Pedido de cotización para el expediente N°: 31325

PROV, INST Y SOP SIST SEGURIDAD FIREWALL

Licitación Pública 572

Apertura: 26/01/2021 Hora: 11:30

1) DEBERÁ FIRMAR Y ACLARAR TODAS LAS HOJAS QUE CONFORMAN LA OFERTA ECONÓMICA, INCLUIDA LA PRESENTE. NO SERÁ NECESARIO ACOMPAÑAR LAS CLAUSULAS GENERALES DEL PLIEGO, TODA VEZ QUE LA PRESENTACIÓN DE LA OFERTA IMPLICA LA ACEPTACIÓN TOTAL Y LA ABSOLUTA CONFORMIDAD CON EL CONTENIDO DEL PLIEGO

2) DEBERÁ COMPLETAR TODOS LOS CAMPOS EN BLANCO EN EL CUADRO A CONTINUACIÓN:

a. Si ofrece CANTIDAD distinta a la solicitada, tachar e indicar.
b. FECHA DE ENTREGA : Si no se indica, se requiere en forma inmediata a la emisión de la Orden de Compra.
c. MARCA / MODELO / PROCEDENCIA deberá indicarse solamente para bienes.
d. Deberá indicar la moneda de cotización. Se admitirán ofertas en moneda extranjera.

PROVEEDOR (NOMBRE O RAZÓN SOCIAL) :

R	R/C	Cod. Artículo	Descripción	Unidad	Cantidad	Exc.	Fecha Entrega	Marca/Modelo /Procedencia	Precio Unit. sin IVA	Subtotal	Alícuota IVA
1)	369471	55047287	SOLUCION DE SEGURIDAD FIREWALLS PRINCIPAL DE ULTIMA TECNOLOGIA, DISEÑADA ESPECIFICAMENTE PARA RESPONDER DE FORMA RAPIDA Y EFICIENTE A LA CRECIENTE TENDENCIA EN CIBER-ATAQUESL. INTERFACE: 2 X 10GE SFP + SLOTS, 10 X GE RJ45 PORTS (INCLUDING 1 X MGMT PORT, 1 X HA PORT, 8 X SWITCH PORTS), 8 X GE SFP SLOTS, SPU NP6 Y CP9 HARDWARE ACCELERATED	Pieza	2	0					
2)	369472	55047295	SOLUCION DE SEGURIDAD FIREWALLS SECUNDARIO DE ULTIMA TECNOLOGIA, DISEÑADA ESPECIFICAMENTE PARA REPLICAR LAS POLITICAS DEFINIDAS EN EL FIREWALL PRINCIPAL Y RESPONDER DE FORMA RAPIDA Y EFICENTE A LA CRECIENTE TENDENCIA EN CIBER-ATAQUES. INTERFACE: 18 X GE RJ45 (INCLUDING 2 X WAN PORTS, 1 X MGMT PORT, 14 X SWITCH), 4 X GE SFP SLOTS. SPU NP6LITE Y CP9 HARDWARE ACCELERATED.	Pieza	2	0					

Lic. LORENA RUIZ IBAÑEZ
JEFA DE SECCION
COMPRAS NACIONALES
S.E. CASA DE MONEDA

Dra. ANDREA LAPADULA
Gerente de Compras
S.E. CASA DE MONEDA

lunes, 04 de enero de 2021

Firma y sello del oferente

Pedido de cotización para el expediente N°: 31325

PROV, INST Y SOP SIST SEGURIDAD FIREWALL

Licitación Pública 572

Apertura: 26/01/2021 Hora: 11:30

3)	369473	55047309	ANTENAS WI-FI (ACCES POINT) QUE PERMITEN EL INGRESO A LA RED DE LAN COMO A LA RED WN, INTERFACES: INDOOR WIRELESS AP-DUAL, RADIO: 802.11 B/G/N/AC WAVE 2,2 X 2 MU-MIMO, INTERNAL ANTENNAS, 1 X 10/100/1000 RJ45 PORT, BT/BLE. CEILING /WALL MOUNT KIT INCLUDED. FOR POWER ORDER: 802.3AF P0E INJECTOR GPI-115 OR AC ADAPTER SP-FAP200-PA. REGION CODE A.	Pieza	80	0				

SUBTOTAL SIN IVA _____

MONTO IVA (SI CORRESPONDE, DE LO CONTRARIO, TACHAR) _____

TOTAL _____

Dra. ANDREA LAPADULA
Gerente de Compras
S.E CASA DE MONEDA

lunes, 04 de enero de 2021

Firma y sello del oferente

3) RESUMEN DEL PLIEGO DE BASES Y CONDICIONES

a. Es condición de validez de la oferta acompañar Garantía de Mantenimiento de Oferta (según detalle en Cláusulas Particulares).
b. Deberá cumplir con lo requerido en las Especificaciones Técnicas (puede contener condiciones de validez de la oferta).
c. La presente contratación se encuentra alcanzada por sus Cláusulas Generales y Cláusulas Particulares.
d. Deberá completar el Formulario del Decreto 202/2017 adjunto, con una vigencia de 1 año, por lo que se eximirá de presentarlo quien lo haya hecho dentro de ese plazo, excepto que hayan cambiado los datos suministrados, en cuyo caso deberá actualizarlos.
e. Deberá completar el Modelo de Carta de Presentación.
f. Deberá acompañar la documentación solicitada en Aspectos Legales. Se tendrá por cumplida si la misma hubiese sido debidamente presentada con anterioridad; siempre y cuando se encontrare vigente y actualizada.
g. Deberá acompañar la documentación solicitada en Aspectos Económicos/Financieros.
h. Deberá acompañar la documentación solicitada en Aspectos Técnicos.
i. La oferta deberá ser presentada en sobre cerrado (según detalle en Cláusulas Particulares).

REQUISITOS COMPLEMENTARIOS

LA PROVISION INCLUYE INSTALACION Y PUESTA EN MARCHA EN LA MODALIDAD "LLAVE EN MANO".

TODOS LOS RENGLONES SE ADJUDICARAN A UN SOLO PROVEEDOR.

DEBERÁN REALIZAR UNA VISITA DE OBRA SEGÚN LO ESTABLECIDO EN EL PUNTO XIII VISITA DE OBRA DE LAS ESPECIFICACIONES TECNICAS.

INFORMACIÓN PARA EL CASO DE RESULTAR ADJUDICATARIO:

Lugar de entrega:Ambas plantas. -

Condición de pago según lo establecido en Cláusulas Generales

Deberá abonar el impuesto a los sellos sobre el valor neto de la orden, a la alícuota del 1% y soportarlo a su cargo, presentando fotocopia del pago junto con el original como condición de pago de facturas.

