capitales propios sean o vengan a ser, después de tal distribución, inferiores al monto del capital suscrito y pagado, aumentado con las reservas que la ley o los estatutos no permitan distribuir.

## **CAPÍTULO VIII DE LA TRANSFORMACIÓN, FUSIÓN, ESCISIÓN, DISOLUCIÓN Y LIQUIDACIÓN**

**Artículo 40. Transformación.** La transformación de la sociedad de responsabilidad limitada en otro tipo de sociedad será decidida por la mayoría requerida para la modificación de los estatutos. La transformación en una Empresa Individual de Responsabilidad Limitada (E.I.R.L.) resultará de la adquisición de parte de un socio, que sea persona física, de todas las cuotas sociales y del cumplimiento de las formalidades establecidas por la Ley para la transformación.

**Párrafo I.** La transformación de la sociedad deberá ser aprobada por los socios, reunidos en asamblea general extraordinaria o por consulta escrita o por el consentimiento de todos los socios contenido en un acta con o sin necesidad de reunión presencial, previa ponderación del balance especial y del informe del comisario de cuentas, en caso de que lo hubiere, los cuales deberán comprobar que el activo neto sea por lo menos igual al capital social suscrito y pagado.

**Párrafo II.** La transformación se hará constar en escritura pública o privada que se inscribirá en el Registro Mercantil, y que contendrá, en todo caso, las menciones exigidas por la Ley para la constitución de la sociedad cuya forma se adopte, así como el balance y el informe referidos en el párrafo anterior.

**Párrafo III.** Quince (15) días antes de la fecha de celebración de la asamblea general extraordinaria que deba conocer de la transformación o de la consulta escrita o del acta en que conste el consentimiento de todos los socios, deberá publicarse en un periódico de amplia circulación nacional un extracto con las estipulaciones más relevantes del proyecto de transformación, en el que se indicará que este último, el balance especial y el informe del comisario de cuentas, en caso de que lo hubiere, estarán a disposición de los socios en la sede social, durante el indicado plazo de quince (15) días.

**Párrafo IV.** La transformación podrá ser revocada si no se inscribiera en el Registro Mercantil dentro del mes que siga a la resolución de la asamblea que la decida, quedando, en este caso, sin ningún efecto. Sin embargo, este plazo podrá ser suspendido en caso de que haya necesidad de rembolsar a los socios sus cuotas sociales.

**Párrafo V.** Para el caso de la transformación de la sociedad en una empresa individual de responsabilidad limitada, el socio único deberá comparecer ante notario a realizar las declaraciones establecidas en la Ley.

**Párrafo VI.** La resolución o decisión de transformación de la sociedad en otro tipo social sólo obligará a los socios que hayan votado a su favor; los socios que hayan votado negativamente o los ausentes quedarán separados de la sociedad siempre que, en el plazo de quince (15) días, contados desde la fecha de la resolución de transformación, no se adhieran por escrito a la misma. Los socios que no se hayan adherido obtendrán el reembolso de sus cuotas sociales, con arreglo a la Ley.

**Párrafo VII.** En todo caso, la transformación no entrañará la creación de una persona moral nueva.

**Artículo 41. Fusión.** La sociedad podrá, por vía de fusión, transmitir su patrimonio a otra sociedad existente o a una nueva sociedad nueva que se constituya. La fisión implicará: a) La disolución sin liquidación de la sociedad, la cual desaparecerá, y la transmisión universal de su patrimonio a la sociedad beneficiaria, en el estado en que se encuentre a la fecha de la realización definitiva de la operación; y, b) Simultáneamente, para los socios de la sociedad, la adquisición de la calidad de socios de la sociedad beneficiaria en las condiciones determinadas por el contrato de fisión. La fusión podrá realizarse entre sociedades de diferentes clases.

**Artículo 42. Escisión** La sociedad podrá también, por vía de escisión, transmitir su patrimonio, o parte de él, a otras sociedades existentes o nuevas. La escisión implicará: a) La extinción de la sociedad con división de su patrimonio en dos o más partes, cada una de las cuales se traspasa en bloque a otra sociedad de nueva creación o es absorbida por una sociedad ya existente; o, b) La segregación de una o varias partes del patrimonio de una sociedad sin extinguirse, que traspase en bloque lo segregado a una o varias sociedades de nueva creación o ya existentes. La escisión podrá realizarse entre sociedades de diferentes clases.

**Artículo 43. Disolución.** La sociedad podrá disolverse: a) Por resolución de la asamblea general extraordinaria o por consulta escrita o por el consentimiento de todos los socios contenido en un acta con o sin necesidad de reunión presencial, adoptada de conformidad con los requisitos y la mayoría establecidos por la Ley; b) Por la conclusión de la empresa que constituya su objeto, la imposibilidad manifiesta de desarrollar el objeto social, ola paralización de la gerencia de modo que resulte imposible su funcionamiento; c) Por falta de ejercicio de la actividad o actividades que constituyan el objeto social durante tres (3) años consecutivos; d) Por consecuencia de pérdidas que dejen reducido el patrimonio contable a menos de la mitad del capital social, a no ser que estos se aumente o se reduzca en la medida suficiente; e) Por la adquisición de parte de un socio que, sea una persona moral, de todas las partes sociales; y Por cualquier otra causa indicada expresamente en estos estatutos.

**Párrafo I.** La sociedad de responsabilidad limitada no se disolverá por la interdicción o la quiebra de uno de sus socios ni tampoco por su muerte.

**Párrafo II.** En caso de muerte de uno de los socios, el cónyuge supérstite y los sucesores del socio fallecido sólo podrán convertirse en socios de la sociedad si fuesen aceptados por socios que representen, por lo menos, las dos terceras (2/3) partes de las cuotas sociales, sin incluir las



cuotas del socio fallecido. La sociedad deberá estatuir dentro de los quince (15) días de la fecha en que le fuere depositada la solicitud de aprobación de la transmisión, la cual deberá llevar anexa los documentos que comprueben la calidad del solicitante. De no decidir la sociedad dentro de dicho plazo, se reputará que la misma ha sido aprobada. En caso de rechazo, el cónyuge superviviente o el sucesor será acreedor de la sociedad por el valor y proporción que deba corresponderle de los derechos de su causante o ex cónyuge, al momento de su fallecimiento, en la sociedad. Dicho valor será el fijado de mutuo acuerdo por las partes y, en su defecto, el valor razonable de las cuotas sociales al momento del fallecimiento, el cual será determinado por un perito designado de mutuo acuerdo por las partes, o, en su defecto, por auto del juez presidente de la Cámara Civil y Comercial del Juzgado de Primera Instancia del Distrito Judicial correspondiente al domicilio social. Una vez determinado el valor de los derechos, la sociedad tendrá un plazo de tres (3) meses para efectuar el pago correspondiente.

**Párrafo III.** La adquisición por un socio que sea persona física de todas las cuotas sociales no entrañará la disolución de la sociedad sino su transformación en una empresa individual de responsabilidad limitada. Si en el plazo de dos (2) años no se ha realizado el proceso de transformación, ni el número de socios ha sido aumentado al mínimo legal de dos (2), entonces la sociedad deberá disolverse y liquidarse. Cualquiera que tenga interés legítimo podrá demandar la disolución por ante la Cámara Civil y Comercial del Juzgado de Primera Instancia del domicilio de la sociedad.

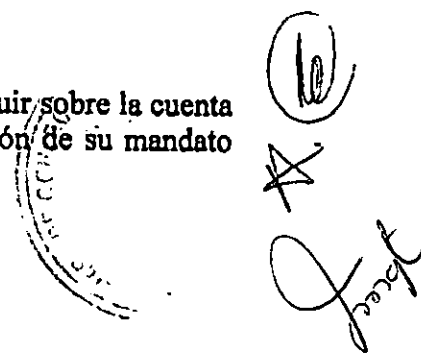
**Párrafo IV.** La adquisición por un socio que sea una persona moral de todas las partes sociales producirá la disolución de la sociedad mediante la transmisión universal del patrimonio de la sociedad al socio único, sin que haya lugar a liquidación. Lo anterior no ocurrirá si dentro del plazo de dos (2) años el número de socios se aumenta al mínimo legal o si todas las partes sociales son adquiridas por una persona física.

**Artículo 44. Liquidación.** En caso de disolución de la sociedad, los socios nombrarán uno o más liquidadores, que podrán ser socios o no, para que procedan a liquidar la sociedad, con arreglo a la Ley.

**Párrafo I.** El nombramiento de los liquidadores dará fin a los poderes de los gerentes, quienes habrán de rendir cuenta de su gestión a la asamblea general, y harán entrega a la misma de las cuentas, libros y documentos sociales.

**Párrafo II.** La liquidación se efectuará de acuerdo con la Ley. El producto neto de la liquidación se empleará en primer lugar para rembolsar el importe de las cuotas sociales que no se hayan reembolsado. El excedente se distribuirá entre los socios en proporción al porcentaje de cuotas sociales que les pertenezcan a cada uno.

**Párrafo III.** Los socios serán convocados al final de la liquidación para estatuir sobre la cuenta definitiva, sobre el descargo de la gestión de los liquidadores y la finalización de su mandato para comprobar el cierre de la liquidación.



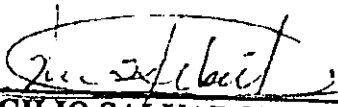
The bottom right corner of the page contains several handwritten marks. At the top is a circled letter 'W'. Below it is a star symbol. At the bottom is a large, stylized signature that appears to be 'J. Lopez'. To the left of these marks is a faint, circular stamp, likely an official seal, though its text is illegible.

**CAPITULO IX  
DE LAS CONTESTACIONES Y GASTOS**

**Artículo 45. Contestaciones.** La interpretación o la aplicación de los presentes estatutos, así como todo conflicto que pudiera surgir durante la vida de la sociedad o de su liquidación, entre los socios y la sociedad, o entre los socios y la gerencia, o entre la sociedad y la gerencia, o entre los socios, y que se refieran a asuntos sociales, serán de la competencia exclusiva de los tribunales de la jurisdicción donde se encuentre el domicilio social, y estarán regidos por las leyes de la República Dominicana.

**Artículo 46. Gastos.** Los gastos, derechos y honorarios de transformación de la sociedad serán soportados por ésta y cargados a la cuenta de gastos generales.

Los presentes estatutos han sido hechos y firmados en dos (2) originales, de un mismo tenor y efecto, en Santo Domingo, República Dominicana, a los veintiocho (28) días del mes de enero del año dos mil once (2011).-

  
**VIRGILIO SALVADOR ALBERT  
FIORINELLI**

  
**RAQUEL MARIA MENICUCCI  
DE ALBERT**

ORIGINAL  
07.04/11 03:13 PM  
91844 5040  
43 228  
RD\$200.00  
ESTATUTOS SOCIALES  
461876TR  
IMPUESTO DUTY





Torre Friusa Av. 27 de Febrero No. 228, La Esperilla, Santo Domingo, Republica Dominicana  
809-682-2686 RNC 401023687

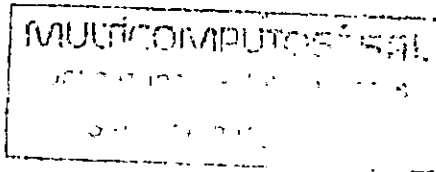
970466

**CAMARA**  
SANTO DOMINGO

**Certificado de Registro Mercantil**  
**Sociedad de Responsabilidad Limitada**

<b>RENOVACIÓN</b>		<b>Registro No.</b> 5040SD	
<b>Denominación Social:</b> MULTICOMPUTOS, S.R.L.			
<b>Fecha Asamblea Constitutiva/Acto</b> 04/03/1994		<b>RNC:</b> 1-01-63880-1	
<b>Fecha Emisión:</b> 29/07/2002		<b>Fecha última Modificación:</b> 24/07/2015	
		<b>Fecha Vencimiento:</b> 02/10/2018	
<b>Dirección de la Empresa</b>			
<b>Calle:</b> AV. ABRAHAM LINCOLN NO. 1007, EDIF. OPTICA FELIX, 4TO PISO			<b>Apartado Postal:</b>
<b>Sector:</b> ENS. PLANTINI		<b>Municipio:</b> SANTO DOMINGO	
<b>Teléfono 1:</b> (809) 540-2144		<b>Teléfono 2:</b>	
<b>Actividades:</b> EXPORTACION, IMPORTACION, SERVICIO, COMERCIO, CONSTRUCCION, DISTRIBUCION		<b>Fax:</b> (809) 540-2847	
<b>Actividad Descripción del Negocio</b>		<b>Principales Productos / Servicios</b>	
NEGOCIO DE SOLUCIONES DE TECNOLOGIA DE INFORMACION A TRAVES DEL DESARROLLO, CONSULTORIA, IMPLEMENTACION, SOPORTE, IMPORTACION, FABRICACION, DISTRIBUCION, EXPORTACION, REPRESENTACION DE CASA NACIONALES Y EXTRANJERAS DE EQUIPOS (HARDWARE), PROGRAMAS (SOFTWARE) DE COMPUTADORAS, REDES, COMUNICACION, TELEFONIA, SEGURIDAD, APLICACIONES, GESTION Y MONITOREO ENTRE OTROS; PROVISION, SUMINISTRO Y COMERCIALIZACION DE ARTICULOS DE PERRUERIA Y PINTURA, AUDIOVISUALES, COMBUSTIBLES Y LUBRICANTES, MATERIALES DE OFICINA, EQUIPOS DE INSUMOS DE INFORMATICA, INMUEBLES, MAQUINARIAS, MUEBLES Y EQUIPOS DE OFICINA, MATERIALES EDUCATIVOS, ASI COMO SERVICIOS DE CAPACITACION, CONSTRUCCION Y EDUCACION, INVERSION EN VALORES O ACCIONES EN OTRAS EMPRESAS Y ENTIDADES		TECNOLOGIA DE LA INFORMACION EQUIPOS DE HARDWARE Y SOFTWARE COMUNICACION, TELEFONIA Y SEGURIDAD ARTICULOS DE FERRERIA Y PINTURA AUDIOVISUALES COMBUSTIBLES Y LUBRICANTES MATERIALES DE OFICINA, EQUIPOS DE INSUMOS DE INFORMATICA INMUEBLES, MAQUINARIAS MUEBLES Y EQUIPOS DE OFICINA, MATERIALES EDUCATIVOS INVERSION EN VALORES O ACCIONES EN OTRAS EMPRESAS Y ENTIDADES	
		<b>Sistema Armonizado (SA)</b>	
<b>Nombre de Socios</b>			
<b>Nombre</b>	<b>Dirección (Calle, Número, Sector)</b>	<b>Registro Mercantil</b>	<b>Cédula / Pasaporte</b>
VERGILIO SALVADOR ALBERT PROSPERELLI	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO		001-0201987-4
RAFAEL MARIA MENDEZ EL MELLA DE ALBERT	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO		001-0202954-5
<b>Órgano de Administración</b>			
<b>Cargo</b>	<b>Nombre y Apellido</b>	<b>Dirección (Calle, Número, Sector)</b>	<b>Cédula / Pasaporte</b>
Presidente	VERGILIO SALVADOR ALBERT PROSPERELLI	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO	001-0201987-4
Presidente	RAFAEL MARIA MENDEZ EL MELLA DE ALBERT	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO	001-0202954-5
<b>Administradores y/o Personas Autorizadas a Firmar</b>			
<b>Nombre</b>	<b>Dirección (Calle, Número, Sector)</b>	<b>Cédula / Pasaporte</b>	<b>Nacionalidad</b>
VERGILIO SALVADOR ALBERT PROSPERELLI	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO	001-0201987-4	REPUBLICA DOMINICANA
RAFAEL MARIA MENDEZ EL MELLA DE ALBERT	C/ TRANSVERSAL NO. 5, ARROYO HONDO SANTO DOMINGO	001-0202954-5	REPUBLICA DOMINICANA
<b>Comisario (s) de Cuenta (s)</b>			
<b>Capital Social RD\$</b>	<b>Bienes Raíces RD\$</b>	<b>Activos RD\$</b>	<b>Duración Sociedad</b>
180,397,300.00			INDEFINIDA
<b>Ente Regulado:</b>	<b>No. Resolución:</b>	<b>Duración Órgano Administrativo</b> 1 Año(s)	
<b>Cantidad Cuotas Sociales</b> 1803973	<b>Fecha Última Asamblea/Acto</b> 13/05/2016		
<b>Referencias Comerciales</b>		<b>Referencias Bancarias</b>	
TEXACO LOPE DE VEGA		BANCO DE RESERVAS	
DORCELLA		BANCO BHD LEON, S. A	
VIAMAR		BANCO POPULAR DOMINICANO	
<b>Número de Empleados</b>	<b>Masculinos</b>	<b>Femeninos</b>	<b>Total Empleados</b>
<b>Sucursales y Agencias que Posee la Sociedad</b>			
<b>Nombre Comercial 1</b> MULTICOMPUTOS			
			<b>No. Registro</b> 53323


