República Dominicana
Procuraduría General de la República
Especificaciones Técnicas de Bienes y Servicios Tecnológicos

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS (A)		CUMPLE (B)
Interfaces & Módulos	➢ 10 GE SFP + slots - 2 ➢ GE RJ45 - 8 ➢ GE SFP Slots - 8 ➢ RJ45 Puertos administración - 2 ➢ USB - 2 ➢ RJ45 puerto de consola - 1		
	Local Storage	2 X 240GB SSD	
Rendimiento del sistema	➢ IPS 7.9 Gbps ➢ NGFW 5 Gbps ➢ Protección contra amenazas 4.7 Gbps		

INFORMACIÓN GENERAL

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

Rendimiento y capacidad del sistema	✓ IPv4 Firewall rendimiento (1518/512/64 byte, UDP) 36/36/22 Gbps ✓ IPv6 Firewall rendimiento (1518 / 512 /64 byte UDP) 36/36/22 Gbps ✓ Latencia Firewall (64 bytes, UDP) 2 ✓ Rendimiento paquetes 33Mbps ✓ Sesiones TCP 8 millones ✓ Nuevas Sesiones/seg (TCP) 300,000 ✓ Firewall Policies 10,000 ✓ IPsec VPN rendimiento (512 byte) 1 20 Gbps ✓ Gateway-to-Gateway IPsec VPN Tunnels 2,000 ✓ Client-to-Gateway IPsec VPN Tunnels 50,000 ✓ SSL-VPN Throughput 5 Gbps ✓ Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) 10,000 ✓ SSL Inspection Throughput (IPS, avg. HTTPS) 3 5.7 Gbps ✓ SSL Inspection CPS (IPS, avg. HTTPS) 3 3,500 ✓ SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 800,000 ✓ Application Control Throughput (HTTP 64K) 2 14 Gbps ✓ CAPWAP Throughput (1444 byte, UDP) 18 Gbps ✓ Configurations Active-Active, Active-Passive, Clustering Características Generales ✓ La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo; ✓ Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos; ✓ Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación; ✓ La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7; ✓ Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;	

INFORMACIÓN GENERAL

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ La gestión del equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red; ✓ Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q; ✓ Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP; ✓ Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; ✓ Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM); ✓ Los dispositivos de protección de red deben soportar DHCP Relay; ✓ Los dispositivos de protección de red deben soportar DHCP Server; ✓ Los dispositivos de protección de red deben soportar sFlow; ✓ Los dispositivos de protección de red deben soportar Jumbo Frames; ✓ Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas; ✓ Debe ser compatible con NAT dinámica (varios-a-1); ✓ Debe ser compatible con NAT dinámica (muchos-a-muchos); ✓ Debe soportar NAT estática (1-a-1);	

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
DTIC
4/12/19

Información General

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ Debe admitir NAT estática (muchos-a-muchos); ✓ Debe ser compatible con NAT estático bidireccional 1-a-1; ✓ Debe ser compatible con la traducción de puertos (PAT); ✓ Debe ser compatible con NAT Origen; ✓ Debe ser compatible con NAT de destino; ✓ Debe soportar NAT de origen y NAT de destino de forma simultánea; ✓ Debe soportar NAT de origen y NAT de destino en la misma política ✓ Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico; ✓ Debe ser compatible con NAT64 y NAT46; ✓ Debe implementar el protocolo ECMP; ✓ Debe soportar SD-WAN de forma nativa ✓ Debe soportar el balanceo de enlace hash por IP de origen; ✓ Debe soportar el balanceo de enlace por hash de IP de origen y destino; ✓ Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;	

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales; ✓ Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red; ✓ Enviar logs a sistemas de gestión externos simultáneamente; ✓ Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL; ✓ Debe soporta protección contra la suplantación de identidad (anti-spoofing); ✓ Implementar la optimización del tráfico entre dos dispositivos; ✓ Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); ✓ Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); ✓ Soportar OSPF graceful restart; ✓ Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red; ✓ Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico; ✓ Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico; ✓ Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	

Información General

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;
- ✓ Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;
- ✓ Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;
- ✓ La configuración de alta disponibilidad debe sincronizar: Sesiones;
- ✓ La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;
- ✓ La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
- ✓ La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
- ✓ En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;
- ✓ Debe soportar la creación de sistemas virtuales en el mismo equipo;
- ✓ Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;
- ✓ Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

- ✓ Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

- ✓ Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;

- ✓ El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;

- ✓ Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;

- ✓ La consola de administración debe soportar como minimo, ingles, Español y Portugues.

- ✓ La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad

- ✓ La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.