Lic. LORENA RUIZ IBAÑEZ
JEFA DE SECCION
COMPRAS NACIONALES
S.E. CASA DE MONEDA

Dra. ANDREA LAPADULA
Gerente de Compras
S.E. CASA DE MONEDA

Firma y sello del oferente

A los efectos de realizar el pago, deberá emitir Factura Electrónica en la misma unidad de medida y moneda establecida por Renglón en la Orden de Compra.

A los efectos de poder generar las conformidades para el pago, deberá indefectiblemente presentar en Mesa de Entradas remito del servicio/producto contratado a nombre de administración de Almacenes.

Deberá dar cumplimiento a lo establecido en el Anexo Provisión y/o Servicios que se efectúen en el ámbito de la SECM

S. E. CASA DE MONEDA

PLIEGO DE ESPECIFICACIONES TECNICAS Y PARTICULARES

Firewall + AP

S. E. CASA DE MONEDA

Contenido

OBJETO

Este pliego tiene por objeto establecer los requisitos mínimos y lineamientos para la provisión, instalación y soporte de un sistema de seguridad (Next Generation Firewall) con capacidad para implementar gestión unificadas de amenazas (UTM) destinado a controlar el tráfico cursado desde y hacia las redes externas a la institución junto con la gestión de conectividad inalámbrica. Se deberán proveer (4) Firewalls de Próxima Generación y 80 antenas.

De lo solicitado dos (2) firewalls serán instalados en la Sede de Retiro y otros dos (2) en la Sede Don Torcuato, en cuanto a las antenas ser instaladas 60 en la Sede de Retiro y 20 en la Sede Don Torcuato.

CONDICIONES GENERALES

CONSIDERACIONES Y REQUERIMIENTOS GENERALES

1.1. Todos los requerimientos técnicos de los equipos y software objeto de este pliego, deben ser considerados mínimos, pudiendo el Oferente presentar ofertas cuyas características superen o mejoren las aquí solicitadas.

1.2. Todas las facilidades solicitadas para los equipos y software, incluidas las ampliaciones y capacidades de expansión, deberán estar disponibles a la fecha de apertura de la presente licitación. Se considera "estar disponible" el haber sido liberado al mercado mundial en forma oficial por la empresa fabricante del equipo o desarrolladora del software.

1.3. No se aceptarán (serán consideradas como no presentadas) facilidades y/o expansiones no soportadas por la versión actual del software y hardware (la vigente a la fecha de apertura de la presente licitación).

1.4. Se proveerán todos los cables necesarios para las interconexiones de los equipos.

1.5. Todos los equipos deberán operar con una alimentación 220 VCA 50Hz, monofásico con conectores C13-C14 o C19-C20 sin el uso de transformadores externos. Como máximo los equipos firewall ocuparán 1 unidad de Rack de altura.

1.6. Todos los requerimientos técnicos y funcionalidades esperadas de acuerdo a lo solicitado en el presente pliego, deben operar tanto en forma independiente unas de otras como en forma totalmente integrada y/o simultánea, sin limitación alguna.

1.7. Los elementos, unidades funcionales, dispositivos y accesorios estarán constituidos por unidades nuevas, sin uso previo y en perfecto estado de conservación y funcionamiento (se entiende por nuevo y sin uso, a que S.E. Casa de Moneda será el primer usuario de los equipos desde que estos salieron de fábrica).

1.8. Todos los sistemas ofrecidos deberán cumplir con las especificaciones en materia de regulación de seguridad eléctrica, emisión de radiofrecuencia, emisión electromagnética y emisión de radiación, emitidas por los organismos competentes.

1.9 Todos los equipos a proveer de un mismo tipo (Equipos que poseen las mismas características técnicas y funcionales, y están destinados a satisfacer una misma necesidad según la especificación particular de cada uno dada en el documento de licitación) deberán ser del mismo modelo.

1.10 Los equipos a proveer deberán estar vigentes y no poseer fecha de discontinuidad de fabricación a la fecha de presentación de la oferta.

1.11 Todos los appliances a proveer deberán operar con corriente alterna de 220 V, 50 Hz, con conexión a tierra, sin posibilidad de conmutar manualmente a otro voltaje/frecuencia.

1.12 Todos los equipos ofrecidos deberán operar en rangos de temperatura ambiente desde 0 a 40 grados centígrados, sin necesidad de acondicionamiento especial.

1.13 Todo el equipamiento deberá entregarse con todos los accesorios necesarios para su correcta instalación y funcionamiento, entiéndase por esto fuentes de alimentación, cables de conexión, y drivers de software.

CONDICIONES DE LAS OFERTAS

Los oferentes deberán presentar en su oferta: folletos, documentación técnica, manual de especificaciones y facilidades del equipamiento ofrecido. No se admitirá especificar simplemente "según pliego" como identificación del equipamiento ofrecido.

La contestación a los puntos del pliego deberá hacerse punto por punto en castellano indicando en qué parte de la documentación presentada se especifica el cumplimiento de los mismos.

La instalación de los equipos ofrecidos será realizada por la Adjudicataria. Los detalles de la instalación deberán ser detallados claramente en ítem separado.

S. E. CASA DE MONEDA

CARACTERISTICAS GENERALES DEL EQUIPAMIENTO

El equipamiento deberá poseer como mínimo las siguientes características técnicas de las prestaciones requeridas:
Poseerá compatibilidad con todos y cada uno de los siguientes estándares:
Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigabit Ethernet IEEE 802.3ae.

Los cuatro equipos deberán poder operar en alta disponibilidad, en modalidad activo-activo y activo-pasivo. Cada uno de los equipos deberá tener la posibilidad de agregado de fuentes redundantes del tipo hot swap. El sistema deberá poder operar en modo Router (permitiendo el envío de paquetes en L2 y L3) como así también en modo transparente.

Deberá permitir la creación de al menos 10 sistemas virtuales dentro del mismo equipo, sin necesidad de hardware o licencias adicionales. Cada sistema virtual podrá operar en modo Router o Transparente sin limitaciones en forma simultánea sobre cada sistema virtual.

El sistema deberá permitir la definición de interfaces virtuales (VLANs) las que podrán estar asignadas a diferentes interfaces físicas en diferentes sistemas virtuales. Deberá soportar el etiquetado de los paquetes según IEEE 802.1Q utilizando cualquier ID (1-4095). Asimismo, deberá contar con soporte de VXLAN.

El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de otros productos, servicios o herramientas de gestión centralizadas.

Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino/origen, puerto destino/origen y geolocalización utilizando rangos horarios.

El dispositivo deberá soportar al menos la generación de 10.000 políticas de firewall.

El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT en forma simultánea sobre una misma conexión.

Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales, que no sean las propias IP declaradas en las interfaces del firewall.

Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores, redes, direcciones basadas en ubicación geográfica y servicios como mínimo.

Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.