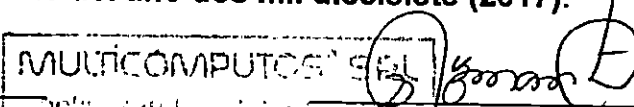
Santiago Mejía Ortiz  
Registrador Mercantil



# PODER

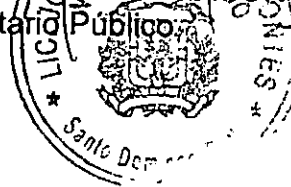
**Multicómputos, S. R. L.**, compañía organizada y constituida de conformidad con las leyes de la República Dominicana, con su Registro Nacional de Contribuyentes (RNC): 1-01-63880-1 y Registro Mercantil No. 5040SD, domicilio social establecido en la Av. Abraham Lincoln No. 1007, debidamente representada por su Gerente, Sr. **Virgilio S. Albert Fiorinelli**, dominicano, mayor de edad, empresario, portador de la cédula de identidad y electoral No. **001-0201987-4**, domiciliado y residente en esta ciudad de Santo Domingo, Distrito Nacional, nombrado como gerente en la Acta de Asamblea General Ordinaria Anual de fecha 13 de Mayo del 2016, por medio del presente acto, otorgo formal poder y mandato legal al Sr. **José Martín Guzmán T.**, dominicano, mayor de edad, soltero, empleado privado, portador de la cédula de identidad y electoral No. **001-0150615-2**, domiciliado y residente en esta ciudad de Santo Domingo, Distrito nacional, para que éste actuando como si fuera yo mismo, represente a la compañía inscribiente y pueda firmar para la **Licitación Pública Nacional Adquisición de Equipos Tecnológicos para el Control de Riesgo y Seguridad, Correspondiente a la Fase I del Proyecto "Modelo de Administración de Riesgo de las Redes de la Jurisdicción Inmobiliaria": LPN-CPJ-12-2017, para el Consejo del Poder Judicial.**

Dada en Santo Domingo, D.N., Capital de la República Dominicana, a los **Dos (02) días del mes de Agosto del año dos mil diecisiete (2017).**

	
<b>Virgilio S. Albert Fiorinelli</b> Multicómputos, S. R. L. Poderdante	<b>José Martín Guzmán T.</b> Multicómputos, S. R. L. Apoderado

YO, LICDA. JOSEFINA VEGA DE MONTES, Abogado y Notario Público de los del Número para el Distrito Nacional, matrícula del Colegio Dominicano de Notarios No. 5582, cón estudio profesional abierto en esta ciudad. CERTIFICO Y DOY FE: Que la firma que aparece en el presente documento fue puesta en mi presencia libre y voluntariamente por el Sr. **Virgilio S. Albert Fiorinelli** y el Sr. **José Martín Guzmán T.**, personas a la que doy fe conocer, y quien me ha declarado bajo la fe del juramento que es la misma firma que acostumbra utilizar en todos sus actos. En la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los **Dos (02) días del mes de Agosto del año dos mil diecisiete (2017).**

  
LICDA. JOSEFINA VEGA DE MONTES  
Notario Público









Código CIS: 003-7102-2012310-7

Código CAS: 15027437225020

REPÚBLICA DOMINICANA  
PROCURADURÍA GENERAL DE LA REPÚBLICA



CERTIFICACIÓN

Certificamos que en el sistema de información de este Ministerio Público, no existen **ANTECEDENTES PENALES** a nombre de **VIRGILIO SALVADOR ALBERT FIORINELLI**, Cédula de Identidad y Electoral Número **001-0201987-4**, por lo que se expide la presente Certificación.

La presente certificación se expide, firma y sella digitalmente a solicitud de la parte interesada. A lo(s) Catorce (14) día(s) del mes de Agosto del año Dos Mil Diecisiete (2017).

MULTICÓMPUTOS® SRL  
optimizando el futuro juntos  
Santo Domingo, R.D.



MINISTERIO PÚBLICO  
<http://servicios.pgr.gob.do/?6LSK-4IER-88BU-787F-LYPF-KTLD>



6LSK-4IER-88BU-787F-LYPF-KTLD



Verifique la legitimidad de la presente certificación en <http://servicios.pgr.gob.do/> en la opción "Consultar Certificados".



Código CIS: 003-7102-2012307-1

Código CAS: 15027435146040

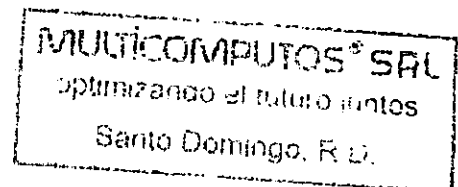
REPÚBLICA DOMINICANA  
PROCURADURÍA GENERAL DE LA REPÚBLICA



CERTIFICACIÓN

Certificamos que en el sistema de información de este Ministerio Público, no existen **ANTECEDENTES PENALES** a nombre de **JOSE MARTIN GUZMAN TAVERAS**, Cédula de Identidad y Electoral Número **001-0150615-2**, por lo que se expide la presente Certificación.

La presente certificación se expide, firma y sella digitalmente a solicitud de la parte interesada. A lo(s) Catorce (14) día(s) del mes de Agosto del año Dos Mil Diecisiete (2017).



MINISTERIO PÚBLICO  
<http://servicios.pgr.gob.do/?EL3R-XXC19-H34F-WXSS-0BKE-EX50>



EL3R-XXC19-H34F-WXSS-0BKE-EX50



Verifique la legitimidad de la presente certificación en <http://servicios.pgr.gob.do/> en la opción "Consultar Certificados".





## Registro de Proveedores del Estado Constancia de Inscripción

RPE 39

**Fecha de Registro:** 29/11/2005  
**Razon Social:** MULTICOMPUTOS, SRL  
**Ocupación:**

**Fecha Actualización:** 03/11/2016  
**No. Documento:** RNC - 101638801  
**Clasificación Proveedor:** Bienes, Servicios, Consultoria  
**Clasificación Empresa:** No clasificada

**Certificacion MIPYME :** NO  
**Registro de Beneficiario:** SI  
**Domicilio:** Avenida Abraham Lincoln, 1007  
Distrito Nacional - REPUBLICA  
DOMINICANA

**Estado:** ACTIVO  
**Motivo:**

**Persona de Contacto :** Raquel

**Observaciones :**

**Actividad Comercial Clasificación Anterior:**

00002 Ferrería y pintura | 00008 Audiovisuales | 00010 Capacitacion | 00011 Combustibles y lubricantes | 00015 Construcción y edificación | 00016 Consultoría | 00017 Suministro de oficina | 00018 Equipo de seguridad | 00021 Equipos e insumos de informática | 00022 Inmuebles | 00024 Maquinarias | 00026 Muebles y mobiliario | 00036 Telefonía y comunicaciones | 00044 Materiales educativos |

**Actividad Comercial Clasificación según Resolución 33/2016**

CÓDIGO	DESCRIPCIÓN	CÓDIGO	DESCRIPCIÓN
15100000	Combustibles	56120000	Mobiliario institucional, escolar y educativo y accesorios
15120000	Lubricantes, aceites, grasas y anticorrosivos	60100000	Materiales didácticos profesionales y de desarrollo y accesorios y suministros
31130000	Forjaduras	72130000	Construcción general de edificios
31140000	Molduras	80100000	Servicios de asesoría de gestión
31150000	Cuerda, cadena, cable, alambre y correa	80130000	Servicios Inmobiliarios
31160000	Ferrería	80140000	Comercialización y distribución
31170000	Rodamientos, cojinetes ruedas y engranajes	84120000	Banca e inversiones

MULTICOMPUTOS S.R.L.  
 Calle

- 31180000 Empaques, glándulas, fundas y cubiertas
- 31190000 Materiales de afilado, pulido y alisado
- 31210000 Pinturas y bases y acabados
- 31250000 Sistemas de control neumático, hidráulico o eléctrico
- 43190000 Dispositivos de comunicaciones y accesorios
- 43200000 Componentes para tecnología de la información, difusión o telecomunicaciones
- 43210000 Equipo informático y accesorios
- 43220000 Equipos o plataformas y accesorios de redes multimedia o de voz y datos
- 43230000 Software
- 44100000 Maquinaria, suministros y accesorios de oficina
- 44110000 Accesorios de oficina y escritorio
- 44120000 Suministros de oficina
- 45110000 Equipos de audio y video para presentación y composición
- 45120000 Equipo de vídeo, filmación o fotografía
- 56100000 Muebles de alojamiento

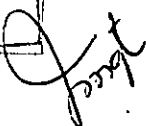
86100000 Formación profesional

MULTICOMPUTER S.A.  
 optimizando el futuro de las  
 Santo Domingo, R.D.

**Este proveedor sólo puede ofrecer al Estado los bienes, servicios u obras conforme al ( o los) rubro(s) detallado(s) en esta constancia de inscripción**

SIGEF -29/05/2017 16:29:25

MULTICOMPUTOS\* SRL  
Calle 2 de Mayo No. 1000  
Santo Domingo, R.D.

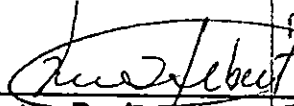


## DECLARACION JURADA

Quien suscribe **Virgilio Albert Fiorinelli** dominicano, mayor de edad, casado, empleado privado, domiciliado y residente en la casa marcada con el numero 1007 de la calle Abraham Lincoln, de la ciudad de Santo Domingo, portador de la cédula de identidad y electoral número 001-0201987-4, actuando en calidad de Presidente y/o Representante Legal de Multicómputos S.R.L., entidad existente de conformidad con las leyes de la Republica Dominicana, con domicilio social en la Av. Abraham Lincoln 1007 Ed. Óptica Félix 4to piso, de esta ciudad, RNC No. 1-01-63880-1, 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 la Licitación No. LPN-CPJ-12-2017 del Consejo del Poder Judicial para la 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", declaro **BAJO LA 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 MULTICOMPOTOS SRL, 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 Santo Domingo, República Dominicana a los dos (02) días del mes de Agosto del año dos mil diecisiete (2017).

  
Declarante

MULTICOMPOTOS SRL  
optimizando el futuro juntos  
Santo Domingo, R.D.

YO, LICDA. JOSEFINA VEGA DE MONTES, Abogado y Notario Público de los del Número para el Distrito Nacional, matrícula del Colegio Dominicano de Notarios No. 5582, con estudio profesional abierto en esta ciudad. CERTIFICO Y DOY FE: Que la firma que aparece en el presente documento fue puesta en mi presencia libre y voluntariamente por el Sr. **Virgilio S. Albert Fiorinelli**, persona a la que doy fe conocer, y quien me ha declarado bajo la fe del juramento que es la misma firma que acostumbra utilizar en todos sus actos. En la ciudad de Santo Domingo, Distrito Nacional, capital de la República Dominicana, a los Dos (02) días del mes de Agosto del año dos mil diecisiete (2017).

LICDA. JOSEFINA VEGA DE MONTES  
Notario Público







República Dominicana  
**MINISTERIO DE HACIENDA**  
**DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS**  
**RNC: 4-01-50625-4**  
**"AÑO DEL DESARROLLO AGROFORESTAL"**  
**CERTIFICACIÓN**

No. de Certificación: **C0217952487471**

La Dirección General de Impuestos Internos **CERTIFICA** que el o la contribuyente **MULTICOMPUTOS SRL**, RNC No. **101638801**, con su domicilio y asiento fiscal en **DISTRITO NACIONAL**, Administración Local **ADM LOCAL GGC**, está al día en la declaración y/o pago de los impuestos correspondientes a las obligaciones fiscales siguientes:

Nombre del Impuesto
RETENCIONES Y RETRIB. EN RENTA
ANTICIPO IMPUESTO A LAS RENTAS
IMPUESTO A LA RENTA SOCIEDADES
ITBIS
OTRAS RETENCIONES Y RETRIB COM

Dada en la **OFICINA VIRTUAL**, a los **atorce (14) días del mes de agosto del año dos mil diecisiete (2017)**.

**NOTAS:**

- La presente certificación tiene una vigencia de treinta (30) días a partir de la fecha y se emite a solicitud del o de la contribuyente o su representante.
- Esta certificación no constituye un juicio de valor sobre la veracidad de las declaraciones presentadas por el o la contribuyente, ni excluye cualquier proceso de verificación posterior.
- Este documento no requiere firma ni sello.

	Código de firma: P1TK-7XYA-FGG1-5027-1892-6455 sha1: qPQ83bwy80JMLkcrw8PIM75L4* DGII - OFICINA VIRTUAL DIRECCION GENERAL DE IMPUESTOS INTERNOS DIRECCION GENERAL DE IMPUESTOS INTERNOS
	 P1TK-7XYA-FGG1-5027-1892-6455

Verifique la legitimidad de la presente certificación en <http://www.dgii.gov.do/verifica> o llamando a los teléfonos 809-689-3444 y 1-809-200-6060 (desde el Interior sin cargos).

**MULTICOMPUTOS<sup>®</sup> SRL**  
 optimizando el futuro juntos  
 Santo Domingo, R.D.



República Dominicana  
**MINISTERIO DE HACIENDA**  
**DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS**  
 RNC: 4-01-50625-4  
 AÑO DEL DESARROLLO AGROFORESTAL  
**CERTIFICACIÓN**

No. de Certificación: **C04363805129**

La Dirección General de Impuestos Internos, **CERTIFICA:** que en sus archivos se encuentra registrado el o la Contribuyente **MULTICOMPUTOS SRL, 101638801, inscrito (a) en el Registro Nacional de Contribuyentes (RNC)** de esta Dirección General de Impuestos Internos, con la actividad económica conforme al Catálogo Internacional Industrial Unificado (CIU): **SERVICIOS DE CONSULTORES EN INFORMÁTICA Y SUMINISTROS DE PROGRAMAS DE INFORMÁTICA.**

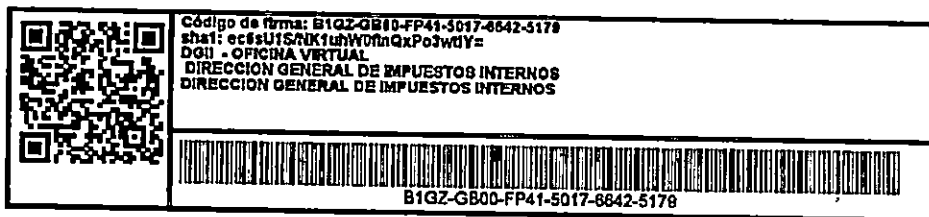
Se encuentra registrado bajo el régimen ordinario de tributación para personas jurídicas.

El domicilio social se encuentra registrado en la **AVENIDA ABRAHAM LINCOLN, No. 1007, APTO. OPTICA FELIX 4TO. PISO, del Sector PIANTINI de la ciudad de DISTRITO NACIONAL**

**NOTAS:**

- La presente certificación tiene una vigencia de treinta (30) días a partir de la fecha y se emite a solicitud del o de la contribuyente o su representante.
- Esta certificación no constituye un juicio de valor sobre la veracidad de las declaraciones presentadas por el o la contribuyente, ni excluye cualquier proceso de verificación posterior.
- Este documento no requiere firma ni sello.

**Dada en la OFICINA VIRTUAL, a los tres (3) días del mes de agosto del año dos mil diecisiete (2017).**



Verifique la legitimidad de la presente certificación en <http://www.dgii.gov.do/verifica> o llamando a los teléfonos 809-689-3444 y 1-809-200-6060.

**MULTICOMPUTOS SAL**  
 optimizando el futuro juntos  
 Santo Domingo, R.D.

*Handwritten signature*



TESORERÍA DE LA SEGURIDAD SOCIAL

**Año del Desarrollo Agroforestal**

**CERTIFICACION No. 778773**

**A QUIEN PUEDA INTERESAR**

Por medio de la presente hacemos constar que en los registros de la Tesorería de la Seguridad Social, la empresa **MULTICOMPUTOS SRL** con RNC/Cédula **1-01-63880-1**, a la fecha no presenta balance con atrasos en los pagos de los aportes a la Seguridad Social.

La presente certificación no significa necesariamente que **MULTICOMPUTOS SRL** haya realizado sus pagos en los plazos que establece la Ley 87-01, ni constituye un juicio de valor sobre la veracidad de las declaraciones hechas por este empleador a la Tesorería de la Seguridad Social, ni le exime de cualquier verificación posterior.

Esta certificación tiene una vigencia de 30 días, a partir de la fecha y se expide **totalmente gratis sin costo alguno** a solicitud de la parte interesada.

Dado en la ciudad de Santo Domingo, Republica Dominicana, a los 14 días del mes de Agosto del año 2017.