Control por Política de Firewall

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ Debe soportar controles de zona de seguridad; ✓ Debe contar con políticas de control por puerto y protocolo; ✓ Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones; ✓ Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad; ✓ Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad; ✓ Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall; ✓ Debe soportar automatización de situaciones como deteción de equipos comprometidos, estado del sistema, cambios de onfiguración, eventos especificos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. ✓ Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF); ✓ Debe soportar integración de nubes publicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes ✓ Debe soportar el protocolo estándar de la industria VXLAN; ✓ La solución debe permitir la implementación sin asistencia de SD-WAN	

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por politicas, IPSEC VPN; ✓ la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electronico, cache y Web application firewall. Control de Aplicación ✓ Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo; ✓ Detección de miles de aplicaciones en 18 categorias, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico; ✓ Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs; ✓ Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor; ✓ Para trafico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	

Información General

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;
- ✓ Actualización de la base de firmas de la aplicación de forma automática;
- ✓ Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por politica de usuarios y grupos;
- ✓ Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;
- ✓ Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;
- ✓ El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;
- ✓ Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;
- ✓ Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

- ✓ Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

- ✓ Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);

- ✓ Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;

- ✓ Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicació

- ✓ Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Prevención de Amenazas

- ✓ Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

- ✓ Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

- ✓ Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante; ✓ Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad; ✓ Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos; ✓ Deber permitir el bloqueo de vulnerabilidades y exploits conocidos ✓ Debe incluir la protección contra ataques de denegación de servicio; ✓ Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo; ✓ Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo; ✓ Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP; ✓ Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP; ✓ Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets); ✓ Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	

Información General

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ Detectar y bloquear los escaneos de puertos de origen;
- ✓ Bloquear ataques realizados por gusanos (worms) conocidos;
- ✓ Contar con firmas específicas para la mitigación de ataques DoS y DDoS;
- ✓ Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);
- ✓ Debe poder crear firmas personalizadas en la interfaz gráfica del producto;
- ✓ Identificar y bloquear la comunicación con redes de bots;
- ✓ Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;
- ✓ Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;
- ✓ Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;
- ✓ Los eventos deben identificar el país que origino la amenaza;

DTIC 11/12/19

Información General	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

- ✓ Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);
- ✓ Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;
- ✓ Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;
- ✓ En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;
- ✓ Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

Filtrado de URL

- ✓ Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);
- ✓ Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;
- ✓ Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;
- ✓ Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación

INFORMACIÓN GENERAL

Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

de direcciones URL;

- ✓ Tener por lo menos 75 categorías de URL;
- ✓ Debe tener la funcionalidad de exclusión de URLs por categoría;
- ✓ Permitir página de bloqueo personalizada;
- ✓ Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);
- ✓ Además del Explicit Web Proxy, soportar proxy web transparente;

Identificación de Usuarios

- ✓ Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
- ✓ Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;
- ✓ Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

PROCURADURÍA GENERAL DE LA REPÚBLICA
Dirección de Tecnología de la Información
DTIC
11/12/19

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios; ✓ Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la políticas/control basados en usuarios y grupos de usuarios; ✓ Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo); ✓ Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios; ✓ Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD; ✓ Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma; **QoS Traffic Shaping** ✓ Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;	

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	✓ Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen; ✓ Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino; ✓ Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo; ✓ Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube; ✓ Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto; ✓ En QoS debe permitir la definición de tráfico con ancho de banda garantizado; ✓ En QoS debe permitir la definición de tráfico con máximo ancho de banda; ✓ En QoS debe permitir la definición de colas de prioridad; ✓ Soportar marcación de paquetes DiffServ, incluso por aplicación; ✓ Soportar la modificación de los valores de DSCP para Diffserv; ✓ Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	

República Dominicana
Procuraduría General de la República
Especificaciones Técnicas de Bienes y Servicios Tecnológicos

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

	CARACTERÍSTICAS TÉCNICAS MÍNIMAS REQUERIDAS (A)	CUMPLE (B)
	✓ Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	
Garantía	1 año en partes y Servicio	

INFORMACIÓN DEL OFERENTE(C)	
Nombre de la Empresa	
Fecha de la propuesta	

Firma del Vendedor | Sello de la Empresa

República Dominicana
Procuraduría General de la República
Especificaciones Técnicas de Bienes y Servicios Tecnológicos

INFORMACIÓN GENERAL	
Bien o Servicio a adquirir	**Clúster Firewall**
Fecha de Vigencia	
Referencia	

INSTRUCCIONES

EN LA SECCIÓN (A) SE MUESTRA LAS CARACTERÍSTICAS O REQUISITOS MÍNIMOS SOLICITADOS PARA EL BIEN O SERVICIO
EN LA SECCIÓN (B) EL OFERENTE DEBERÁ MARCAR CON UNA X LAS CARACTERÍSTICAS CON LAS QUE CUENTA EL BIEN O SERVICIO OFERTADO
EN LA SECCIÓN (C) EL OFERENTE REGISTRARÁ EL NOMBRE DE LA EMPRESA Y LA FECHA EN LA QUE PRESENTA LA OFERTA, ASÍ MISMO DEBERÁ FIRMAR Y SELLAR AMBAS PÁGINAS.

NOTA: PARA QUE PUEDA SER EVALUADA SU PROPUESTA DEBERÁ PRESENTAR ESTE FORMULARIO DEBIDAMENTE COMPLETADO Y ANEXARLE LA COTIZACIÓN CORRESPONDIENTE.