El equipo deberá permitir la implementación de políticas de calidad de servicio y Traffic Shaping soportando al menos:

- Puertos físicos e interfaces agregadas o redundantes.
- Políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo.
- La definición de tráfico con ancho de banda garantizado.
- La definición de tráfico con máximo ancho de banda.
- La definición de colas de prioridad.
- La priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- El etiquetado de paquetes DiffServ, incluso por aplicación.
- La modificación de los valores de DSCP para Diffserv.
- La priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).

El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).

Cada Firewall deberá además soportar las siguientes funcionalidades:

- Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser totalmente compatible con Active Directory.
- Soporte de IPSec NAT Traversal.

El equipo deberá permitir la terminación de túneles VPN.
El Firewall deberá soportar túneles utilizando protocolo IPSEC estándar o a través de SSL. Para el caso de VPNs SSL, el equipo debe soportar que el usuario pueda realizar la conexión a través de un cliente VPN instalado en el sistema operativo de su máquina o a través de una interface web.

El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar el throughput requerido medido con tráfico real con las siguientes funcionalidades habilitadas simultáneamente:
Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor

nivel de seguridad posible; considerando múltiples políticas de seguridad y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.

El Control de Amenazas avanzadas (Sandboxing) deberá ser provisto en la solución. El mismo deberá estar disponible durante el período de garantía.

El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS, detección de anomalías y anti-malware para los protocolos soportados.

- Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas.
- Deberá permitir armar firmas propias de IPS.
- Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía.
- Deberá poseer una base de conocimiento que detalle la definición de la regla.
- Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico.
- Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas.
- El motor de IPS deberá soportar el agregado de firmas específicas para ambientes industriales a los fines de interpretar los protocolos específicos de esos ambientes.

El Firewall deberá identificar potenciales vulnerabilidades y sugerir las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución. La información podrá brindarse mediante la GUI o vía reportes.

El Firewall deberá funcionar como proxy web explícito (validación en Active Directory o por medio del protocolo LDAP) y como proxy transparente.

El Firewall deberá incorporar funcionalidades para SD-WAN. Si fuese necesario el agregado de licencias adicionales indicar cómo se aplican las mismas.

Capacidades de SD-WAN a soportar en el firewall:

- Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS)
- Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame.
- Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas.
- Soporte a más de 5 vínculos a Internet.
- Debe contar con un mecanismo por el cual se puedan recuperar los datos enviados sin necesidad de recurrir a las retransmisiones de protocolo TCP y que permita la reconstrucción del stream en el lado receptor.

El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de Servicio).

Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.

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.

Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.

Deberá tener la funcionalidad de filtrado de contenidos Web.

- Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos.
- Deberá permitir el 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).
- Deberá permitir la actualización automática de la base de filtrado de contenidos durante el transcurso del período de garantía.
- Deberá soportar al menos sesenta (60) categorías en la base de filtrado.
- Deberá tener la funcionalidad para detectar aplicaciones. Para ello el equipo deberá:
  - Inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas, independiente de puerto y protocolo que utilicen.
  - Deberá reconocer al menos 3000 aplicaciones diferentes, permitiendo agrupar las mismas en al menos 16 categorías y aplicar políticas de seguridad a las mismas.
  - Debe permitir la creación de firmas de aplicación manuales.
- Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo.
- Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo.
- Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.

Deberá soportar la inspección de sesiones que atraviesan el firewall y utilizan el protocolo SSL (Secure Sockets Layer) para encriptación, incluyendo el protocolo HTTPS.

El equipo deberá proveerse con los servicios de actualización de firmas para los motores de filtrado descriptos en los puntos anteriormente mencionados por el término de 12 meses.

S. E. CASA DE MONEDA

Debe permitir la administración del equipo por medio de los protocolos HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.

Deberá permitir el registro local y remoto de eventos utilizando servidores syslog.

Controlador de puntos de conexión inalámbricos o WIFI. Dicha función deberá estar integrada dentro de la solución de firewall requerida.

En el caso de requerir una licencia específica para la funcionalidad de Controlador WIFI especificarlo.

Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador.

La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor.

El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS.

La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario.

Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points.

El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tuneleados hasta el controlador inalámbrico.

Cuando tuneleado, el tráfico debe ser encriptado a través de DTLS o IPSEC.

Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico.

Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica.

La solución debe permitir definir qué redes serán tuneleadas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso.

La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tuneleados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso.

La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso.

La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados.

La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación.

La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio de interfaz de origen el SSID de la red WIFI.

La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos.

Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID.

Debe implementar la autenticación administrativa a través del protocolo RADIUS.

En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES).

En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3.

La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado.

Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada.

La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS.

La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X.

La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP.

La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red.

La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico.

La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes.

La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red.

La solución debe permitir que la página de autenticación se quede alojada en un servidor externo.

La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada.

La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6.

La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución.

Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado.

La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes.

La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica.

La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible.

La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog.

La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps.

La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP.

La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB).

La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos.

La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal.

La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado.

La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios.

La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming.

La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia.

La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectado mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos.

La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica.

La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado.

La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz.

La solución provista debe tener la capacidad de hacer Reporting, Análisis y guardar logs. Esta solución deberá ser de la misma marca que los equipos propuestos.

- Deberá poder ser desplegado como una Máquina Virtual (VM) sobre infraestructura KVM o VMWare.
- El sistema deberá analizar los registros provenientes de múltiples dispositivos, por usuario o por grupo de usuarios
- Deberá generar una variedad de reportes que permiten a los administradores de red asegurar las redes de manera proactiva conforme se presentan las amenazas, evitando los abusos de red.
- El sistema deberá permitir la visualización de registros o cualquier mensaje o archivo de registro desde los dispositivos registrados. Deberá implementar filtros que permitan navegar sobre los registros de forma simple y amigable.
- El sistema deberá implementar reportes que permitan a los administradores conocer al menos:
- Ataques: por unidad, por hora del día, por categoría, y por fuentes de los ataques.
- Virus: principales virus detectados en la red y detectados por Protocolo.
- Eventos: Por Firewall, eventos en general, eventos de seguridad desencadenados y eventos desencadenados por el día de la semana.
- Utilización de la Red: Principales usuarios de la Red y principales clientes intentando acceder a sitios bloqueados.
- Ancho de banda: Principales usuarios de ancho de banda.

Ancho de banda por día, por hora y utilización de ancho de banda por familia de protocolos.

- Protocolos: los principales protocolos utilizados, usuarios FTP y usuarios de Telnet.
- El sistema deberá implementar análisis forenses de forma que se pueda rastrear las actividades de un usuario.
- El sistema deberá ser administrable vía Web utilizando HTTPs.

Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse.

- El sistema deberá soportar al menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only).
- Debe contar con reporte de AP´s y SSID´s autorizados, así como clientes WIFi.

La solución provista deberá contar con el espacio para el almacenamiento permanente de los logs y espacio para el guardado de los logs diarios que se utilizarán para la Analítica.

Debe soportar servicio de Indicadores de Compromiso del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.