  
**Sahadía E. Cruz Abreu**  
Directora  
Dirección de Asistencia al Empleador

Para verificar la autenticidad de esta certificación diríjase a la siguiente dirección:  
<http://www.tss2.gov.do/sys/VerificarCertificacion.aspx>

E introduzca los siguientes datos:

- Código: 778773-J0989883-52017
- Pin: 7640



**NO HAY NADA ESCRITO DEBAJO DE ESTA LINEA**

**MULTICOMPUTOS® SRL**  
optimizando el futuro juntos  
Santo Domingo, R.D.



**MULTICOMPUTOS, SRL**  
**ESTADOS FINANCIEROS**  
**AL 31 DE DICIEMBRE DEL 2016**  
**VALORES EXPRESADOS EN RD\$**

*[Handwritten signature]*



**M. Vásquez & Asociados**  
CONTADORES PUBLICOS AUTORIZADOS  
CONSULTORES FINANCIEROS IMPOSITIVOS Y ADMINISTRATIVOS

**INFORME DE LOS AUDITORES INDEPENDIENTE**

04 de Abril del 2017

Al Consejo de Administración y  
Asamblea General de Accionistas de

**MULTICOMPUTOS, S.R.L.**

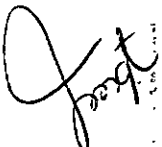
**Opinión sin Salvedad**

Hemos auditados los estados financieros de **MULTICOMPUTOS, S.R.L.**, los cuales comprenden los estados de situación financiera al 31 de diciembre de 2016, y los correspondientes estados de resultados integrales, de cambios en el patrimonio de los accionistas y de flujo de efectivo por el año terminado en esa fecha, así como las notas explicativas de los estados financieros que incluyen un resumen de las políticas contables significativas.

En nuestra opinión, los estados financieros que se acompañan presentan razonablemente, en todos los aspectos materiales, la situación financiera de la Compañía **MULTICOMPUTOS, S.R.L.**, al 31 de diciembre de 2016, así como de sus resultados, sus cambios en el patrimonio de los accionistas y sus flujos de efectivos por el año terminado en esa fecha, de conformidad con las Normas Internacionales de Información Financieras (NIIF).

**Fundamento de la Opinión**

Hemos llevado a cabo nuestras auditorías de conformidad con las Normas Internacionales de Auditoría (NIAS), emitidas por el Consejo de Normas Internacionales de Auditoría y Aseguramiento, de la Federación Internacional de Contadores y adoptadas por el Instituto de Contadores Públicos Autorizados de la República Dominicana (ICPARD). Nuestras responsabilidades de acuerdo a dicha normas se describen más adelante en la sección de Responsabilidades de los Auditores en relación con las Auditorías de los Estados Financieros de nuestro informe. Somos independientes de la empresa de conformidad con el Código de Ética para Contadores Profesionales (Código de Ética del IESBA), emitido por el Consejo de Normas Internacionales de Ética para Contadores, junto con los requerimientos de ética que son aplicables a nuestras auditorías a los estados financieros en la República Dominicana, y hemos cumplidos las demás responsabilidades de ética de conformidad con esos requerimientos y con el Código del IESBA. Consideramos que las evidencias de auditoría que hemos obtenido proporcionan una base suficiente y adecuada para sustentar nuestra opinión.



**M. Vásquez & Asociados**  
**CONTADORES PUBLICOS AUTORIZADOS**  
**CONSULTORES FINANCIEROS IMPOSITIVOS Y ADMINISTRATIVOS**

**Empresa en Funcionamiento**

Los estados financieros de la Empresa han sido preparados utilizando las bases contables de empresa en funcionamiento. El uso de estas bases contables es apropiado a menos que la Administración tenga la intención de liquidar a la Entidad o detener las operaciones, o no tiene otra alternativa realista más que hacerlo. Como parte de nuestra auditoria de los estados financieros, hemos concluido que el uso de las bases contables de empresa por parte de la Administración en la preparación de los estados financieros de la empresa es apropiado.

La Administración no ha identificado una incertidumbre material que pueda dar lugar a una duda significativa sobre la capacidad de la Entidad de continuar como una empresa en funcionamiento y, por consiguiente, no se revela en los estados financieros de la Entidad. Con base en nuestra auditoria de los estados financieros, tampoco hemos identificado dicha incertidumbre material. Sin embargo, ni la administración ni el auditor pueden garantizar la capacidad de la Empresa de seguir como empresa en funcionamiento.

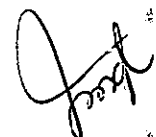
**Responsabilidades de la Administración y el Consejo de Administración de la Entidad sobre los Estados Financieros**

La Administración es responsable por la preparación y presentación razonable de estos estados financieros de conformidad con las Normas Internacionales de Información Financiera (NIIF), emitidas por el Consejo de Normas Internacionales de Contabilidad (IASB), de la Fundación IFRS, y adoptadas por el Instituto de Contadores Públicos Autorizados de la Republica Dominicana (ICPARD), y del control interno que la Administración determine necesario para permitir la preparación de los estados financieros libre de incorrección material, debida a fraude o error.

En la preparación de los estados financieros, la administración es responsable de evaluar la capacidad de la Empresa para continuar como empresa en funcionamiento, revelando, según corresponda, de las cuestiones relacionadas con la empresa en funcionamiento y utilizando el principio contable de empresa en funcionamiento, excepto si la administración tiene intención de liquidar la entidad o de cesar sus operaciones, o bien no exista otra alternativa realista.

El consejo de Administración es responsable de la supervisión del proceso de información financiera de la Empresa.

**Responsabilidad de los Auditores Externos en Relación con la Auditoria de los Estados Financieros.**



**M. Vásquez & Asociados**  
**CONTADORES PUBLICOS AUTORIZADOS**  
**CONSULTORES FINANCIEROS IMPOSITIVOS Y ADMINISTRATIVOS**

Los objetivos de nuestras auditorias son los de obtener una seguridad razonable de que los estados financieros en su conjunto están libres de incorrecciones materiales, debidas a fraudes o error, y emitir un informe de auditoria que contiene nuestra opinión. La seguridad razonable es

un alto nivel de seguridad, pero no es garantía de que una auditoria llevada a cabo de conformidad con las NIA siempre detecte una desviación material cuando existe. Las incorrecciones pueden surgir de un fraude o error y se consideran materiales si, individualmente o agregadas, puede preverse razonablemente que influyan en las decisiones económicas que los usuarios toman basándose en los estados financieros.

Como parte de una auditoria de conformidad con las Normas Internacionales de Auditoria (NIA), aplicamos nuestro juicio profesional y mantenemos una actitud de escepticismo profesional durante toda la auditoria. También:

- Identificamos y evaluamos los riesgos de incorrecciones materiales en los estados financieros, debidas a fraude o error, diseñamos y aplicamos procedimientos de auditoria para responder a dichos riesgos, y obtenemos evidencias de auditoria suficiente y adecuada para proporcionar una base para nuestra opinión. El riesgo de no detectar desviaciones materiales que resulten de un fraude es mayor que en el caso de una incorrección material debida a un error, ya que el fraude puede implicar colusión, falsificación, omisiones deliberadas, manifestaciones intencionalmente erróneas o la elusión del control interno.
- Obtenemos conocimiento del entendimiento del sistema de control interno relevante para la auditoria con el fin diseñar procedimientos de auditoria que sean adecuados en las circunstancias, pero no con la finalidad de expresar una opinión sobre la efectividad del control interno de la Entidad.
- Evaluamos la presentación global, la estructura y el contenido de los estados financieros, incluida la información revelada, y si los estados financieros presentan las transacciones y hechos subyacentes de un modo que logran su presentación razonable.

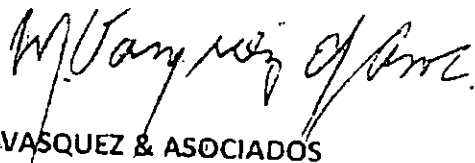
Comunicamos a la Gerencia de la Entidad en relación, entre otros asuntos, el alcance, el enfoque planeado, la oportunidad de ejecución de la auditoria y los hallazgos significativos detectados en su realización, incluyendo cualquier deficiencia significativa en el control interno que detectemos en nuestra auditoria.



**M. Vásquez & Asociados**  
**CONTADORES PUBLICOS AUTORIZADOS**  
**CONSULTORES FINANCIEROS IMPOSITIVOS Y ADMINISTRATIVOS**

También proporcionamos a la Gerencia de la Entidad una declaración de que hemos cumplidos con los requisitos éticos aplicables en relación con la independencia y comunicado de cualquier relación y otros asuntos de las que se puede esperar, de manera razonable, pensarse que afectan a nuestra independencia, y en su caso, las correspondientes salvaguardas.

El socio del trabajo responsable por la auditoria que resulta en este informe del auditor independiente es el Lic. Manuel Emilio Monegro Paredes, Exequátur No.3420



M:VASQUEZ & ASOCIADOS

INSC. ICPARD NO.089

INSC.SIB NO. A - 032-0101



MULTICOMPUTOS, SRL  
BALANCE GENERAL  
AL 31 DE DICIEMBRE DEL 2016  
VALORES EN RD\$

**ACTIVOS**

**CORRIENTES**

Efectivo en Caja y Bancos	191,488,479
Cuentas y Documentos por cobrar	124,771,258
Mercancía en Transito	8,900,289

**TOTAL ACTIVOS CORRIENTES** **325,160,026**

**PROPIEDAD, PLANTA Y EQUIPOS**

Mobiliarios y Equipos de oficina	863,546
Equipos de Transporte	6,088,568
Equipos de Arrendamiento	1,210,990
Mejoras	117,967

**TOTAL PROPIEDAD, PLANTA Y EQUIPOS** **8,281,071**

**ACTIVOS DIFERIDOS**

Programas de Computadora	7,860
--------------------------	-------

**OTROS ACTIVOS**

Depósitos y Fianzas	42,030
Anticipos ISR	33,277,985
Saldo a Favor ITBIS	5,655,036
Publicidad	18,715
Pagos Anticipados	163,948
Proyectos en Proceso	38,094,635
Anticipos Proveedores	214,087

**TOTAL OTROS ACTIVOS** **77,466,436**

**TOTAL ACTIVOS** **410,915,393**

MULTICOMPUTOS, SRL  
BALANCE GENERAL  
AL 31 DE DICIEMBRE DEL 2016  
VALORES EN RD\$

PASIVOS Y PATRIMONIO DE ACCIONISTAS

CORRIENTES

Cuentas por Pagar Proveedores	80,643,841
Anticipo Clientes	14,174,798
Retenciones y Acumulaciones	46,845,478
Otras Cuentas por Pagar	1,332,918


TOTAL PASIVOS CORRIENTES 142,997,035

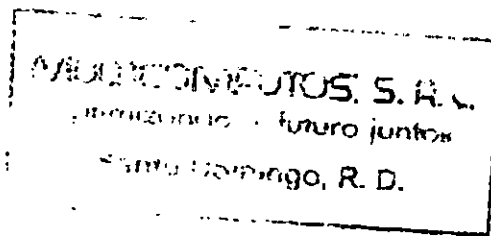
PATRIMONIO DE ACCIONISTAS

Acciones Emitidas	180,397,300
Reserva Legal	5,177,747
Resultado de Periodos Anteriores	43,786,749
Resultados del Periodo después de Imp/Renta	38,556,562

TOTAL PATRIMONIO DE ACCIONISTAS 267,918,358

TOTAL PASIVO Y CAPITAL 410,915,393

  
ING. VIRGILIO ALBERT  
GERENTE



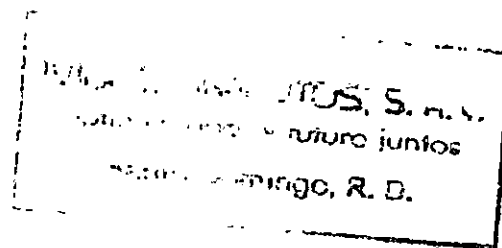


MULTICOMPUTOS, SRL  
ESTADO DE RESULTADOS  
AL 31 DE DICIEMBRE DEL 2016  
VALORES EN RD\$

INGRESOS

Ventas Netas	870,634,406
Menos: Costo de Ventas	<u>727,988,471</u>
Utilidad Bruta en Ventas	142,645,935
Más: Otros Ingresos	<u>6,278,375</u>
Utilidad Bruta en Operaciones	148,924,310
Menos: Gastos Operacionales	
Gastos Generales y Administrativos	<u>93,327,248</u>
Total Gastos de Operación	93,327,248
Resultados Antes de Impuestos	55,597,062
Menos: Impuestos Sobre la Renta	<u>15,011,207</u>
UTILIDAD NETA DEL PERIODO	40,585,855
Menos aumento de la Reserva Legal	<u>2,029,293</u>
UTILIDAD NO DISTRIBUIDA	<u>38,556,562</u>

  
ING. VIRGILIO ALBERT  
GERENTE





***MONEDAS EN QUE SE EXPRESAN LAS CIFRAS***

Las cifras contenidas en los presentes estados financieros están expresados en pesos dominicanos (RDS), cuya equivalencia con el dólar al 31 de diciembre del 2016 es como sigue:

RDS46.62    US\$1.00

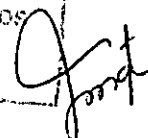
A handwritten signature in black ink, located in the bottom right corner of the page. The signature is stylized and appears to be a name, possibly "Jorge".



# Procedimiento de Escalación, para garantía y soporte

**CITRIX®**  
**NetScaler**

MULTICÓMPUTOS® SAL  
optimizando el futuro juntos  
Santo Domingo, R.D.  
Versión 1.0  
15/08/2017



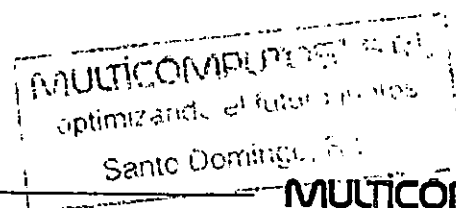
## 1 Personas contacto para solicitudes de servicio.

---

Las personas contacto son las autorizadas por el cliente y registradas por Multicómputos en el contrato de soporte o Control de Equipos en Garantía para abrir solicitudes de servicio. El listado de personas contacto es un documento dinámico que puede ser modificado a solicitud escrita del cliente.

Por ello se realizó especialmente para informar acerca del procedimiento de atención al cliente, los medios de comunicación para acceso normal y de contingencia a la infraestructura y los niveles de servicio. A continuación algunos elementos que definen el perfil de las personas contacto y su rol en el soporte:

- Deben tener conocimientos técnicos de la plataforma instalada en el Cliente.
- Estarán entrenados adecuadamente en el procedimiento de Soporte del Centro de Atención al Cliente y los medios de comunicación y de contingencia.
- Las personas contacto fijarán la prioridad de su solicitud de servicio (urgente, seria y no crítica) de acuerdo a las definiciones incluidas en los niveles de servicio.
- Manejan la información sobre los niveles de servicio acordados en el contrato o Equipos bajo Garantía, particularmente lo referido a tiempos de respuesta telefónico, en sitio y por soporte de hardware y software.
- Intercambian información con los ingenieros de soporte de Multicómputos que atienden las solicitudes de servicio hasta el cierre de las mismas, por ejemplo, instrucciones para instalación de herramientas, envío de las informaciones resultantes de los mismos, etc.
- Participan en el plan de soporte y las revisiones en sitio.
- Para recibir cualquier asistencia adicional, a continuación los contactos de Multicómputos S.R.L.



**MULTICÓMPUTOS**

**1.1 Lista de Contactos y Teléfonos para Soporte Técnico:**

**1.1.1 Multicóputos, S. R. L.**

**1. Horario Normal: 8:00 A. M. a 05:45 P.M.**

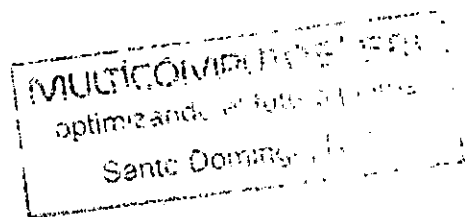
Asistente de Servicios	Carla Espino	Ofic. (809)-540-2846 Opcion 1	<a href="mailto:Asist_servicios@Multicóputos.com">Asist_servicios@Multicóputos.com</a>
Director de Operaciones	Martin Guzman	(809)-540-2846 x 228	<a href="mailto:Martin.guzman@Multicóputos.com">Martin.guzman@Multicóputos.com</a>

**2 Informaciones de Equipos y Cobertura**

**2.1 Niveles de Servicio**

Su llamada de servicio se puede clasificar de tres (3) maneras según su prioridad:

- Urgente – Prioridad 1: Equipo sin prestar servicio, equipo caído.
- Serio – Prioridad 2: Equipo prestando servicio con problemas.
- No Crítico – Prioridad 3: Equipo prestando servicio con operación normal.



### 2.1.1 Consultas técnicas operativas

Al tener un contrato de servicio o Equipos en Garantía dentro de los programas ofrecidos por Multicómputos, Usted tiene el derecho de fijar la prioridad de su llamada, basándose estrictamente en las definiciones anteriores.

### 2.2 Asistencia Telefónica

---

La asistencia telefónica sin límites para problemas de Software, Hardware y red está disponible Veinticuatro (24) horas de lunes a domingo, incluyendo los días feriados nacionales.

### 2.3 Asistencia en el Sitio

---

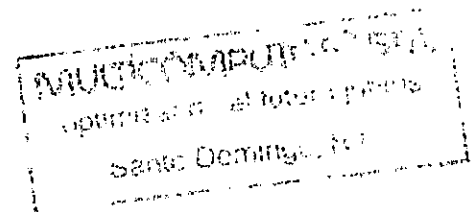
La asistencia en el sitio de instalación para problemas de Hardware está disponible Veinticuatro (24) horas de lunes a domingo, incluyendo los días feriados nacionales.

### 2.4 Prioridad y Tiempo de Respuesta Definido por el Cliente

---

Según su contrato adquirido los tiempos de respuesta telefónicos son:

- **Urgente:** Transferencia al instante o dentro de un máximo de quince (15) minutos de la solicitud de servicio. El personal llegará al sitio de instalación dentro de dos (2) Horas después de la Solicitud de Servicio, para problemas de Software y/o Hardware.
- **Serio:** Respuesta a la llamada dentro de dos (2) horas después de la Solicitud. El personal llegará al sitio de instalación dentro de cuatro (4) horas después de la solicitud de servicio para problemas de Software y/o Hardware.
- **No Crítico:** Respuesta a la llamada dentro de cuatro (4) horas después de la solicitud de servicio. El personal llegará al sitio de instalación después de un día hábil o a una hora mutuamente convenida (posterior al siguiente día hábil) después de la solicitud de servicio, para problemas de Software y/o Hardware.



**MULTICÓMPUTOS**

La entrega de piezas para reparación de equipos debe ocurrir en un término de 4 horas contadas desde que se detecta la necesidad de reemplazo de pieza.

El cliente cuenta con el "Escalamiento Gerencial", que permite además que tanto el Director de Operaciones Técnicas como el Gerente General de Soporte de Múltiples Computos estén informados sobre la atención al cliente, si el cliente así lo solicitara, en caso de que este método no funcione apropiadamente o por otros motivos.

### 3 Procedimiento de Soporte del Centro de Atención al Cliente

#### PARA SOPORTE FUERA DE HORARIO FAVOR LLAMAR AL (809)-722-1951

Para atender su solicitud rápidamente, es conveniente que tenga la siguiente información antes de contactar a nuestro Centro de Atención al Cliente:

- Persona contacto:** [ ]
- Tipo de Equipo** [ ]
- Marca** [ ]
- Modelo** [ ]
- Número de serial del equipo:** [ ]

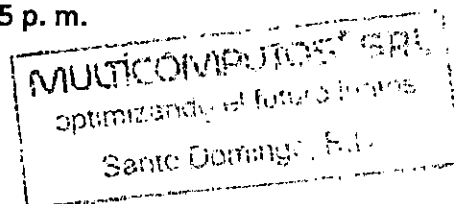
Descripción del problema: [ ]

Acciones correctivas que ya se hayan tomado: [ ]

- Fecha:** [ ]
- Hora:** [ ]

El cliente debe llamar al Centro de Atención al Cliente por el Telf. 809-540-2846 Opción 1 para solicitar un servicio, soporte o instalación.

El horario del Centro de Atención al Cliente es de 8:00 a. m. a 5:45 p. m.



**MULTICOMPUTOS**

Al cliente se le indicará un Número de Orden de Servicio el cual deberá ser utilizado como referencia y para consultar el estado de dicha orden, desde su inicio hasta la completación del soporte.

Un ingeniero del Centro de Atención al Cliente se comunicará con el cliente dentro de los tiempos establecidos en los niveles de servicios acordados según el contrato o la garantía adquirida. Es importante recalcar que el personal que atiende al cliente por el (809)-540-2846 opción 1 tiene la responsabilidad de registrar y enrutar la llamada al ingeniero que atenderá el caso; no representa un primer nivel de soporte técnico.

El cliente debe tener personal con los conocimientos necesarios para que nuestros ingenieros puedan efectuar un diagnóstico adecuado y resolver el problema.

Las instalaciones se consideran actividades sujetas a planificación, por lo que se ejecutarán dentro de los cinco (5) días hábiles siguientes a la llamada del cliente.

Las instalaciones fuera de horario de oficina tienen un costo adicional, para lo cual el cliente debe emitir una orden de compra y solicitar el servicio al menos con cinco (5) días hábiles de anticipación y quedando sujeto a la disponibilidad de nuestros ingenieros.

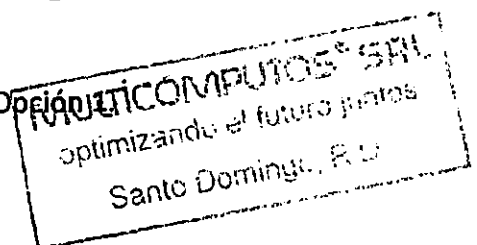
Los servicios no amparados bajo contrato o la garantía adquirida tienen un costo adicional, para lo cual el cliente debe emitir una orden de compra y solicitar el servicio al menos con cinco (5) días hábiles de anticipación y quedando sujeto a la disponibilidad de nuestros ingenieros.

A clientes sin contrato y sin garantía se les enviará una cotización por el servicio requerido, la cuál deberá ser aceptada (para poder el cliente recibir el servicio solicitado) mediante la emisión de una orden de compra. La orden de compra es requisito indispensable para ser atendido.

Medios de Comunicación y de Contingencia al (809) 540-2846 opción 1.

Nuestro objetivo al estar preparados internamente para soporte a clientes, es el de cumplir nuestras obligaciones contractuales, es decir, los niveles de servicios por ustedes contratados. Hemos implementado varios medios de comunicación para asegurar al cliente la comunicación con Multicómputos, aún en situaciones de contingencia:

Teléfono de atención en horario de oficina: (809) 540-2846 Opción 1



A handwritten signature in black ink, appearing to be "Josef", located in the bottom right corner of the page.

Para llamadas fuera de horario de oficina contactar en el siguiente orden a:

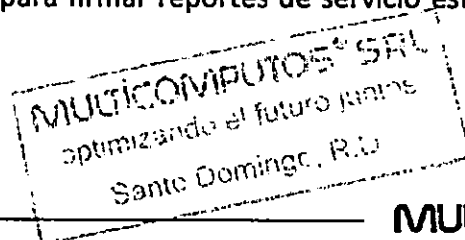
Nivel de Soporte	Descripción	Periodo de Respuesta Telefónica		Numero Localizable
		Desde	Hasta	
1	Gerente de Guardia	Inicio de Llamada	Primeros 15 Minutos	(809)-722-1951
2	Ingeniero de Servicio de Turno	16 Minutos	30 Minutos	N/A
3	Director de Operaciones y Servicios	31 Minutos	En adelante	(809)-722-1978

**3.1 Limitaciones en el Servicio:**

Este contrato está limitado a corregir fallas o errores propios de los sistemas. El mismo no incluye: a) accesorios o implementos operacionales; b) abastecimientos o artículos de consumo para la operación de los sistemas; c) terminación de los sistemas o provisión de materiales para ese objeto; d) trabajos eléctricos externos de los sistemas; e) mantenimiento de accesorios, alteraciones u otros productos que no hayan sido proporcionados por Multicómputos; f) gastos de desinstalación, g) reconfiguraciones que no sean motivadas por una falla del equipo, h) reinstalación de los sistemas que no sean motivadas a una falla de los mismos a un cambio (upgrade de sistema operativo); i) fallas de los equipos motivadas por descargas eléctricas o condiciones fuera de las normas para manejo de los equipos.

**3.2 Procedimientos de Backup y Recuperación:**

El Cliente debe establecer y mantener un procedimiento externo a los sistemas para la reconstrucción de archivos, datos o programas perdidos o alterados. El Cliente debe asegurarse que un representante suyo, autorizado para firmar reportes de servicio esté presente durante el servicio.



**MULTICÓMPUTOS**

### 3.3 El Cliente debe proveer:

---

- Acceso razonable y seguro a los sistemas.
- Espacio y medios adecuados en el sitio de instalación para que Multicómputos pueda prestar servicios a los sistemas.
- Cooperación en el mantenimiento de un Registro de Actividades del Sitio (si el Cliente selecciona esta opción).
- El Cliente deberá mantener las condiciones ambientales, electromagnéticas y la adecuada energía eléctrica según haya sido especificado por el fabricante.
- Si este acuerdo aplica para componentes de Hardware, El Cliente reconoce, que la inspección, el reemplazo y manejo de los componentes del hardware pueden ser peligrosos, y que las tareas de soporte relacionadas con los sistemas deben ser realizadas sólo por personal de servicio calificado con la capacitación y experiencia técnica apropiadas para identificar estos peligros (por ej. descargas electrostáticas) y observar todos los procedimientos de protección y precauciones. El Cliente acuerda usar personal de servicio calificado y emplear seguridad adecuada al cumplir con sus obligaciones acordadas en el presente instrumento.

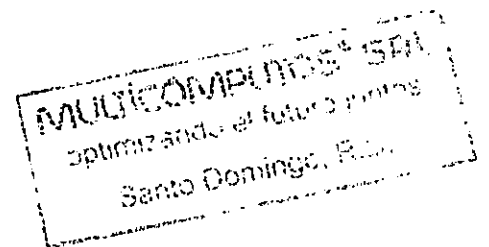
### 3.4 Escalación:

---

En caso de que no haya podido comunicarse a través de ninguno de los medios anteriores ó que el servicio recibido no esté de acorde con lo esperado sírvase llamar a Multicómputos por alguno de los siguientes medios:

\* (809) 540-2846 y dejar un mensaje con su número de teléfono, a fin de devolverle la llamada a la brevedad posible.

Para presentar sugerencias generales de mejoras o quejas del servicio recibido, por favor utilice la dirección de correo electrónico [info@multicómputos.com](mailto:info@multicómputos.com).



**MULTICÓMPUTOS**

A handwritten signature in black ink, appearing to be "Jorge".



---

## **Anexos (Documentos de Soporte)**

---

# AppExpert

Sep 14, 2016

The following topics provide a conceptual reference and configuration instructions for the AppExpert and other features of the NetScaler appliance.

Action Analytics	Collects run-time statistics on the basis of pre-defined criteria. When used with policies, the feature also provides you with the infrastructure for automatic, real-time traffic optimization.
AppExpert Applications and Templates	Simplify configuration steps for the Citrix® NetScaler® appliance by using applications, application templates, NetScaler Gateway applications, and entity templates.
Entity Templates	Describes how to use entity templates to set up and configure individual NetScaler entities, such as a policy or virtual server. An entity template provides a specification and a set of defaults for the object.
AppQoE	Application level Quality of Experience (AppQoE) integrates several existing policy-based security features of the NetScaler appliance into a single integrated feature that takes advantage of a new queuing mechanism, fair queuing.
HTTP Callouts	An HTTP request that the NetScaler appliance generates and sends to an external application when certain criteria are met during policy evaluation.
Pattern Sets	Allow string matching during the evaluation of a default syntax policy.
Policies and Expressions	Rules that determine the operations that the NetScaler appliance must perform.
Rate Limiting	Defines the maximum load for a given network entity or virtual entity on the NetScaler appliance.
Responder	Bases responses on who sends the request, where it is sent from, and other criteria with security and system management implications.
Rewrite	Rewrites information in the requests or responses handled by the NetScaler appliance.
String Maps	Perform pattern matching in all NetScaler features that use the default policy syntax.

Give us your feedback



**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use

MULTICOMPUTOS® SAL  
optimizando al futuro juntos  
Santo Domingo, R.D.

*[Handwritten signature]*



**ICSA Labs**  
**Web Application Firewalls (WAF) Certification Testing Report**  
**WAF – Criteria Version 2.1**

**Citrix Systems, Inc.**

Citrix NetScaler AppFirewall

May 6, 2016

Prepared by ICSA Labs  
 1000 Bent Creek Blvd., Suite 200  
 Mechanicsburg, PA 17050  
[www.icsalabs.com](http://www.icsalabs.com)

WAFX-CITRIXSYST-2016-0506-01



MULTICOMPUTOS® SRI  
 optimizando el futuro juntos  
 Santo Domingo, R.D.  
*Jose*

Citrix Systems, Inc.  
 Web Application Firewalls Certification Testing Report  
 WAF – Criteria Version 2.1



**Table of Contents**

Executive Summary .....	1
Introduction .....	1
Customer Provided Product Overview .....	1
Scope of Assessment .....	1
Summary of Findings .....	1
Certification Maintenance .....	1
Candidate WAF Product Components .....	2
Introduction .....	2
Hardware .....	2
Software .....	2
Documentation .....	2
Introduction .....	2
Candidate WAF Product Configuration .....	2
Documentation .....	3
Introduction .....	3
Results .....	3
Functional and Vulnerability Testing .....	3
Introduction .....	3
Results .....	3
Logging .....	4
Introduction .....	4
Results .....	4
Administration .....	4
Introduction .....	4
Results .....	4
Persistence .....	5
Introduction .....	5
Results .....	5
Criteria Violations and Resolutions .....	5
Introduction .....	5
Results .....	5
Testing Information .....	6
Lab Report Date .....	6
Test Location .....	6
Product Developer's Headquarters .....	6



## Executive Summary

### Introduction

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 20 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

ICSA Labs manages and facilitates technology consortia that focus on emerging, well-defined technologies. The consortia provide for information exchanges among industry leading developers, and for the development of product testing and certification programs and standards. For more information about ICSA Labs, please visit [www.icsalabs.com](http://www.icsalabs.com).

### Customer Provided Product Overview

Citrix® NetScaler AppFirewall™ is a comprehensive web application security solution that blocks known and unknown attacks against web and web services applications. NetScaler AppFirewall enforces a hybrid security model that permits only correct application behavior and efficiently scans and protects known application vulnerabilities. It analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

### Scope of Assessment

ICSA Labs Web Application Firewalls (WAF) certification program test and certify products that implement security policy enforcement for the protection of HTTP and HTTPS Web-based applications. In conjunction with ongoing efforts in the industry to classify and categorize application security issues and mitigate potential vulnerabilities, the Web Application Firewall certification criteria was developed to provide security managers, application developers and others deploying web based applications with confidence in the products that secure vital application services from exploitation or attack.

### Summary of Findings

The Candidate WAF Product has met all of the WAF criteria elements and therefore has retained ICSA Labs WAF Certification. The Candidate WAF Product will remain continuously deployed at ICSA Labs for the length of the testing contract and will be periodically checked as new attacks and vulnerabilities are discovered. In the event that the Candidate WAF Product is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs will work with the vendor to resolve the problems in order for the Candidate WAF Product to maintain its ICSA Labs WAF Certification.

### Certification Maintenance

The Candidate WAF Product, like all products and product groups that are granted ICSA Labs WAF Certification, will remain certified on this and future released versions of the product for the length of the testing contract. Future versions will be certified since the product is continuously deployed at ICSA Labs and subjected to periodic spot-checks on the most current product version.

Three circumstances will cause the Candidate WAF Product to have its ICSA Labs WAF Certification revoked:

1. The Candidate WAF Product vendor withdraws from the ICSA Labs WAF Certification Program.
2. The product fails a periodic spot-check and The Candidate WAF Product vendor subsequently fails to provide an adequate fix within a prescribed length of time.



3. The product fails to meet the next full test cycle against the current version of the criteria.

## Candidate WAF Product Components

### Introduction

The term Candidate WAF Product refers to the complete system submitted by the vendor for certification testing including all documentation, hardware, firmware, software, host operating systems, and management systems. Common network services such as Syslog, DNS, NTP, etc. are provided by ICSA Labs and are not considered part of the Candidate WAF Product.

### Hardware

- NetScaler 14020

### Software

Testing began and was successfully completed with version NS11.0.65.31.nc.

### Documentation

To satisfy documentation requirements, Citrix Systems, Inc. provided ICSA Labs with the following documents in order to assist in the installation, configuration, and administration of the Candidate WAF Product:

- Citrix Product Documentation for NetScaler 11.0.65.31

### Introduction

Web Application Firewall products can be configured different ways; therefore, ICSA Labs may face many configuration related decisions before and after installing the Candidate WAF Product. During testing, ICSA Labs attempted to exploit the Candidate WAF Product and its protection of services, so configuration decisions were made to prevent exploitation.

### Candidate WAF Product Configuration

ICSA Labs installed and configured the Candidate WAF Product following the vendor's supplied documentation. For the purposes of this testing, the Candidate WAF Product is assumed to be deployed in a firewalled DMZ. Any special configuration or deviations from the documentation that were necessary to execute a test or meet a requirement are documented in this section.