La solución provista deberá tener no menos de 3 TB de Almacenamiento permanente de logs y 6 Gbps para Analítica de logs diarios.

iV: ESPECIFICACIONES PARTICULARES

iV.a) Firewall de Próxima Generación Sede Retiro. Cantidad 2

Número de Interfaces Requeridas	8x GE RJ45 8x GE SFP (Bahias) 2x GE SFP+ (Bahias) 2 x GE RJ45 Puertos administrativos
Throughput de Firewall (con paquetes de 512 Bytes)	36 Gbps
Latencia de firewall (con paquetes de 64 byte)	2 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	20 Gbps
Throughput de NGFW	9 Gbps
Throughput de Inspección SSL	8 Gbps
Políticas de Firewall admitidas	10.000
Túneles IPsec gateway to gateway	2.000
Túneles IPsec client to gateway	50.000
Túneles SSL	5.000
Throughput VPN SSL	7 Gbps
Sesiones Concurrentes	7 Millones

Sesiones SSL Concurrentes	800.000
Nuevas sesiones / segundo	430.000
Nuevas sesiones SSL / segundo	5.000
Puntos acceso soportados en modo túnel	512
Sistemas Virtuales incluidos	10

IV.b) Firewall de Próxima Generación Sede Don Torcuato. Cantidad 2

Número de Interfaces Requeridas	16x GE RJ45 4x GE SFP (Bahias) 2 x GE RJ45 Puertos administrativos
Throughput de Firewall (con paquetes de 512 Bytes)	20 Gbps
Latencia de firewall (con paquetes de 64 byte)	3 µs
Throughput de VPN IPSec (con paquetes de 512 byte)	7 Gbps
Throughput de NGFW	1.5 Gbps
Throughput de Inspección SSL	800 Mbps
Políticas de Firewall admitidas	10.000
Túneles IPsec gateway to gateway	2.000
Túneles IPsec client to gateway	10.000
Túneles SSL	500
Throughput VPN SSL	900 Mbps
Sesiones Concurrentes	2 Millones
Sesiones SSL Concurrentes	240.000
Nuevas sesiones / segundo	130.000

Nuevas sesiones SSL / segundo	1.000
Puntos acceso soportados en modo túnel	128
Sistemas Virtuales incluidos	10

iV. c) Puntos de conexión inalámbricos

Cantidad de dispositivos Access Point sede Retiro: 60

Cantidad de dispositivos Access Point sede Don Torcuato: 20

Tipo	Indoor
Throughput	800 Mbps
Nro. Máximo de Clientes por radio	512
Tecnología 802.11 a/b/g/n/ac	SI
Cantidad de **Puertos Ethernet**	2
Frecuencias de Radios	2.4 y 5 GHz
MIMO	2x2
802.11ac Wave2	SI
Potencia Máx de Transmisión	24 dBm
Spatial Stream	2
Antenas Internas	4
Ganancias de Antenas por radio	2.4 GHz: 4dBi ; 5 GHz: 5 dBi
Capacidad BLE	SI
Interfaces ethernet 1x 10/100/1000 Base-T RJ45	1
IEEE 802.3az	SI
SSIDs Simultáneos	16
Tipos EAP	EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST
Estandares IEEE	802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11ac, 802.1X, 802.3af, 802.3az
Transmit Beam Forming (TxBF)	SI
Maximum Likelihood Demodulation (MLD)	SI

Maximum Ratio Combining (MRC)	SI
A-MPDU and A-MSDU Packet Aggregation	SI
MIMO Power Save	SI
Short Guard Interval	SI
Rogue Scan Radio Modes	SI
WIPS / WIDS Radio Modes	SI
Spectrum Analyzer	SI
Peso Max.	500 gramos
Consumo Max.	12.5 Watts
Alimentación POE	SI
Accesorios incluídos para su instalación y fijación.	SI

V: INSTALACION

La adjudicataria deberá estar presente a través de sus representantes autorizados en el momento de la instalación de los equipos en el destino que esta S.E. Casa de Moneda le indique.

A los fines precedentemente señalados, la adjudicataria coordinará con personal de S.E. Casa de Moneda día y horario para realizar las tareas.

Los oferentes deberán especificar claramente en la oferta las condiciones ambientales que deberán ser cumplidas por S.E. Casa de Moneda para la correcta instalación de los equipos:

- Tipo de alimentación y potencia eléctrica requerida por las unidades ofrecidas, aclarando si es necesaria la instalación de un estabilizador externo para prever anomalías de la red domiciliaria de alimentación o si es suficiente con el estabilizador propio de la fuente de alimentación del equipo.
- Superficie propia ocupada por los equipos incluyendo puertas o paneles abiertos para su mantenimiento y espacio destinado a la operación de los mismos, si fuera necesario.
- Otras características que deban ser tenidas en cuenta para la instalación.

Si el oferente no suministra las especificaciones de la instalación física, se entenderá que no es imputable la falla al mal uso de los equipos por parte del usuario y por lo mismo las eventuales fallas estarán sujetas a reparación dentro de la cobertura que ofrece la garantía.

VI: GARANTIA

El adjudicatario deberá proveer, a partir de la fecha de instalación y puesta en funcionamiento y por el período de cinco (5) años, un servicio de garantía integral (partes, mano de obra y reemplazo inmediato de partes dañadas) para todo el hardware ofertado, con atención en el lugar de instalación incluyendo repuestos, traslados y mano de obra.

La garantía de funcionamiento comprenderá el servicio de reparación con provisión de repuestos y/o cambio de las partes que sean necesarias sin cargo alguno para S.E. Casa de Moneda. El proveedor garantizará que el servicio técnico será brindado por personal especializado de la empresa fabricante de los productos ofrecidos, o en su defecto por su propio plantel especializado el que deberá estar debidamente autorizado por los fabricantes de los productos ofrecidos.

Los materiales y repuestos a emplear deberán ser originales de fábrica o de calidad similar, nuevos y sin uso, debiendo presentarse la documentación que respalde las citadas características.

La propiedad de los repuestos que se instalen será de S.E. Casa de la Moneda. La propiedad de las partes reemplazadas será del proveedor.

La relación para el cumplimiento de la garantía será directamente entre el representante del oferente y el responsable de la S.E. Casa de Moneda.

Los oferentes que consideren necesaria la realización de mantenimiento preventivo durante el período de garantía solicitado deberán incluir un plan a efectos de coordinar con la S.E. Casa de Moneda las fechas y horarios en que serán llevados a cabo. De no ser presentado se interpretará que la firma oferente no considera necesario el mismo.

Los siguientes criterios son aplicables al equipamiento solicitado:
- El servicio de garantía deberá estar disponible en la modalidad de 7x24.
- El tiempo de respuesta a los llamados deberá ser en la modalidad de 7x24.
- El tiempo máximo para la reparación o reemplazo de los equipos será de 48hs. de efectuarse el llamado (considerando solo días hábiles).