#### Note

The following commands were entered via the SSH command line:

- add policy patset mysql\_errors
- bind policy patset mysql\_errors "Query execution was interrupted"
- bind policy patset mysql\_errors "There was a problem processing the query on the foreign data source."
- bind policy patset mysql\_errors "Query was empty"
- bind policy patset mysql\_errors "Got timeout reading communication packets"
- add rewrite action err\_act replace\_http\_res "HTTP/1.1 500 Internal Error\n\nServer: Apache\n\nContent-length: 97\n\n<HTML><HEAD><TITLE>Internal Error</TITLE></HEAD><BODY><B>Internal Error occured</B></BODY></HTML>"
- set syslogparams-userDefinedAuditlog YES

optimizando el futuro juntos  
COMUNICACIONES SRL  
Santo Domingo, R.D.  
Derecho



- add audit messageaction mact1 INFORMATIONAL "Id: "HTTP.REQ.TXID+Host"+CLIENT.IP.SRC+" "+CLIENT.TCP.SRCPORT+"Dest"+CLIENT.IP.DST+" "+CLIENT.TCP.DSTPORT+" URL:http://"+HTTP.REQ.HOSTNAME+HTTP.REQ.URL+" Method:"+HTTP.REQ.METHOD+"SessionCookie:"+HTTP.REQ.COOKIE.VALUE("store\_cookie")+"Parameters:"+HTTP.REQ.BODY(100).BEFORE\_STR("password=")+"password="+HTTP.REQ.BODY(100).TYPECAST\_NVLIST\_T(=",&").VALUE("password").ENCRYPT
- set audit messageaction custom1 -stringBuilderExpr "HTTP.REQ.URL + \"\|\" + HTTP.REQ.USER.NAME + \"\|\" + CLIENT.IP.SRC + \"\|\" + CLIENT.TCP.SRCPORT"

## Documentation

### Introduction

The Candidate WAF Product documentation should be accurate and applicable to the version tested in providing appropriate guidance for installation, administration, among other information.

### Results

ICSA Labs determined the Candidate WAF Product documentation provided adequate and accurate guidance throughout testing for installation and administration.

The Candidate WAF Product met all documentation requirements. No violations were found in this area throughout testing.

## Functional and Vulnerability Testing

### Introduction

Once configured to enforce a security policy the Candidate WAF Product should properly permit and protect the services allowed by that policy while maintaining the integrity and confidentiality of the data. In this case, "properly" means that the service functions correctly. Confidentiality includes the masking of the internal application structure as well as information displayed to the user of the protected website.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the Candidate WAF Product. ICSA Labs used these tools to attempt to defeat or circumvent the security policy enforced by the Candidate WAF Product or exploit the product itself. The attacks include Denial-of-Service, buffer overflow, cross site scripting (XSS), cross site request forgery (CSRF), improper input validation, session mismanagement, information leakage, and other vulnerability testing.

Since there is overlap between functional and vulnerability testing, the results of both phases of testing are presented here.

### Results

The Candidate WAF Product was not susceptible to the attacks targeting the product or the intended services. The Candidate WAF Product allowed the services to function as expected while maintaining the integrity and confidentiality of the data.

The Candidate WAF Product met all functional and vulnerability requirements. No violations were found in this area throughout testing.



## Logging

### Introduction

The Candidate WAF Product is required to provide an extensive logging capability. In practice, this degree of logging may not be enabled at all times or by default; however, the capability must exist on Candidate WAF Product in the event that detailed logging is needed.

ICSA Labs tested the logging functionality provided by the Candidate WAF Product ensuring that it has the ability to capture and present the required system and network event information to audit security related events. ICSA Labs either configured the local logging mechanism or a remote logging mechanism such as syslog. For all logged events ICSA Labs verified that all required log data were recorded.

### Results

The Candidate WAF Product has the ability to store logs on either the product itself or send the logs to a host. To meet specific persistence requirements, the Candidate WAF Product was configured to send log messages to a private host via syslog.

The following log example is an unsuccessful login attempt taken from syslog.

```
Apr 15 15:10:59 10.32.16.69 04/15/2016:11:12:54 GMT citrix-nsmpr8200 0-PPE-2 : default GUI CMD_EXECUTED 15625 0 : User admin - Remote_ip 172.26.25.26 - Command "login admin "*****" - Status "ERROR: Invalid username or password"
```

The Candidate WAF Product met all logging requirements. No violations were found in this area throughout testing.

## Administration

### Introduction

Web application firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor provided administration software, from a web browser based interface, via some non-networked connection such as a serial port, or some other means, authentication must be possible before access to administrative functions is granted. ICSA Labs tested not only that authentication mechanisms existed but also that they could not be bypassed and that the remote administration traffic was encrypted and provided session controls.

### Results

The Candidate WAF Product was remotely administered from the private network using the available web-based GUI, as well as SSH. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful. The remote administration session controls functioned as expected.

The Candidate WAF Product met all administration requirements. No violations were found in this area throughout testing.

Santo Domingo, R.D.  
Optimizando el  
COMPU  
OS SRI  
no juntos  
Avec



## Persistence

### Introduction

Power outages, electrical storms, and inadvertent power losses should not cause the Candidate WAF Product to lose valuable information such as the remote administration configuration, security policy being enforced, log data, time and date, and authentication data. This section documents the findings of ICSA Labs testing of the Candidate WAF Product against the persistence requirements.

### Results

The Candidate WAF Product continued to maintain its configuration, settings, data, and enforcement of the security policy when power was restored following a forced power outage.

The Candidate WAF Product met all persistence requirements. No violations were found in this area throughout testing.

## Criteria Violations and Resolutions

### Introduction

In the event that ICSA Labs uncovers criteria violations while testing the Candidate WAF Product, the vendor must make repairs before testing can be completed and certification granted. The section that follows documents all criteria violations discovered during testing.

### Results

The Candidate WAF Product met all WAF Certification Criteria requirements. No violations were found throughout testing.



## Testing Information

This report is issued by the authority of the Managing Director, ICSA Labs. Tests are done under normal operating conditions.

### Lab Report Date

May 6, 2016

Please visit [www.icsalabs.com](http://www.icsalabs.com) for the most current information about this and other products.

### Test Location

ICSA Labs  
1000 Bent Creek Blvd., Suite 200  
Mechanicsburg, PA 17050



### Product Developer's Headquarters

Citrix Systems, Inc.  
4988 Great America Parkway  
Santa Clara, CA 95054  
USA



This test is accredited under ICSA Labs' ISO/IEC 17025 accreditation issued by ANSI-ASQ National Accreditation Board. Refer to certificate and scope of accreditation number AT – 1423.

Copyright © 2016 ICSA Labs. All rights reserved. Testing reports shall not be reproduced except in full, without prior written approval of ICSA Labs.

MULTICOMPUSRI  
optimizando el futuro  
Santo Domingo, R.D.  
Tercer

## Citrix NetScaler AppFirewall and Web App Security Service

Citrix® NetScaler AppFirewall™ is a comprehensive full function ICSA, Common Criteria, FIPS-certified web application firewall that analyzes all bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats. It provides the ability to perform deep-packet inspection of HTTP, HTTPS and XML as well as protection against OWASP top 10. NetScaler AppFirewall threat protection includes and is not limited to SQL injection attacks, cross-site scripting attacks, cookie tampering, form validation and protection, HTTP and XML reply and request format validation, JSON payload inspection, signature and behavior based protections, data loss prevention (DLP) support including the monitoring of traffic for intended and unintended data exposure, DoS protection, authentication, authorization and auditing support and reporting, and policy tools that provide for easier PCI-DSS compliance verification



### Delivers PCI-DSS v.3.2 compliance

- Protects credit and debit card account numbers to comply with the Payment Card Industry Data Security Standards.
- Prevents data losses for which government regulations require customer notification.
- Simplifies desktop management.

### Protects online revenue sources

- Improves uptime of web sites and web services by defeating L7 denial of service (DoS) attacks.
- Application learning ensures protection without false positives.
- Maintains trust relationship between consumer and vendor by preventing cross-site scripting (XSS) and cross-site request forgery attacks.

NetScaler AppFirewall technology is included in and integrated with Citrix® NetScaler™ MPX and VPX, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler AppFirewall is also available as a stand-alone solution on several NetScaler MPX appliances. The stand-alone NetScaler AppFirewall module can be upgraded via software license to a full NetScaler Application Delivery Controller (ADC).

We also have a cloud-based service through NetScaler Web App Security Service\* that protects customers' web applications and infrastructure from cyber security attacks.

### Addressing security challenges

Not only are web applications vulnerable to attack, they are attractive targets for hackers because they often have direct connectivity with one or more databases containing sensitive customer and company information. Threats against web applications are often devised specifically for a target application, making threat identification by network-level security devices (e.g., intrusion protection systems and network firewalls) impossible—leaving web applications exposed to a myriad

of known and zero-day exploits. NetScaler AppFirewall comprehensively addresses the challenge of delivering centralized application-layer security for all web applications and web services.

### Hybrid security model

NetScaler AppFirewall enforces both positive and negative security models to ensure correct application behavior. The positive security model understands good application behavior and treats all other traffic as malicious. This is the only proven approach delivering zero-day protection against unpublished exploits. Scanning of thousands of automatically updated signatures provides protection against known attacks.

### Meeting PCI compliance and auditing requirements

NetScaler AppFirewall aids corporate IT security teams in conforming to governmental privacy regulations and industry mandates. For example, organizations subject to Payment Card Industry Data Security Standard (PCI-DSS) requirements can now fully meet the requirements detailed in PCI-DSS Section 6.6, which mandates the

installation of web application firewall in front of public-facing applications as one method of maintaining a proper security posture. In support of PCI security audits, NetScaler AppFirewall can generate dedicated reports detailing all security protections defined in the application firewall policy that pertain to PCI requirements. In addition, NetScaler AppFirewall prevents the inadvertent leakage or theft of sensitive information, such as credit card numbers or custom-defined data objects, by either removing or masking content from application responses—before being publicly disclosed.

### Defeating XML-based threats

In addition to detecting and blocking common application threats that can be adapted for attacking XML-based applications (i.e. cross-site scripting, command injection, etc.), NetScaler AppFirewall includes a rich set of XML-specific security protections. These include schema validation to thoroughly verify SOAP messages and XML payloads, and a powerful XML attachment check to block attachments containing malicious executables or viruses. Automatic traffic inspection methods block XPath injection attacks on URLs and forms aimed at gaining access. NetScaler AppFirewall also thwarts a variety of DoS attacks, including external entity references, recursive expansion, excessive nesting and malicious messages containing either long or a large number of attributes and elements.

### Tailoring security policies

NetScaler AppFirewall incorporates an advanced and proven adaptive learning engine that discovers aspects of application behavior that might be blocked by the positive security model even if the behavior is intended by the web application. This would include, for example, modifications made by client-side application scripting that legally modifies HTML form fields. Once application behavior is learned, NetScaler AppFirewall generates human-readable policy recommendations, which bring to security managers a clearer understanding of actual application behavior. Tailored security policies may then be applied to each application.

### Industry-leading performance

NetScaler AppFirewall provides high capacity application security throughput to meet the needs of even the largest networks. In addition, the solution can actually improve application performance and lower response times by offloading compute-intensive tasks, such as TCP connection management, SSL encryption and compression from web servers. In addition, the integrated caching functionality available on the NetScaler platform offloads the servers while still applying full firewall functionality. Freeing valuable server resources improves the overall application experience.

### IP Reputation Service is Built-In

NetScaler IP Reputation Service is built-in into NetScaler. This service is available at no extra cost with NetScaler AppFirewall solution. No service contract, no yearly renewals necessary.

NetScaler IP Reputation Service provides a continuously updated list of malicious IP addresses in near real-time, providing an additional layer of protection and helping to reduce the burden on security teams. Rather than relying on static, rapidly out-of-date public black lists, the NetScaler IP Reputation service automatically analyzes and correlates feeds from millions of global sensors in real-time and is updated every five minutes.

### Flexibility to adapt to changing business requirements

NetScaler AppFirewall permits flexible, stepwise deployment of web application protection. The default web application protection profile defends against the most common dangerous threats and adds full protection against both data theft and layer 4-7 denial of service (DoS) attacks. The advanced web application protection profile adds session-aware protections to protect dynamic elements, such as cookies, form fields and session-specific URLs. Attacks that target the trust between the client and server including cross-site request forgery are stopped, requests are validated by checking for a unique ID inserted by NetScaler. Such protection is imperative for any application that processes user-specific content, such as an e-commerce site. To make sure these

NetScaler AppFirewall is a registered trademark of Citrix Systems, Inc.  
 © 2013 Citrix Systems, Inc. All rights reserved.  
 Santo Domingo, R.D.



  
 C&I.com  
 Sano Domingo, R.D.  
**MULTICOMPUTOS e SRL**  
 optimizando el futuro juntos

NetScaler AppFWall Model		MPX 1150		MPX 1150		MPX 1150	
Memory	8 GB	8 GB	32 GB	48 GB	48 GB	48 GB	48 GB
Ethernet ports	6x10/100/1000 BASE-T or 6x100BASE-T-SFP and 4x1000BASE-X-SFP+	6x10/100/1000 BASE-T or 6x100BASE-T-SFP and 4x1000BASE-X-SFP+	Upgrade option to MPX 11540	Upgrade option to MPX 11540	4x1000 BASE-X-SFP+ and 4x1000 BASE-X-SFP+	4x1000 BASE-X-SFP+ and 4x1000 BASE-X-SFP+	4x1000 BASE-X-SFP+ and 4x1000 BASE-X-SFP+
Upgrade Option							
Platform performance							
Throughput Basic mode (Gbps)	0.5	5.3	5.4	14	17	20	25,000
SSL transactions/second	1,500	2,800	6,500	22,500	43,000	43,000	43,000
Platform mechanical environment and regulatory							
Power supplies	Single	Single	Single-Optional	Second	Dual	Dual	Dual
Height	1U	1U	1U	1U	2U	2U	2U

- security measures are compatible with any application. NetScaler AppFWall learning capabilities help the administrator create managed exceptions and relaxations when the application is rendered—and legal—behavior might otherwise cause a violation of the default security policy.
- NetScaler Web App Security Service based service that protects customers' web applications and infrastructure from application and network level attacks. It has historical applications and create reports using a simplified GUI.
- Easy of Use: Quick and easy to deploy, manage, and create reports using a simplified GUI.
- NetScaler Web App Security Service is cloud-based service that protects customers' web applications and infrastructure from application and network level attacks. It has historical applications and create reports using a simplified GUI.
- Fast Deployment: Click & Protect with NetScaler Web App Security Service — less than 5 clicks from first time login to protection.
- Comprehensive Security: Protection against web application attacks using signatures, IP blacklisted and whitelisted URLs/applications, IP reputation etc. and helps maintain compliance.

NetScaler Platform		MPX 2560-40G		MPX 2560-40G		MPX 2560-40G	
Memory	256 GB	256 GB	256 GB	64 GB	64 GB	64 GB	64 GB
Ethernet ports	4x 40GE QSFP+ or 4x 40GE QSFP+ compatible per IEEE802.3-2002/2005/2008/2012	4x 40GE QSFP+ or 4x 40GE QSFP+ compatible per IEEE802.3-2002/2005/2008/2012	16x 10GE SFP+	16x 10GE SFP+	16x 10GE SFP+	16x 10GE SFP+	16x 10GE SFP+
Transceivers support	10GE QSFP+, SR LR 10GE SFP+, SR LR	10GE QSFP+, SR LR 10GE SFP+, SR LR	10GE SFP+, SR LR, 16 cu	10GE SFP+, SR LR, 16 cu	10GE SFP+, SR LR, 16 cu	10GE SFP+, SR LR, 16 cu	10GE SFP+, SR LR, 16 cu
Pay as you grow and burstable license upgrades	Upgrade option to MPX/SOX 2560-40G	Upgrade option to MPX/SOX 2560-40G	Upgrade option to MPX/SOX 14080 and 14100	Upgrade option to MPX/SOX 14080 and 14100	Upgrade option to MPX/SOX 14080 and 14100	Upgrade option to MPX/SOX 14080 and 14100	Upgrade option to MPX/SOX 14080 and 14100
Platform performance							
Throughput Basic mode (Gbps)	44	33	29	26	26	26	26
SSL transactions/sec (2K key certificates)	69,000	43,000	69,000	69,000	69,000	69,000	69,000
Platform mechanical							
Power supplies	2	2	2	2	2	2	2
Height	2U	2U	2U	2U	2U	2U	2U

Note: The above models are available as stand-alone NetScaler AppFWall solutions. Additional application firewall support is provided as an integrated module within NetScaler VPX 10, 200, 1000 and 3000 virtual appliances and all NetScaler MPX Application Delivery Controller (ADC) hardware platforms.

*Handwritten signature*

**CITRIX**

**Enterprise Sales**

North America | 800-424-8749  
Worldwide | +1 408-790-8000

**Locations**  
Corporate Headquarters | 875 Cypress Creek Road Fort Lauderdale, FL 33309 United States  
Silicon Valley | 4988 Creek America Parkway Santa Clara, CA 95054 United States

Copyright © 2007 by Citrix, Inc. All rights reserved. Citrix, The Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the US Patent and Trademark Office and in other countries. All other marks are the property of their respective owners.

**MULTICOMPUTOS S.P.A.**  
Santo Domingo, R.D.  
Calle Comandante el Fuero Junco

**Technical aspects**

- Buffer overflow
- Call ID parameters manipulation
- Form/hidden field manipulation
- Forced browsing protection
- Cookie or session poisoning
- Cross-site scripting (XSS)
- Cross-site request forgery
- Command injection
- SQL injection
- Error logging sensitive information leak
- Insecure use of cryptography
- Server misconfiguration
- Back doors and debug options
- Rate-based policy enforcement
- Web-known platform vulnerabilities
- SQLi array attack protection
- Content rewrite and response control
- Content filtering
- Authentication, authorization and auditing
- (A-Z) DoS protection
- Simplified management and deployment
- User interface
- Secure web-based GUI
- SNET based (L) access network management
- SNET
- Syslog-based logging
- PCI-DSS compliance reporting tool
- Appropriate templates for Web interface and Microsoft SharePoint
- Import/export Application Firewall profiles
- Convert third party application vulnerability tool output to Metasploit rules
- Quick deployment of new rules from Common Event Format (CEF) logs
- Comprehensive web server and web services security
- Deep stream inspection, bi-directional analysis
- HTTP & HTML header and payload inspection
- Full HTML parsing, semantic redirection
- Session-aware and stateful
- HTTP signature scanning
- Scan thousands of signatures
- Response size checks
- Protocol neutrality
- HTML form field protection
- Required fields returned, no added fields allowed.
- Drop-down list & radio button field enforcement
- Form-field name-length enforcement
- Code protection - Signatures to prevent tampering
- Code encryption and proxying
- Legal URL enforcement - Web application content integrity
- Full SSL offload
- Decrypts traffic prior to inspection, encrypts traffic prior to forwarding
- Configurable back-end encryption
- Support for client-side certificates
- XML data protection
- XML security protects against XML denial of service (DoS), XML SSI, and XPath injection and cross site scripting
- XML message and schema validation, format checks, WS - base profile compliance, XML attachments check
- URL transformation
- WSDL scan prevention to protect unpublished APIs
- Support for Cliented POST requests

# Configuring Backup Persistence

Nov 12, 2013

The NetScaler appliance uses backup persistence to choose a new type of persistence when the primary persistence type fails. For example, if the primary persistence type is set to Cookie Insert, and backup persistence is set to Source IP, the NetScaler appliance uses Source IP-based persistence when the cookie is missing from the HTTP header or when the client browser does not support cookies.

You can set a time-out value for backup persistence only when the primary persistence type is HTTP Cookie-based or RTSP session ID-based persistence, and the backup persistence type is Source IP-based.

To set backup persistence for a virtual server by using the command line interface

At the command prompt, type:

```
set lb vserver <name>@ -persistenceType <PersistenceType> -  
persistenceBackup<BackupPersistenceType>
```

## Example

```
set lb vserver Vserver-LB-1 -persistenceType CookieInsert -  
persistenceBackup SourceIP
```

To set backup persistence for a virtual server by using the configuration utility

1. Navigate to Traffic Management > Load Balancing > Virtual Servers.
2. In the details pane, select the virtual server for which you want to configure backup persistence (for example, Vserver-LB-1), and then click Open.
3. The Configure Virtual Server (Load Balancing) dialog box, click the Method and Persistence tab.
4. In the Persistence list, select the persistence type you want (for example, COOKIEINSERT).
5. In the Time-out text box, type the time-out value you want (for example, 20).
6. In the Backup Persistence list, select the backup persistence type that you want to configure (for example, SOURCEIP).
7. In the Backup Time-out and Netmask text boxes, type the backup time-out value and netmask (for example, 20 and 255.255.255.255).
8. Click OK.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use



# Content Switching

May 25, 2015

In today's complex Web sites, you may want to present different content to different users. For example, you may want to allow users from the IP range of a customer or partner to have access to a special Web portal. You may want to present content relevant to a specific geographical area to users from that area. You may want to present content in different languages to the speakers of those languages. You may want to present content tailored to specific devices, such as smartphones, to those who use the devices. The Citrix NetScaler content switching feature enables the NetScaler appliance to distribute client requests across multiple servers on the basis of specific content that you wish to present to those users.

To configure content switching, first create a basic content switching setup, and then customize it to meet your needs. This entails enabling the content switching feature, setting up load balancing for the server or servers that host each version of the content that is being switched, creating a content switching virtual server, creating policies to choose which requests are directed to which load balancing virtual server, and binding the policies to the content switching virtual server. You can then customize the setup to meet your needs by setting precedence for your policies, protecting your setup by configuring a backup virtual server, and improving the performance of your setup by redirecting requests to a cache.

## How Content Switching Works

Updated: 2013-08-22

Content Switching enables the NetScaler appliance to direct requests sent to the same Web host to different servers with different content. For example, you can configure the appliance to direct requests for dynamic content (such as URLs with a suffix of .asp, .dll, or .exe) to one server and requests for static content to another server. You can configure the appliance to perform content switching based on TCP/IP headers and payload.

You can also use content switching to configure the appliance to redirect requests to different servers with different content on the basis of various client attributes. Some of those client attributes are:

- **Device Type.** The appliance examines the user agent or custom HTTP header in the client request for the type of device from which the request originated. Based on the device type, it directs the request to a specific Web server. For example, if the request came from a cell phone, the request is directed to a server that is capable of serving content that the user can view on his or her cell phone. A request from a computer is directed to a different server that is capable of serving content designed for a computer screen.

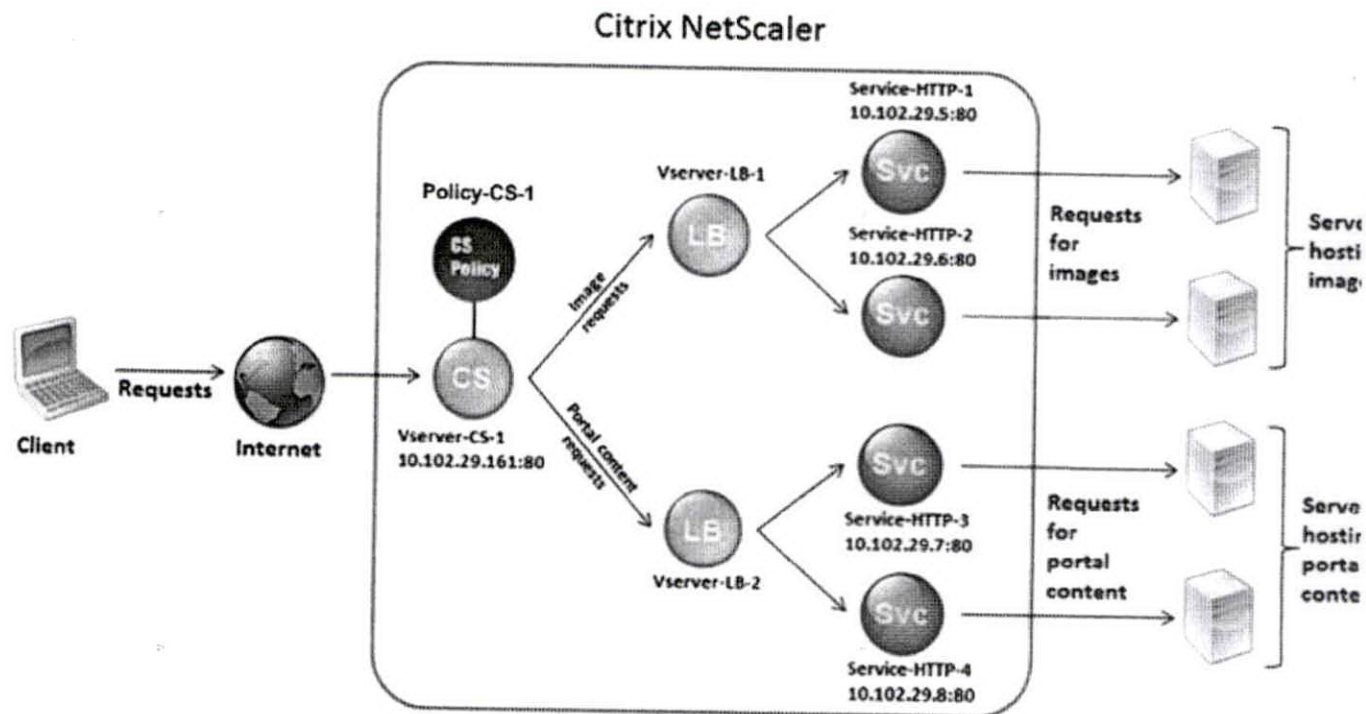


- **Language.** The appliance examines the Accept-Language HTTP header in the client request and determines the language used by the client's browser. The appliance then sends the request to a server that serves content in that language. For example, using content switching based on language, the appliance can send someone whose browser is configured to request content in French to a server with the French version of a newspaper. It can send someone else whose browser is configured to request content in English to a server with the English version.
- **Cookie.** The appliance examines the HTTP request headers for a cookie that the server set previously. If it finds the cookie, it directs requests to the appropriate server, which hosts custom content. For example, if a cookie is found that indicates that the client is a member of a customer loyalty program, the request is directed to a faster server or one with special content. If it does not find a cookie, or if the cookie indicates that the user is not a member, the request is directed to a server for the general public.
- **HTTP Method.** The appliance examines the HTTP header for the method used, and sends the client request to the right server. For example, GET requests for images can be directed to an image server, while POST requests can be directed to a faster server that handles dynamic content.
- **Layer 3/4 Data.** The appliance examines requests for the source or destination IP, source or destination port, or any other information present in the TCP or UDP headers, and directs the client request to the right server. For example, requests from source IPs that belong to customers can be directed to a custom web portal on a faster server, or one with special content.

A typical content switching deployment consists of the entities described in the following diagram.

Figure 1. Content Switching Architecture





A content switching configuration consists of a content switching virtual server, a load balancing setup consisting of load balancing virtual servers and services, and content switching policies. To configure content switching, you must configure a content switching virtual server and associate it with policies and load balancing virtual servers. This process creates a *content group*—a group of all virtual servers and policies involved in a particular content switching configuration.

Content switching can be used with HTTP, HTTPS, TCP, and UDP connections. For HTTPS, you must enable SSL Offload.

When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. The priority of the policy defines the order in which the policies bound to the content switching virtual server are evaluated. If you are using default syntax policies, when you bind a policy to the content switching virtual server, you must assign a priority to that policy. If you are using NetScaler classic policies, you can assign a priority to your policies, but are not required to do so. If you assign priorities, the policies are evaluated in the order that you set. If you do not, the NetScaler appliance evaluates your policies in the order in which they were created.

In addition to configuring policy priorities, you can manipulate the order of policy evaluation by using Goto expressions and policy bank invocations. For more details about default syntax policy configuration, see "Configuring Default Syntax Policies."

After it evaluates the policies, the content switching virtual server routes the request to the appropriate load balancing virtual server, which sends it to the appropriate service.

Content switching virtual servers can only send requests to other virtual servers. If you are using an external load balancer, you must create a load balancing virtual server for it and bind its virtual server as a service to the content switching virtual server.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use

MULTICOMPUTOS® SAL  
optimizando el futuro juntos  
Santo Domingo, R.D.



# Enabling Proxy Support for User Connections

Feb 04, 2014

User devices can connect through a proxy server for access to internal networks. NetScaler Gateway supports the HTTP, SSL, FTP, and SOCKS protocols. To enable proxy support for user connections, you specify the settings on NetScaler Gateway. You can specify the IP address and port used by the proxy server on NetScaler Gateway. The proxy server is used as a forward proxy for all further connections to the internal network.

To configure proxy support for user connections

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced Settings.
4. On the Proxy tab, under Proxy Settings, select On.
5. For the protocols, type the IP address and port number and then click OK.

Note: If you select Appliance, you can configure proxy servers that support secure and unsecure HTTP connections only.

After you enable proxy support on NetScaler Gateway, you specify configuration details on the user device for the proxy server that corresponds to the protocol.

After you enable proxy support, NetScaler Gateway sends the proxy server details to the client Web browser and changes the proxy configuration on the browser. After the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user's network.

To configure one proxy server to use all protocols for NetScaler Gateway

You can configure one proxy server to support all of the protocols that NetScaler Gateway uses. This setting provides one IP address and port combination for all of the protocols.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced Settings.
4. On the Proxy tab, under Proxy Settings, select On.
5. For the protocols, type the IP address and port number.
6. Click Use the same proxy server for all protocols and then click OK.



When you disable split tunneling and set all proxy settings to On, proxy settings are propagated to user devices. If proxy settings are set to Appliance, the settings are not propagated to user devices.

NetScaler Gateway makes connections to the proxy server on behalf of the user device. The proxy settings are not propagated to the user's browser, so no direct communication between the user device and the proxy server is possible.

To configure the NetScaler Gateway to be a proxy server

When you configure NetScaler Gateway as a proxy server, unsecure and secure HTTP are the only supported protocols.

1. In the configuration utility, on the Configuration tab, in the navigation pane, expand NetScaler Gateway and then click Global Settings.
2. In the details pane, under Settings, click Change global settings.
3. On the Client Experience tab, click Advanced Settings.
4. On the Proxy tab, under Proxy Settings, select Appliance.
5. For the protocols, type the IP address and port number and then click OK.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use



# Global Server Load Balancing

Mar 22, 2012

NetScaler appliances configured for global server load balancing (GSLB) provide for disaster recovery and ensure continuous availability of applications by protecting against points of failure in a wide area network (WAN). GSLB can balance the load across data centers by directing client requests to the closest or best performing data center, or to surviving data centers in case of an outage.

Following are some typical GSLB configurations:

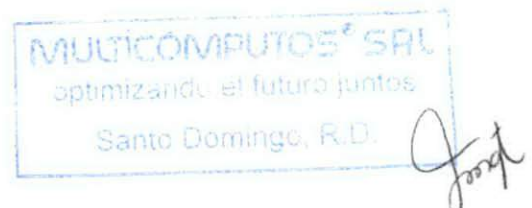
- **Active-active data center setup.** Consists of multiple active data centers. Client requests are load balanced across active data centers.
- **Active-standby data center setup.** Consists of an active and a standby data center. When a failover occurs as a result of a disaster event, the standby data center becomes operational.
- **Proximity setup.** Directs client requests to the data center that is closest in geographical distance or network distance.

In a typical configuration, a local DNS server sends client requests to a GSLB virtual server, to which are bound GSLB services. A GSLB service identifies a load balancing or content switching virtual server, which can be at the local site or a remote site. If the GSLB virtual server selects a load balancing or content switching virtual server at a remote site, it sends the virtual server's IP address to the DNS server, which sends it to the client. The client then resends the request to the new virtual server at the new IP.

The GSLB entities that you must configure are the GSLB sites, the GSLB services, the GSLB virtual servers, load balancing or content switching virtual servers, and authoritative DNS (ADNS) services. You must also configure MEP. You can also configure DNS views to expose different parts of your network to clients accessing the network from different locations.

Note: To take full advantage of the NetScaler GSLB features, you should use NetScaler appliances for load balancing or content switching at each data center, so that your GSLB configuration can use the proprietary Metric Exchange Protocol (MEP) to exchange site metrics.

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use



# Load Balancing Algorithms

Aug 29, 2013

The load balancing algorithm defines the criteria that the NetScaler appliance uses to select the service to which to redirect each client request. Different load balancing algorithms use different criteria. For example, the least connection algorithm selects the service with the fewest active connections, while the round robin algorithm maintains a running queue of active services, distributes each connection to the next service in the queue, and then sends that service to the end of the queue.

Some load balancing algorithms are best suited to handling traffic on websites, others to managing traffic to DNS servers, and others to handling complex web applications used in e-commerce or on company LANs or WANs. The following table lists each load balancing algorithm that the NetScaler appliance supports, with a brief description of how each operates.

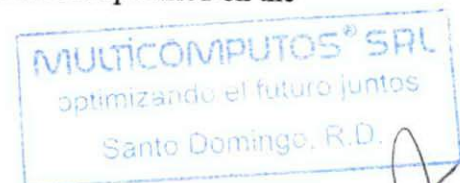
Name	Server Selection Based On
LEASTCONNECTION	Which service currently has the fewest client connections. This is the default load balancing algorithm.
ROUNDROBIN	Which service is at the top of a list of services. After that service is selected for a connection, it moves to the bottom of the list.
LEASTRESPONSETIME	Which load balanced server currently has the quickest response time.
URLHASH	A hash of the destination URL.
DOMAINHASH	A hash of the destination domain.
DESTINATIONIPHASH	A hash of the destination IP address.
SOURCEIPHASH	A hash of the source IP address.
SRCIPDESTIPHASH	A hash of the source and destination IP addresses.
CALLIDHASH	A hash of the call ID in the SIP header.
SRCIPSRCPORTHASH	A hash of the client's IP address and port.

Name	Server Selection Based On
LEASTBANDWIDTH	Which service currently has the fewest bandwidth constraints.
LEASTPACKETS	Which service currently is receiving the fewest packets.
CUSTOMLOAD	Data from a load monitor.
TOKEN	The configured token.
LRTM	Fewest active connections and the lowest average response time.

Depending on the protocol of the service that it is load balancing, the NetScaler appliance sets up each connection between client and server to last for a different time interval. This is called load balancing granularity, of which are three types: request-based, connection-based, and time-based granularity. The following table describes each type of granularity and when each is used.