Cuando la magnitud de la avería requiera el traslado del equipamiento para su reparación en laboratorio, el mismo será por cuenta y responsabilidad del adjudicatario y no generará ningún costo adicional para S.E. Casa de Moneda. Sólo se aceptará que los equipos sean retirados de las oficinas de S.E. Casa de Moneda para su reparación si previamente:
- El proveedor lo reemplaza por otro equipo de idénticas características.
- S.E. Casa de la Moneda autoriza en forma explícita el retiro de los equipos.

Si hubiera elementos o situaciones para los cuales no fuera aplicable la garantía, éstos y éstas deberán estar detallados en forma clara y explícita en la oferta. NO se aceptarán descripciones

ambiguas como ser "mal uso del equipamiento". No se aceptarán posteriores adiciones a la lista explícita de elementos y/o situaciones no cubiertas por la garantía.

El costo del servicio de garantía deberá estar incluido en el precio de los equipos.

Todas las características del servicio ofrecido se deberán encontrar operativas al día de la apertura de esta licitación.

Los oferentes deberán especificar claramente las condiciones ambientales para que la garantía cubra cualquier eventualidad incluyendo:

- Tipo de alimentación y potencia eléctrica requerida por las unidades ofrecidas, aclarando si es necesaria la instalación de un estabilizador externo para prever anomalías de la red domiciliaria de alimentación o si es suficiente con el estabilizador propio de la fuente de alimentación del equipo.
- Superficie propia ocupada por los equipos incluyendo puertas o paneles abiertos para su mantenimiento y espacio destinado a la operación de los mismos, si fuera necesario.

VII: LUGAR Y PLAZO DE ENTREGA

Los equipos serán entregados por cuenta del adjudicatario en:
Sede Retiro
Av. Antártida Argentina 2085, Ciudad Autónoma de Buenos Aires. Código postal C1104ACH
Dos (2) equipos

Sede Don Torcuato
Ruta Panamericana 24500 Don Torcuato, Prov. Buenos Aires. Código postal B1611KRN
Dos (2) equipos

Se deberá realizar la entrega del total adjudicado dentro de los .....30.... días hábiles, contados a partir de la notificación de la orden de compra.

VIII: CONDICIONES DEL SERVICIO DE SEGURIDAD Y VIGILANCIA

La Adjudicataria deberá proporcionar antes del inicio de su actividad una nómina de la dotación que concurrirá a esta S. E. CASA DE MONEDA, detallando: Apellido y nombre, Tipo y Número de Documento de Identidad, Fecha de nacimiento, Nacionalidad, Domicilio, Teléfono (si lo tuviese).

Dicha nómina deberá ser actualizada con suficiente anticipación en caso de reemplazos y/o ampliaciones.

La Adjudicataria cumplirá y hará cumplir a todo su personal las normas y procedimientos de Seguridad que le exija S. E. CASA DE MONEDA.

Asimismo, presentará una nómina pormenorizada de las herramientas y/o maquinaria que ingresará a esta S. E. CASA DE MONEDA para realizar las tareas.

IX: CONDICIONES DE HIGIENE Y SALUBRIDAD

La Adjudicataria deberá generar y preservar a su costo las condiciones de higiene y salubridad requeridas para cumplir con las regulaciones vigentes y con los requerimientos solicitados por S. E. CASA DE MONEDA, referentes a documentación a presentar para ingreso a la Planta, desenvolvimiento de trabajos en obra y Normas de Seguridad, para todo su personal durante la ejecución de los trabajos.

La Adjudicataria deberá especificar por nota, en forma previa a la iniciación de los trabajos, los encuadramientos que dentro de las actividades a desarrollar se aplicarán dentro del marco normativo vigente y conforme a las condiciones de riesgo que, como resultado de los trabajos a efectuar, puedan originar situaciones de peligro para las instalaciones y/o personal de S. E. CASA DE MONEDA.

La Adjudicataria deberá designar un responsable de la aplicación, control y desarrollo de las medidas de Seguridad surgidas del ítem precedente, el cual deberá contactarse con los responsables del Servicio de Higiene y Seguridad de S. E. CASA DE MONEDA al correo electrónico: seguridadehigiene@casademoneda.gob.ar, en forma previa a la iniciación de las tareas, con el fin de garantizar el normal cumplimiento de las actividades.

X: SEGURO- CERTIFICADO DE COBERTURA

La Adjudicataria presentará en forma mensual y durante la extensión del contrato y/o ampliaciones, el Certificado de Cobertura emitido por la Aseguradora de Riesgos del Trabajo (ART) que tiene contratada para su personal en relación de dependencia o, en su defecto, el pago mensual de la Póliza de Accidentes Personales para el personal que reviste en otra modalidad de prestación.

Deberá informar de igual modo, el procedimiento a seguir en caso de accidente de trabajo de su personal.

XI: CUADRO DE CUMPLIMIENTO TECNICO

Se detalla a continuación cuadro con las características de prestaciones requeridas a fin de que el oferente indique en el mismo las características de lo cotizado:

Características	Especificación requerida	Especificación ofrecida	Observaciones
PRESTACIONES			
Poseerá compatibilidad con todos y cada uno de los siguientes estándares: Ethernet IEEE 802.3, Fast Ethernet IEEE 802.3u, Gigabit Ethernet IEEE 802.3z, 10 Gigabit Ethernet IEEE 802.3ae.	SI		
Los equipos deberán poder operar en alta disponibilidad (2 en sede retiro y 2 en sede Don Torcuato), en modalidad activo-activo y activo-pasivo. Cada uno de los equipos deberá tener la posibilidad de agregado de fuentes redundantes del tipo hot swap. El sistema deberá poder operar en modo Router (permitiendo el envío de paquetes en L2 y L3) como así también en modo transparente.	SI		
Deberá permitir la creación de al menos 10 sistemas virtuales dentro del mismo equipo, sin necesidad de hardware o licencias adicionales. Cada sistema virtual podrá operar en modo Router o Transparente sin limitaciones en forma simultánea sobre cada sistema virtual.	SI		
El sistema deberá permitir la definición de interfaces virtuales (VLANs) las que podrán estar asignadas a diferentes interfaces	SI		

físicas en diferentes sistemas virtuales. Deberá soportar el etiquetado de los paquetes según IEEE 802.1Q utilizando cualquier ID (1-4095). Asimismo deberá contar con soporte de VXLAN.			
El mecanismo de control de filtrado utilizado por el engine del firewall deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.	SI		
El Firewall deberá poseer las configuraciones localmente, no dependiendo su funcionamiento de otros productos, servicios o herramientas de gestión centralizadas.	SI		
Las reglas deben permanecer en medio físico, no volátil. Estas reglas deberán poder definirse, diferenciando protocolo, IP destino/origen, puerto destino/origen y geolocalización utilizando rangos horarios.	SI		
El dispositivo deberá soportar al menos la generación de 10.000 políticas de firewall.	SI		
El dispositivo deberá soportar SNAT, DNAT y PAT. Será posible la aplicación de SNAT y DNAT y PAT en forma simultánea sobre una misma conexión.	SI		
Deberá soportar NAT estático y dinámico y PAT sobre cualquier tipo de conexión, tanto para IPv4 como IPv6. Deberá soportar NAT46 y NAT64 sobre la totalidad de las políticas de firewall.	SI		