Granularity	Types of Load Balanced Service	Specifies
Request - based	HTTP or HTTPS	A new service is chosen for each HTTP request, independent of TCP connections. As with all HTTP requests, after the Web server fulfills the request, the connection is closed.
Connection-based	TCP and TCP-based protocols other than HTTP	A service is chosen for every new TCP connection. The connection persists until terminated by either the service or the client.
Time-based	UDP and other IP protocols	A new service is chosen for each UDP packet. Upon selection of a service, a session is created between the service and a client for a specified period of time. When the time expires, the session is deleted and a new service is chosen for any additional packets, even if those packets come from the same client.

During startup of a virtual server, or whenever the state of a virtual server changes, the virtual server can initially use the round robin method to distribute the client requests among the physical servers. This type of distribution, referred to as *startup round robin*, helps prevent unnecessary load on a single server as the initial requests are served. After using the round robin method at the startup, the virtual server switches to the load balancing method specified on the virtual server.



The Startup RR Factor works in the following manner:

- If the Startup RR Factor is set to zero, the NetScaler switches to the specified load balancing method depending on the request rate.
- If the Startup RR Factor is any number other than zero, NetScaler uses the round robin method for the specified number of requests before switching to the specified load balancing method.
- By default, the Startup RR Factor is set to zero.

Note: You cannot set the startup RR Factor for an individual virtual server. The value you specify applies to all the virtual servers on the NetScaler appliance.

#### **To set the startup round-robin factor by using the command line interface**

At the command prompt, type:

```
set lb parameter -startupRRFactor <positive_integer>
```

Example

```
set lb parameter -startupRRFactor 25000
```

#### **To set the startup round-robin factor by using the configuration utility**

1. Navigate to Traffic Management > Load Balancing.
2. Under Settings, click Configure Load Balancing Parameters.
3. In the Configure Load Balancing Parameters dialog box, for Startup RR Factor type a value.
4. Click OK.

# Networking

May 13, 2016

The following topics provide a conceptual reference and instructions for configuring the various networking components on the NetScaler appliance.

IP Addressing	Learn the various types of NetScaler-owned IP addresses and how to create, customize, and remove them.
Interfaces	Configure some of the basic network configurations that must be done to get started.
Access Control Lists (ACLs)	Configure the different types of Access Control Lists and how to create, customize, and remove them.
IP Routing	Learn and configure the routing functionality of the NetScaler appliance, both static and dynamic.
Internet Protocol version 6 (IPv6)	Learn how the NetScaler appliance supports IPv6.
Traffic Domains	Learn and configure traffic domains to segment network traffic for different applications.
VXLAN	Learn and configure VXLANs to meet the scalability needs in your datacenter.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use



# NITRO API

Oct 14, 2015

The NetScaler NITRO protocol allows you to configure and monitor the NetScaler appliance programmatically by using Representational State Transfer (REST) interfaces. Therefore, NITRO applications can be developed in any programming language. Additionally, for applications that must be developed in Java or .NET or Python, NITRO APIs are exposed through relevant libraries that are packaged as separate Software Development Kits (SDKs).

## Important

- XML API are deprecated from NetScaler 10.5 onwards.
- Until specified otherwise, this NITRO documentation applies to NetScaler versions 11.0 and 10.5.

To use NITRO, you must have a basic understanding of the NetScaler appliance and you must make sure that the client application has the following:

- Access to a NetScaler appliance, version 9.2 or later.
- To use REST interfaces, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the NetScaler appliance. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from <http://www.microsoft.com/downloads/en/default.aspx>.
- The Python SDK is available from NetScaler 10.5 onwards. For Python clients, you must have a system with Python 2.7 or above version and the Requests library (available in <NITRO\_SDK\_HOME>/lib) installed. The NITRO library must be installed on the client path. For installation instructions, read the <NITRO\_SDK\_HOME>/README.txt file.

## Obtaining the NITRO Package

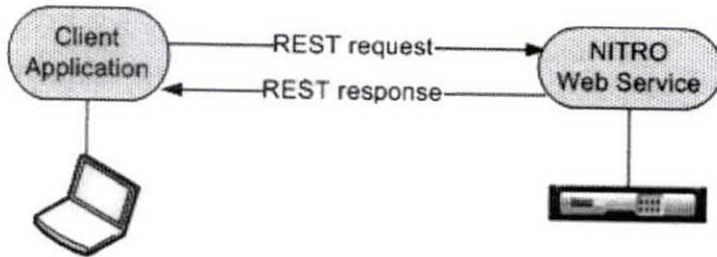
The NITRO package is available as a tar file on the **Downloads** page of the NetScaler appliance's configuration utility. You must download and un-tar the file to a folder on your local system. This folder contains the NITRO libraries in the **lib** subfolder. The libraries must be added to the client application classpath to access NITRO functionality.

**Note:** The REST package contains only documentation for using the REST interfaces.



## How NITRO Works

The NITRO infrastructure consists of a client application and the NITRO Web service running on a NetScaler appliance. The communication between the client application and the NITRO web service is based on REST architecture using HTTP or HTTPS.



As shown in the above figure, a NITRO request is executed as follows:

1. The client application sends REST request message to the NITRO web service. When using the SDKs, an API call is translated into the appropriate REST request message.
2. The web service processes the REST request message.
3. The NITRO web service returns the corresponding REST response message to the client application. When using the SDKs, the REST response message is translated into the appropriate response for the API call.

To minimize traffic on the NetScaler network, you retrieve the whole state of a resource from the server, make modifications to the state of the resource locally, and then upload it back to the server in one network transaction. For example, to update a load balancing virtual server, you must retrieve the object, update the properties, and then upload the changed object in a single transaction.

**Note:** Local operations on a resource (changing its properties) do not affect its state on the server until the state of the object is explicitly uploaded.

NITRO APIs are synchronous in nature. This means that the client application waits for a response from the NITRO web service before executing another NITRO API.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | [Terms of Use](#)

MULTICOMPUTOS<sup>®</sup> SRL  
optimizando el futuro juntos  
Santo Domingo, R.D.



# Optimization

May 13, 2016

The NetScaler optimization features reduce transaction times between the clients and the servers, and they reduce bandwidth consumption. They also enhance server performance by offloading some tasks and making others more efficient.

Client Keep-Alive	Handles multiple requests on a single client connection. The client does not have to negotiate a new connection for each request to the server.
HTTP Compression	Compresses HTTP responses sent from the servers to compression-aware browsers. The smaller responses reduce download time and save bandwidth.
Integrated Caching	Stores responses to client requests. Subsequent requests for the same content are served from the NetScaler cache instead of being forwarded to the origin server.
Front End Optimization	Reduces the load and render time of web pages by simplifying and optimizing the content served to the client browser. Note: Supported from NetScaler 10.5 onwards.
Content Accelerator	Stores server responses on a Citrix ByteMobile T2100 appliance. Note: Supported from NetScaler 10.1 onwards.
SPDY (Speedy)	Acts as a SPDY gateway between clients and your servers, providing SPDY support without the need to configure/upgrade SPDY on the servers. Note: Supported from NetScaler 10.1 onwards.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use

MULTICOMPUTOS<sup>®</sup> S.A.  
optimizando el futuro juntos  
Santo Domingo, R.D.



# Security

May 03, 2013

The following topics cover configuration and installation information for NetScaler security features. Most of these features are policy based.

Authentication, Authorization, Auditing (AAA)	Keeps unauthorized users out of the network, denies users access to tasks for which they are not authorized, and tracks the resources used during user sessions.
Application Firewall	Prevents security breaches, data loss, and possible unauthorized modifications to web sites that access sensitive business or customer information.
Content Filtering	Blocks inappropriate HTML requests, preventing the requests from reaching the Web servers.
HTTP Denial-of-Service Protection	Prevents hackers from attacking your Web site with large numbers of HTTP requests.
Priority Queuing	Detects high-priority connections and allows those connections to proceed ahead of other connections, guaranteeing unimpeded access to those users.
SureConnect	Serves all incoming connections with either the requested content or a custom Web page that displays information about a delay in the request being serviced.
Surge Protection	Detects any rapid rise in connection attempts and adjusts the rate at which connections are allowed to proceed to the server, preventing server overload.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use

MULTICOMPUTOS<sup>®</sup> SAL  
optimizando el futuro juntos  
Santo Domingo, R.D.  
*Jmd*

# Traffic Management

Nov 09, 2016

The following topics cover configuration and installation information for NetScaler traffic management features.

Cache Redirection	Analyzes incoming requests and forwards the requests for already cached data to cache servers. Dynamic HTTP requests and non-cacheable requests are forwarded to the origin servers. Cache redirection is a policy-based feature.
Content Switching	Analyzes client requests and redirects the requests to specific servers on the basis of geographical area, authorization credentials, and device from which the request was initiated.
DataStream	Ensures optimal distribution of traffic from the application and web servers to the database servers. Enables you to segment traffic according to information in the SQL query and on the basis of database names, user names, character sets, and packet size.
Domain Name System	Provides authoritative domain name server (ADNS server) functionality for a domain. The NetScaler appliance functions as a DNS end resolver and forwarder, and also helps in name resolution when fully qualified domain names are not configured.
Firewall Load Balancing	Distributes the traffic across multiple firewalls, providing fault tolerance, increased throughput, and high availability.
Global Server Load Balancing	Enables disaster recovery and ensures continuous availability of applications by protecting against points of failure in a wide area network (WAN).
Link Load Balancing	Load balances outbound traffic across multiple Internet connections to transmit packets seamlessly over the best possible link.
Load Balancing	Distributes user requests for web pages and other protected applications across multiple servers to prevent server overloading and failure. Load balancing also provides fault tolerance.
SSL Offload and Acceleration	Offloads SSL processing from a server to the NetScaler appliance to accelerate SSL transactions.

**CITRIX**

© 1999-2017 Citrix Systems, Inc. All rights reserved. | Terms of Use

MULTICOMPUTOS® SRL  
optimizando el futuro juntos  
Santo Domingo, R.D. *J. J. J.*



## Firewall de aplicaciones web: ofrece la protección imprescindible para la empresa moderna

Descubra lo que las soluciones de seguridad de red tradicionales no pueden hacer y por qué su organización necesita un firewall de aplicaciones web como piedra angular de su estrategia de seguridad de TI

**CITRIX**

Proteger eficazmente las propiedades web que están generalizadas a través de las organizaciones de hoy depende de un conocimiento profundo de las capacidades y las limitaciones de las tecnologías de seguridad disponibles. Por ejemplo, aunque los firewall de red tradicionales y los sistemas de prevención de intrusiones son útiles para la detección de grandes cantidades de amenazas de nivel inferior, son mucho menos capaces de defenderse de las amenazas cada vez más específicas de la aplicación que habitualmente se utilizan contra las organizaciones de hoy. A pesar de proporcionar una granularidad marcadamente mejorada para controlar el acceso a los recursos de red, los cortafuegos de próxima generación también se quedan cortos en la zona crítica de protección de las propiedades web.

Este white paper describe los desafíos de la defensa adecuada de las modernas propiedades web contra las ciberamenazas y examina los roles que las diferentes tecnologías de seguridad pueden y, quizás más importante todavía, no pueden satisfacer a este respecto. También explica por qué el firewall de aplicaciones web es un componente esencial de la estrategia de protección web de cualquier organización y cómo NetScaler AppFirewall, con su combinación única de seguridad de las aplicaciones y capacidades de optimización del rendimiento de aplicaciones, es la solución ideal para satisfacer esta necesidad.

### El problema de la protección de aplicaciones web

Existen numerosas razones por las que las propiedades web representan un riesgo importante para las organizaciones de hoy. Lo más destacado es la omnipresencia de estas propiedades, el hecho de que se han convertido en el destino elegido por la comunidad "hacker" de hoy y la insuficiente protección que brindan las soluciones de seguridad de la llamada "capa de aplicación".

Las propiedades web están en todos lados

Actualmente, las organizaciones desarrollan y compran aplicaciones web de manera abrumadora. Este es definitivamente el caso de aplicaciones de cara al cliente y sus componentes y cada vez más para aplicaciones móviles y las que se utilizan para activar las funciones y servicios de back-office. Aunque todavía se presta mayor atención a las aplicaciones que generan ingresos, sería imprudente subestimar lo importante que son para el promedio de las empresas, estas otras clases de aplicaciones, incluidas las de gestión de la cadena de suministro, financieras, recursos humanos, investigación y desarrollo de productos.

¿Qué significa esto para los equipos de seguridad de las TI de hoy? Para empezar, como las aplicaciones web son cada vez más utilizadas dentro de una organización por usuarios tanto externos como internos, se necesitan las correspondientes protecciones en algo más que el perímetro de la red.

Otra implicación importante se deriva de la gran diversidad de aplicaciones web que se están implementando en las empresas. Con las innumerables combinaciones de aplicaciones web y a la medida disponibles, es poco realista esperar que las tecnologías de seguridad que utilizan solo las reglas del amplio espectro y mecanismos tales como la detección de anomalías del protocolo de la capa de red, puedan proteger completamente a todas ellas. Los equipos de seguridad también necesitan herramientas que ofrezcan una mayor flexibilidad, mucho más nivel de detalle en la inspección y control e, idealmente, la capacidad de aprender/adaptarse automáticamente a nuevas aplicaciones.

Las propiedades web son "el objetivo preferido" de los hacker

Como si la generalización no fuera suficiente para hacerlas objetivos atractivos para los hacker, las propiedades web son además muy vulnerables. Esta arriesgada situación obedece a varios factores:

- El alto grado de complejidad de muchas propiedades web
- El uso regular de bibliotecas de terceros integradas
- La incorporación rutinaria de (no probados) protocolos, tecnologías y características de vanguardia
- Desarrolladores y administradores de empresas que hacen hincapié en las características y el rápido lanzamiento al mercado en detrimento de los esfuerzos por mejorar la calidad del código y reducir las vulnerabilidades

Ampliando el objetivo sobre sus espaldas, muchas aplicaciones web también sirven como conductos directos a información valiosa o confidencial, como por ejemplo los pagos del cliente y los datos de los pedidos, especificaciones de producto propietario, registros médicos y una gran cantidad de información personal identificable (PII). Una vez que un hacker logra perforar la puerta de acceso fácil de la típica aplicación web pública, es solo cuestión de elegir una o varias de las rutas configuradas asociadas a las bases de datos.

Dadas las circunstancias, no es sorprendente oír hablar sobre importantes violaciones de la web que comprometen millones de registros, o encontrar estadísticas como las del informe sobre la investigación de la violación de datos de Verizon de 2014, que indica que el 35 por ciento de las violaciones confirmadas de datos analizadas en 2013 fueron atribuidas a ataques a la aplicación web. También es importante reconocer que los ataques web que salen a la luz pública representan solo la punta del iceberg. La situación real es considerablemente peor de lo que la mayoría de los responsables pueden esperar, ya que la gran mayoría de ataques web no se consideran de interés periodístico o simplemente no son notificados por la organización afectada.

La protección de servicios en la capa de la aplicación no es suficiente

No puede pasarse por alto la potencial confusión introducida por los esquemas tradicionales de red y su terminología. En particular, aunque se llama "capa de aplicación", la capa 7 del bien conocido modelo de referencia OSI sigue tratando, como todas las otras capas en este modelo, sobre comunicaciones de red. Técnicamente, se refiere a la colección de protocolos y servicios que utilizan las aplicaciones para identificar a los participantes de las comunicaciones, determinar la disponibilidad de los recursos y sincronizar la comunicación entre dos partes usando la misma aplicación. Ejemplos de protocolos de la capa de aplicación incluyen HTTP (para web), FTP (para transferencia de archivos) y SMTP (para correo electrónico).

La confusión se debe a la gran cantidad de tecnologías de seguridad que se comercializan diciendo que proporcionan protección a la "capa de aplicación". Aunque tales afirmaciones pueden ser técnicamente precisas, por ejemplo, cuando un sistema de prevención de intrusión realiza RFC para HTTP, también son, desgraciadamente, algo engañosas. El problema es que la protección proporcionada por estas soluciones se encuentra muy por debajo de la plena cobertura de la "aplicación", ya que solo indirectamente ayuda a fijar la infraestructura de aplicaciones de "capa alta" (p. ej., servidores web y sistemas de administración de bases de datos), aplicaciones comerciales (p. ej., Salesforce.com) y datos que, invariablemente, están presentes también (ver Imagen 1).

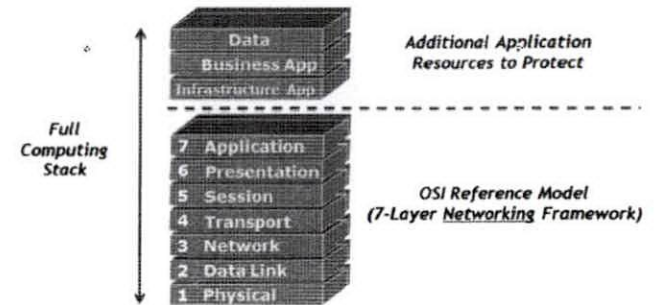


Imagen 1: El modelo informático completo

Para proteger completamente sus importantes propiedades web, las organizaciones necesitan tecnologías de seguridad que ofrezcan una completa:

- Cobertura física que proporcione protección para todos los casos de uso, tanto perimetral como internamente
- Cobertura funcional que proporcione no solo la aplicación de políticas en la forma de control de acceso granular, sino también la detección y prevención de amenazas explícitas
- Cobertura lógica que proporcione protección a través de todas las capas de la cadena informática, desde la red y servicios y protocolos de la capa de aplicación hasta las aplicaciones de infraestructuras, aplicaciones de negocios personalizadas e incluso datos.

El establecimiento de una cobertura como esta requiere invertir en algo más que en cortafuegos de red ordinarios y sistemas de prevención de intrusiones (IPS).

#### Tecnologías de seguridad de red existentes

Las tecnologías de seguridad de red comúnmente desplegadas tienen un papel claro que desempeñar en la defensa de propiedades web empresariales de una organización. Es importante entender, sin embargo, que tienen limitaciones y, ellas solas, no proporcionan un nivel adecuado de protección.

## Firewalls de red

La función principal de un firewall de red ordinario es el control de acceso, vigilar qué tráfico de la aplicación puede ir y venir a través de los límites de la red donde se implementa. Ser verdaderamente operativo conlleva la capacidad de concordar y permitir dinámicamente el tráfico de vuelta correspondiente a las sesiones salientes autorizadas (y viceversa). Sin embargo:

- Como se basa únicamente en los atributos de la capa de red (p. ej., puerto, protocolo y origen/destino de las direcciones IP), la capacidad de control de acceso de un firewall ordinario no es especialmente granular. Como resultado, el firewall no siempre puede distinguir y, por lo tanto, controlar las aplicaciones individuales usando un determinado puerto/protocolo, como por ejemplo la amplia gama de aplicaciones web HTTP que utilizan puerto TCP 80.
- Los firewall de red ordinarios no están equipados para detectar o prevenir explícitamente amenazas. La única protección que ofrecen contra malware, ataques y otras actividades no autorizadas es un subproducto de las políticas de control de acceso que están configuradas para que se cumplan. Por ejemplo, si una amenaza se basa en una vía de comunicación que no está "abierta", se parará por defecto (sin ni siquiera ser detectada).

El resultado neto es que los firewall de red normales proporcionan una protección relativamente limitada para las propiedades web de una organización.

## Sistemas de prevención de intrusiones de red

Ofreciendo normalmente poco en funciones de control de acceso, la tecnología de red IPS se centra en cambio en la detección de amenazas. Los mecanismos de amplio espectro en los que se basa esta tecnología incluyen firmas para amenazas y vulnerabilidades conocidas y detección de anomalías de protocolo y comportamiento para actividades maliciosas sospechosas y amenazas desconocidas. Normalmente se proporciona cobertura hasta incluso la capa de servicios de aplicación y para todos los protocolos comunes de Internet, incluyendo HTTP(s), DNS, SMTP, SSH, Telnet y FTP.

Una cobertura esporádica también está disponible en las capas más altas de la cadena informática, ya que no es infrecuente incluir firmas para vulnerabilidades conocidas y amenazas asociadas con las aplicaciones comerciales y de infraestructura más populares funcionando en las empresas de hoy. A pesar de ser un paso en la dirección correcta, esta cobertura extendida simplemente no es suficiente y deja la tecnología IPS atascada en el medio, sujeta a dos cosas:

- Falsos negativos, como la falta de mayor visibilidad y comprensión de las aplicaciones ocultan la mayoría de amenazas de la capa más alta (como por ejemplo los que trabajan mediante la manipulación de procesos lógicos de la aplicación), y
- Falsos positivos; al intentar escribir firmas ampliamente aplicables que representan una extensa gama de amenazas de la capa más alta en ambas aplicaciones web estándar y personalizadas, invariablemente conduce a innumerables falsas alarmas.

Aunque al proporcionar una detección y prevención de amenazas explícita, la tecnología IPS es un complemento valioso para los firewall de red comunes, la cobertura irregular sobre la capa de servicios de aplicación resulta solo un aumento incremental en la protección de propiedades web de la organización.

## Firewall de próxima generación

El firewall de próxima generación (NGFW) combina las capacidades de cortafuegos de red e IPS en una única solución. A estas capacidades, el NGFW típicamente agrega identidad de usuario y aplicación como atributos para controlar el acceso a/desde una red. Para los casos de uso con todos excepto los requisitos de rendimiento más alto (p. ej., por encima de varios Gbps), el resultado es una solución convenientemente consolidada con unos cuantos accesorios adicionales como buena medida. Sin embargo y relativo a la protección de aplicaciones web, permanece un defecto significativo: el conocimiento de la aplicación. La capacidad para identificar fiablemente aplicaciones independientemente del puerto y protocolo que se utiliza, también conocido como conocimiento de la aplicación, no es lo mismo que tener el dominio de la aplicación.

Con el conocimiento de la aplicación, técnicas como la decodificación del protocolo y las firmas de la aplicación identifican la infraestructura y aplicaciones de negocio específicas responsables de todo el tráfico de red. De este modo el conocimiento de la aplicación permite un control de acceso preciso, donde políticas separadas ahora pueden agruparse cuando múltiples aplicaciones y servicios utilizan los mismos protocolos y puertos. Por ejemplo, el tráfico puede ser analizado por partes para permitir el acceso a un puñado de aplicaciones web útiles y empresariales al restringir selectivamente o completamente bloquear aplicaciones web menos deseables, tales como correo web, servicios de intercambio de archivos y juegos de Facebook.

Como requisito previo para la detección de amenaza explícita en las capas más altas, la fluidez de la aplicación requiere un entendimiento más profundo de la aplicación protegida, incluyendo qué entradas y secuencias de navegación son válidas y cómo la aplicación está pensada para trabajar (versus no trabajar).

La conclusión es que aunque los NGFW ofrecen capacidades de control de acceso mejorado y una oportunidad para eliminar numerosos dispositivos de una sola tecnología, las organizaciones todavía se quedan con las capacidades de detección o protección de amenaza explícita de un IPS ordinario. La amplitud y profundidad de cobertura simplemente no son suficientes para proteger propiedades web, especialmente las personalizadas, de los ataques cada vez más sofisticados y específicos que ahora constituyen una parte importante del paisaje de amenazas.

## El firewall de aplicaciones web, el maestro del dominio de la aplicación

El firewall de aplicaciones web (WAF) comienza donde otras tecnologías de seguridad abandonan, proporcionando protección frente a las amenazas que operan en las más altas capas de la cadena informática. Rutinas de aprendizaje automatizado complementadas con políticas configuradas manualmente dan como resultado una comprensión de alta fidelidad sobre cómo cada aplicación web protegida funciona, incluyendo todas las funciones personalizadas y la lógica del negocio. Desviaciones detectadas posteriormente representan tráfico malicioso sospechoso, que es automáticamente apartado, por ejemplo, bloqueado, permitido con restricciones o registrado, según las políticas definidas por el administrador.

En comparación con las tecnologías de seguridad discutidas anteriormente en este documento, las WAF son únicas en su capacidad para:

- Validar entradas, deteniendo por lo tanto peligrosas inyecciones SQL, cross-site scripting y ataques transversales al directorio
- Detectar ataques a las cookies, a las sesiones o manipulaciones a los parámetros
- Bloquear ataques que explotan vulnerabilidades en propiedades de web personalizadas
- Parar la extracción de datos sensibles a través de la identificación a nivel de objeto y el bloqueo
- Inspeccionar por completo el tráfico cifrado SSL para todos los tipos de amenazas incrustadas
- Prevenir las amenazas que operan mediante la explotación de lagunas de lógica de aplicaciones del negocio personalizadas

- Defendese contra los ataques de denegación de servicio a la capa de aplicación y denegación de servicio distribuido (DDoS)
- Ocultar dinámicamente la información de la respuesta del servidor que sea potencialmente útil para los hackers
- Entregar protecciones XML completas, incluyendo la validación del esquema para mensajes SOAP y defensas de inyección XPath, e identificar y bloquear XML adjuntos que alberguen contenido malicioso
- Permitir el cumplimiento del requisito 6.6 de Payment Card Industry Data Security Standard (PCI DSS)

Sustentar todas estas protecciones centradas en las aplicaciones, WAF líderes del sector, tales como NetScaler AppFirewall, también incluye soporte para las normas de control de acceso de la capa de red y un componente basado en firmas para la detección de amenazas conocidas. Los equipos de seguridad tienen que reconocer, sin embargo, que las defensas de WAF, por diseño, se centran principalmente en protocolos web como HTTP, HTTPS, XML y SOAP.

### Resumen de tecnología de seguridad

El cuadro 1 proporciona una comparativa de las tecnologías de seguridad vistas anteriormente. Los puntos claves son los siguientes:

- Aunque son útiles para la detección de grandes volúmenes de amenazas a la capa baja, la mayoría de las tecnologías de seguridad comúnmente implementadas, firewall de red e IPS, dejan mucho terreno sin cubrir cuando se trata de proteger aplicaciones web
- Aunque ninguna tecnología de seguridad proporciona protección completa para las aplicaciones web, las WAF son las que más se acercan
- Combinar NGFW con WAF es una forma eficaz de crear una protección potente y de amplio espectro contra amenazas para todas las propiedades web empresariales importantes

Comparativa de tecnologías de seguridad para proteger las propiedades web

	Firewall de redes	Sistema de prevención de intrusión	Firewall de próxima generación	Firewall de aplicaciones Web
Funciona en	Capas 3-4	Capas 3-7	Capas 3-7	Capas 3-7+
Arquitectura de despliegue (típica)	Puerta capa 3	Modo transparente	Puerta capa 3	Proxy inverso
Control granular de acceso	Puerto, protocolo, dirección IP	N/C	Puerto, protocolo, dirección IP, usuario, aplicación	Puerto, protocolo, dirección IP
Detección de amenaza/técnicas de prevención	N/C	Firmas, coincidencia de patrones, y detección de anomalías de protocolo y comportamiento	Firmas, coincidencia de patrones, y detección de anomalías de protocolo y comportamiento	Firmas, detección de anomalías en el protocolo, detección de anomalías en aplicaciones específicas
Cobertura del Protocolo	Cualquiera	Cualquiera	Cualquiera	Centrado en la Web (HTTP), XML, SOAP, SPDY
Inspección del tráfico SSL cifrado	N/C	N/C	SI	SI
Protección DDoS	Capa de red (básica)	Capa de red	Capa de red	Capa de aplicación
Protección de aplicaciones Web	Mínima	Conocido/desconocido vulnerabilidades/amenazas principalmente para capas de servicios de red y aplicaciones	Conocido/desconocido vulnerabilidades/amenazas principalmente para capas de servicios de red y aplicaciones	Amplia, incluyendo cobertura completa de la capa de aplicación

### NetScaler AppFirewall

Sus capacidades de protección web únicas hacen del WAF un componente esencial de la arquitectura de seguridad de la organización y elevan la importancia de seleccionar una solución de características completas.

NetScaler Application Firewall es una solución de seguridad de aplicaciones web integral certificada por ICSA que bloquea ataques conocidos y desconocidos contra la web y aplicaciones de servicios web. Empleando un modelo de seguridad híbrido y analizando todo el tráfico bidireccional, incluyendo las comunicaciones cifradas SSL, Application firewall contrarresta una amplia gama de amenazas a la seguridad sin que se requieran modificaciones en las aplicaciones.

Las siguientes son características claves de protección de NetScaler AppFirewall:

**Modelo híbrido de seguridad.** Para derrotar ataques nuevos y desconocidos, un motor de políticas de modelo positivo que entiende las interacciones de aplicaciones de usuario permitidas bloquea automáticamente todo el tráfico que queda fuera de este ámbito. Como complemento, un motor de modelo negativo utiliza firmas de ataques para protegerse de las amenazas conocidas contra las aplicaciones.

**Protección de XML.** NetScaler AppFirewall no solo bloquea las amenazas comunes que se pueden adaptar para atacar aplicaciones basadas en XML (p. ej., cross-site scripting, comandos de inyección), también incorpora un conjunto de protecciones específicas de XML, incluyendo el esquema integral de validación y la capacidad para frustrar los ataques relacionados con la capa de aplicación (p. ej., excesiva repetición).

**Protección avanzada para elementos dinámicos.** Múltiples protecciones de sesión aseguran los elementos dinámicos de la aplicación tales como cookies, campos de formulario y los URL específicos de sesión, de modo que frustran los ataques que apuntan a la relación de confianza entre cliente y servidor (p. ej., falsificación de solicitud entre sitios).

**Políticas de seguridad adaptadas.** Un avanzado motor de aprendizaje determina automáticamente el comportamiento esperado de las aplicaciones web empresariales y genera políticas recomendadas legibles por el ser humano. Los administradores pueden personalizar la política de seguridad según las necesidades específicas de cada aplicación y evitar potenciales eventos falsos positivos.

**Conformidad garantizada.** NetScaler AppFirewall permite a las empresas cumplir con los mandatos de seguridad de datos tales como PCI DSS, fomentando explícitamente el uso de WAF para aplicaciones de cara al público que manejan información de tarjetas de crédito. Se pueden generar informes detallados para documentar todas las protecciones definidas en el firewall que corresponden a mandatos PCI.

**No compromete el rendimiento.** La solución de seguridad con más alto rendimiento en aplicaciones web del sector ofrece hasta 12+ Gbps de protección completa sin degradar los tiempos de respuesta de la aplicación.

Para más distinción NetScaler AppFirewall es el único capaz de implementarse como un componente integral de la plataforma NetScaler completa de entrega de aplicaciones. Los beneficios de este enfoque incluyen aumentos sustanciales en el rendimiento de las aplicaciones web (debido a la aceleración avanzada y capacidades de descarga de servidor) y fiabilidad (debido al balanceo de carga de servidor, supervisión de la salud del servidor y capacidades de failover). El resultado neto es una solución ideal que ofrece una protección web incomparable junto con una experiencia de aplicación de alta definición para las exigencias de los usuarios de hoy.

### Conclusión

En el pasado, los firewall de red ordinarios y los sistemas de prevención de intrusiones habrían abordado la protección adecuada para el puñado de aplicaciones web que la organización estándar consideraba importantes. En la actualidad la mayor dependencia de las propiedades web y el cambio radical por parte de los piratas informáticos hacia los ataques específicos a la aplicación, esto ya no es posible. Incluso la próxima generación de firewalls se quedan cortos, ya que las mejoras que ofrecen son principalmente en la consolidación de la infraestructura y una mayor granularidad para establecer y aplicar políticas de control de acceso.

Para proteger totalmente las numerosas propiedades web internas y externas de su organización, los equipos de seguridad deben complementar estas otras contramedidas, que son todavía útiles para la filtración de grandes volúmenes de amenazas de nivel inferior, con una solución de firewall de aplicación web. Manteniendo una profunda comprensión de cómo cada aplicación protegida funciona normalmente y buscando actividades anómalas e información más allá de la capa de aplicación de servicios/protocolo, los WAF completos tales como NetScaler AppFirewall ofrecen un grado de protección frente a amenazas no disponibles en otras tecnologías de seguridad comúnmente desplegadas, heredadas y de otro tipo.

**Sede central corporativa**  
Fort Lauderdale, FL (EE. UU.)

**Sede central de Silicon Valley**  
Santa Clara, CA (EE. UU.)

**Sede central de EMEA**  
Schaffhausen (Suiza)

**Centro de Desarrollo de la India**  
Bangalore (India)

**Sede central de la División Online**  
Santa Bárbara, CA (EE. UU.)

**Sede central del Pacífico**  
Hong Kong (China)

**Sede central de América Latina**  
Coral Gables, FL (EE. UU.)

**Centro de Desarrollo del Reino Unido**  
Chalfont (Reino Unido)

#### Acerca de Citrix

Citrix (NASDAQ:CTXS) Citrix (NASDAQ:CTXS) está liderando la transición hacia soluciones de software que definen el lugar de trabajo, reuniendo virtualización, gestión de la movilidad, networking y SaaS habilitando nuevas formas para que las empresas y personas trabajen mejor. Las soluciones de Citrix impulsan la movilidad empresarial a través de espacios de trabajo móvil seguros y personales que proporcionan a los usuarios un acceso instantáneo a las aplicaciones, puestos de trabajo, datos y comunicaciones en cualquier dispositivo sobre cualquier red y cloud. Con unos ingresos anuales de 3140 millones de dólares en 2014, las soluciones de Citrix son utilizadas en más de 330 000 organizaciones y por más de 100 millones de personas en todo el mundo. Más información en [www.citrix.es](http://www.citrix.es)

Copyright © 2015 Citrix Systems, Inc. Todos los derechos reservados. Citrix, NetScaler y NetScaler AppFirewall son marcas comerciales de Citrix Systems, Inc. o una de sus subsidiarias y pueden estar registradas en los Estados Unidos y otros países. Otros nombres de productos y compañías mencionados aquí pueden ser marcas comerciales de sus respectivas empresas.

MULTICORPUS<sup>®</sup> S.P.A.  
optimiza el futuro juntos  
Santo Domingo, R.D.  
0715/PDF/1024

Free