Deberá soportar la configuración de NAT estático sobre todas las interfaces físicas y lógicas utilizando direcciones IP virtuales, que no sean las propias IP declaradas en las interfaces del firewall.	SI		
Cada Firewall deberá permitir el uso de objetos dinámicos aplicables a todo tipo de regla, definiendo las propiedades de los mismos sobre cada Firewall en particular. Los objetos deben poder referenciar servidores, redes, direcciones basadas en ubicación geográfica y servicios como mínimo.	SI		
Cada Firewall deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (HTTP, SMTP, FTP, H323, SIP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.	SI		
El equipo deberá permitir la implementación de políticas de calidad de servicio y Traffic Shaping soportando al menos: • Puertos físicos e interfaces agregadas o redundantes. • Políticas de QoS y Traffic Shaping por dirección de origen y destino, usuario y grupo. • La definición de tráfico con ancho de banda garantizado. • La definición de tráfico con máximo ancho de banda. • La definición de colas de prioridad. • La priorización de protocolo en tiempo real de voz (VoIP)	SI		

como H.323, SIP, SCCP, MGCP y aplicaciones como Skype. • El etiquetado de paquetes DiffServ, incluso por aplicación. • La modificación de los valores de DSCP para Diffserv. • La priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).			
El equipo deberá poseer la capacidad de entregar direcciones IP a los hosts conectados en sus interfaces LAN por medio del protocolo DHCP (DHCP server).	SI		
Cada Firewall deberá además soportar las siguientes funcionalidades: • Autenticación de usuarios en forma local y remota por medio de los protocolos RADIUS y LDAP, debiendo ser compatible con Active Directory. • Soporte de IPSec NAT Traversal.	SI		
El equipo deberá permitir la terminación de túneles VPN. • El Firewall deberá soportar túneles utilizando protocolo IPSEC estándar o a través de SSL. Para el caso de VPNs SSL, el equipo debe soportar que el usuario pueda realizar la conexión a través de un cliente VPN instalado en el sistema operativo de su máquina o a través de una interface web.	SI		
El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar un throughput requerido medido con tráfico real con la funcionalidad de control de	SI		

aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible.			
El equipo, con su funcionalidad de Next Generation Firewall activa deberá soportar el throughput requerido medido con tráfico real con las siguientes funcionalidades habilitadas simultáneamente: Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando múltiples políticas de seguridad y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.	SI		
El Control de Amenazas avanzadas (Sandboxing) deberá ser provisto en la solución. El mismo deberá estar disponible durante el período de garantía.	SI		
El Firewall deberá soportar la activación y desactivación de la funcionalidad de IPS, detección de anomalías y anti-malware para los protocolos soportados. • Deberá realizar el análisis de IPS basado en firmas las cuales se deberán poder agrupar para aplicar a las reglas. • Deberá permitir armar firmas propias de IPS.	SI		

• Deberá realizar la actualización de firmas de IPS en forma automática y periódica, durante el periodo de garantía. • Deberá poseer una base de conocimiento que detalle la definición de la regla. • Deberá ante un ataque de IPS responder con una notificación o un bloqueo del tráfico. • Deberá poseer la capacidad de excluir para una regla específica, una firma en particular; sin que ello implique deshabilitar por completo la utilización de esa firma en las demás reglas. • El motor de IPS deberá soportar el agregado de firmas específicas para ambientes industriales a los fines de interpretar los protocolos específicos de esos ambientes.			
El Firewall deberá identificar potenciales vulnerabilidades y sugerir las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de la solución. La información podrá brindarse mediante la GUI o vía reportes.	SI		
El Firewall deberá funcionar como proxy web explícito y como proxy transparente.	SI		
El Firewall deberá incorporar funcionalidades para SD-WAN. Si fuese necesario el agregado de licencias adicionales indicar cómo se aplican las mismas.	SI		
Capacidades de SD-WAN a soportar en el firewall:	SI		

• Balanceo de vínculos a Internet, VPNs y enlaces WAN (ej: MPLS) • Balanceo Round Robin, Balanceo por peso, cantidad de sesiones, ancho de banda y derrame. • Definición de políticas de SDWAN por Aplicación, Servicio de internet, usuarios, IPs o Interfaces/zonas. • Soporte a más de 5 vínculos a Internet. • Debe contar con un mecanismo por el cual se puedan recuperar los datos enviados sin necesidad de recurrir a las retransmisiones de protocolo TCP y que permita la reconstrucción del stream en el lado receptor.			
El Firewall deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de Servicio).	SI		
Cada Firewall deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular.	SI		
Debe tener la función de protección a través de la resolución de	SI		

direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos.			
Deberá tener la posibilidad de aplicar la funcionalidad de antivirus por regla sobre conexiones HTTP, FTP, SMTP, POP3, IMAP y túneles VPN encriptados establecidas a través del equipo.	SI		
Deberá tener la funcionalidad de filtrado de contenidos Web. • Deberá permitir o bloquear el acceso de los usuarios a diferentes sitios web considerados o no maliciosos. • Deberá permitir el 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). • Deberá permitir la actualización automática de la base de filtrado de contenidos durante el transcurso del período de garantía. • Deberá soportar al menos sesenta (60) categorías en la base de filtrado.	SI		
Deberá tener la funcionalidad para detectar aplicaciones. Para ello el equipo deberá: • Inspeccionar el contenido del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas,	SI		

independiente de puerto y protocolo que utilicen. • Deberá reconocer al menos 3000 aplicaciones diferentes, permitiendo agrupar las mismas en al menos 16 categorías y aplicar políticas de seguridad a las mismas. Debe permitir la creación de firmas de aplicación manuales. • Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo. • Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo. • Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos.			
Deberá soportar la inspección de sesiones que atraviesan el firewall y utilizan el protocolo SSL (Secure Sockets Layer) para encriptación, incluyendo el protocolo HTTPS.	SI		
El equipo deberá proveerse con los servicios de actualización de firmas para los motores de filtrado descriptos en los puntos anteriormente mencionados por el término de 60 meses.	SI		
Debe permitir la administración del equipo por medio de los protocolos	SI		

HTTP/HTTPS, Telnet/SSH y SNMP v1/v2.			
Deberá permitir el registro local y remoto de eventos utilizando servidores syslog.	SI		
Controlador de puntos de conexión inalámbricos o WIFI. Dicha función deberá estar integrada dentro de la solución de firewall requerida (sede Retiro: 60 dispositivos y sede Don Torcuato: 20 dispositivos).	SI		
En el caso de requerir una licencia específica para la funcionalidad de Controlador WIFI especificarlo.	SI		
Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;	SI		
La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	SI		
El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS	SI		
La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario	SI		

Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points	SI		
El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tuneleados hasta el controlador inalámbrico	SI		
Cuando tuneleado, el tráfico debe ser encriptado a través de DTLS o IPSEC	SI		
Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;	SI		
Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse	SI		

la conexión de nuevos usuarios a la red inalámbrica			
La solución debe permitir definir qué redes serán tuneleadas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	SI		
La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tuneleados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso	SI		
La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso	SI		
La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados	SI		
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura	SI		

inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación			
La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio de interfaz de origen el SSID de la red WIFI	SI		
La solución debe monitorear y clasificar el riesgo de las aplicaciones accesadas por los clientes inalámbricos	SI		
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID	SI		
Debe implementar la autenticación administrativa a través del protocolo RADIUS	SI		
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES)	SI		
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3	SI		

La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado	SI		
Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada	SI		
La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS	SI		
La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X	SI		
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP	SI		
La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red	SI		
La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico	SI		
La solución debe permitir la personalización de la página de	SI		

autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes			
La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red	SI		
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo	SI		
La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada	SI		
La solución debe garantizar que los usuarios se autentiquen en el portal cautivo que utilice la dirección IPv6	SI		
La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución	SI		
Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado	SI		
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes	SI		
La solución debe identificar automáticamente el tipo de equipo y sistema operativo	SI		

utilizado por el dispositivo conectado a la red inalámbrica			
La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible	SI		
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog	SI		
La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps	SI		
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP	SI		
La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB)	SI		
La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos	SI		
La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal,	SI		

además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal			
La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado	SI		
La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios	SI		
La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming	SI		
La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia	SI		
La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente	SI		

conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos			
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica	SI		
La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado	SI		
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz	SI		
La solución provista debe tener la capacidad de hacer Reporting, Análisis y guardar logs. Esta solución deberá ser de la misma marca que los equipos propuestos. • Deberá poder ser desplegado como una Máquina Virtual (VM) sobre infraestructura KVM o VMWare. • El sistema deberá analizar los registros provenientes de múltiples dispositivos, por usuario o por grupo de usuarios • Deberá generar una variedad de reportes que permiten a los administradores de red asegurar las redes de manera proactiva conforme se presentan las amenazas, evitando los abusos de red. • El sistema deberá permitir la visualización de registros o	SI		

cualquier mensaje o archivo de registro desde los dispositivos registrados. Deberá implementar filtros que permitan navegar sobre los registros de forma simple y amigable. • El sistema deberá implementar reportes que permitan a los administradores conocer al menos: • Ataques: por unidad, por hora del día, por categoría, y por fuentes de los ataques. • Virus: principales virus detectados en la red y detectados por Protocolo. • Eventos: Por Firewall, eventos en general, eventos de seguridad desencadenados y eventos desencadenados por el día de la semana. • Utilización de la Red: Principales usuarios de la Red y principales clientes intentando acceder a sitios bloqueados. • Ancho de banda: Principales usuarios de ancho de banda. Ancho de banda por día, por hora y utilización de ancho de banda por familia de protocolos. • Protocolos: los principales protocolos utilizados, usuarios FTP y usuarios de Telnet. • El sistema deberá implementar análisis forenses de forma que se pueda rastrear las actividades de un usuario. • El sistema deberá ser administrable vía Web utilizando HTTPs.			

Los administradores podrán ser por dominio y deberá poder asignarse de qué equipos (por dirección IP y máscara) puede el administrador conectarse. • El sistema deberá soportar al menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only). • Debe contar con reporte de AP's y SSID's autorizados, así como clientes WIFi			
La solución provista deberá contar con el espacio para el almacenamiento permanente de los logs y espacio para el guardado de los logs diarios que se utilizarán para la Analítica.	SI		
Debe soportar servicio de Indicadores de Compromiso del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	SI		
La solución provista deberá tener no menos de 3 TB de Almacenamiento permanente de logs y 6 Gbps para Analítica de logs diarios.	SI		
GARANTIA integral por el término de cinco (5) años.	SI		

XII: PRUEBAS Y COMPROBACIONES

- S.E. CASA DE MONEDA se reserva el derecho de solicitar al oferente, cuando este lo requiera, ponga a su disposición, un equipo de idénticas características al que cotiza en la oferta, de manera de poder verificar que responde al modelo ofertado con las características solicitadas y poder realizar sobre el mismo las pruebas de performance.

- Estas pruebas y comprobaciones no implicarán reconocimiento de gasto por parte de S.E. CASA DE MONEDA y el material necesario para la misma será facilitado sin cargo por el oferente.

- La fecha y lugar de aplicación de las pruebas serán convenidos entre el S.E. CASA DE MONEDA y el oferente a efecto de que las mismas se realicen dentro de los 10 (diez) días hábiles siguientes a la apertura de las ofertas. Con tal fin el oferente deberá disponer de los elementos ofrecidos a las 48hs. contadas a partir de su notificación por parte de S.E. CASA DE MONEDA.

- No se aceptará probar equipamiento cuyas características, marca y/o modelo no se correspondan exactamente con la oferta.

XIII: VISITA DE OBRA

A los fines de la exacta apreciación de las características de los trabajos, sus dificultades y sus costos, el oferente deberá efectuar una visita (obligatorio) a los lugares de emplazamiento de los trabajos, a fin de examinar por su cuenta las condiciones en que recibirá las instalaciones, previo a la presentación de la oferta.

Al momento de la visita se le extenderá un certificado de visita de obra, que deberá ser presentado junto con la oferta. Las visitas podrán efectuarse hasta 96 hs. antes de la fecha de apertura de ofertas, en el horario de 10:00hs. a 16:00hs. y deberán coordinarse en tecnologia@casademoneda.gob.ar.

El no cumplimiento de la inspección puede ser causa de desestimación de la oferta, al sólo y exclusivo juicio de Casa de Moneda, no dará derecho a reclamo alguno a los oferentes por desconocimiento de las instalaciones.

CLAUSULAS PARTICULARES

Licitación Pública Nº 572

Expediente Nº 31325

Objeto: PROVISION, INSTALACION Y SOPORTE SISTEMA SEGURIDAD FIREWALL.

Presentación de ofertas: Las ofertas deberán presentarse en Mesa de Entradas en sobre cerrado, detallando solamente el Nº de Expediente y Fecha de Apertura, antes de la fecha y hora indicada para la apertura.
Se recomienda que el sobre con la oferta sea presentado con 24 hs. de antelación a la fecha de apertura, el cual permanecerá cerrado hasta el Acto de la Apertura, pudiendo el oferente presenciar la misma.

Apertura: el acto de apertura se celebrará el día 26 de enero a las 11:30 Hs.

Cronograma:

	Inicio	Fin	Hora	Lugar
Retiro de Pliegos	Desde la publicación y/o invitación	Hasta el momento de la apertura	9:30 a 17:00	**Área de Compras**
Consultas	Hasta 3 (tres) días antes de la apertura		9:30 a 17:00	**Área de Compras**
Presentación de Ofertas	Hasta el momento de la apertura		11:30	**Área de Compras Nacionales**
Apertura	**26/01/2021**	**26/01/2021**	11:30	**Sala de aperturas Área de Compras**

Mantenimiento de la Oferta: las ofertas tendrán validez por el término de sesenta (60) días corridos, contados a partir de la fecha del Acto de Apertura, de acuerdo a lo establecido en el punto 4 de las Clausulas Generales.

AV. ANTARTIDA ARGENTINA 2085
(C 1104 ACH) CIUDAD AUTONOMA DE BUENOS AIRES
TEL: (0541) 5776 – 3400 y líneas rotativas
TEL-FAX (0541) 5776 - 3400
cmcompras@casadelamoneda.gob.ar
www.casadelamoneda.gob.ar

Dra. ANDREA LAPADULA
Gerente de Compras
S.E. CASA DE MONEDA

Garantías

Las garantías a consignar para la presente licitación son las siguientes:

Garantía de mantenimiento de oferta: El oferente deberá constituir una Garantía por un importe no inferior al 5% (cinco por ciento) del monto total cotizado debiendo acompañar la misma en su propuesta. En el caso de cotizar con alternativas, la garantía se calculará sobre el mayor valor propuesto.

Garantía de adjudicación: El adjudicatario deberá constituir dentro de los 10 (diez) días subsiguientes a la notificación de la adjudicación una garantía por un importe total del 15% (quince por ciento) del monto total adjudicado. En caso de firma del exterior el plazo para la presentación de la garantía se extiende a 10 (diez) días de recibida la orden de compra.

Plazo de entrega: 30 días hábiles, a partir de la firma del acta de inicio de prestación del servicio.

Lugar de Entrega: *Retiro Sito en Pedro Zanni 370 C.A.B.A. de 09,30 a 18 hs. y Planta Don Torcuato Sito en Ruta Panamericana Km. 25,500 DON TORCUATO.*

Criterio de evaluación y selección de ofertas: la adjudicación deberá realizarse a favor de la oferta más conveniente para la S.E.C.M., teniendo en cuenta el precio, la calidad, la idoneidad del oferente y demás condiciones de la oferta.

Dra. ANDREA LAPADULA
Gerente de Compras
S.E. CASA DE MONEDA

S. E. CASA DE MONEDA

10C

Foja N° 48

ANEXO N° I

MODELO DE CARTA DE PRESENTACION

Buenos Aires, ...

Señores
S.E. CASA DE MONEDA
Av. Antártida Argentina 2085
Buenos Aires
República Argentina

La Empresa. . . . . en adelante el Oferente, representada legalmente por el Señor . . . . . presenta su oferta de conformidad con lo establecido en el PLIEGO DE BASES Y CONDICIONES denominado PROV, INST Y SOP-SIST SEGURIDAD FIREWALL que es objeto de la Licitación Pública N° 572 .

El Oferente declara expresamente que:

La oferta se ajusta íntegramente a los documentos de la contratación y que la presentación no está impedida o afectada por ninguna de las incompatibilidades que allí se establecen.

Que no tiene relación de dependencia ni vinculación directa o indirecta con S.E.C.M., ni con el Estado Nacional, ni con sus directivos o funcionarios.

Que la Oferta es válida y permanecerá vigente por el lapso y en los términos establecidos en el Pliego de Bases y Condiciones.

Declara que la presentación de la oferta significa el pleno conocimiento y aceptación de las normas y cláusulas establecidas en el pliego (Especificaciones Técnicas; Cláusulas Generales; Cláusulas Particulares y Anexos).

Que renuncia a cualquier reclamación o indemnización en caso de error en la interpretación de los Pliegos de Bases y Condiciones y demás documentos aplicables al

presente llamado. S.E.C.M. no será responsable por cualquier error u omisión en la preparación de esta oferta.

Declara la veracidad y exactitud de toda la información proporcionada, y autoriza mediante la presente, a que cualquier persona física o jurídica suministre a S.E.C.M. toda la información que se considere necesaria para verificar la documentación que se presenta.

Que se compromete a proporcionar cualquier información adicional que le fuera requerida o aclaraciones sobre la documentación presentada y en caso de no hacerlo será motivo suficiente para eliminar su oferta.

Que en el caso de resultar adjudicatario, se compromete a presentar la garantía de cumplimiento del Contrato, así como también a suscribir la Orden de Compra dentro del plazo fijado por S.E. C.M.

Que en el caso de que no mantuviera la oferta por el plazo indicado, que no presentase la garantía de cumplimiento del contrato a satisfacción de esta Sociedad, o que no suscribiese la Orden de Compra dentro del plazo fijado por S.E.C.M., se perderá la garantía de oferta.

Atentamente.

Firma del Representante Legal .....

Nombre y Sello de la Empresa .....

Domicilio legal / especial .....

Correo electrónico .....

Teléfono .....

ANEXO N° II

ASPECTOS LEGALES

A los efectos de acreditar su capacidad legal, el oferente deberá presentar:

a- Estatuto o Contrato Social, con todas las modificaciones, si las hubiere vigentes, y constancias de sus respectivas inscripciones en los Registros Públicos correspondientes.

b- Acta de Asamblea y/o Acta de Directorio con la distribución de los cargos vigentes al momento de realizar la oferta o Acta de socios donde conste la designación de los socios gerentes vigentes.

c- En caso de ser una empresa unipersonal deberá acompañar copia del D.N.I. del titular y copia de la constancia de Inscripción a Ingresos Brutos o Convenio Multilateral.

d- Poder especial y/o General, otorgado ante Escribano Público, por el que se designa, a uno o más representantes con facultades amplias y suficientes para representar al oferente sin limitación alguna, y para obligar a los mandantes durante el proceso licitatorio, en el supuesto que la persona designada no fuere el representante legal de la oferente.
Si se tratare del representante legal, bastará que el documento social que contenga, de manera expresa, las facultades requeridas anteriormente.

NOTA: Toda la documentación solicitada en los ítems anteriores, con excepción del ítem c, deberá estar certificada por Escribano Público; indicando el notario que interviene de manera expresa, libro, folio, numero de acta y demás circunstancias identificatorias del documento original cuya copia certifica.

e- A los efectos del cumplimiento de sus obligaciones los oferentes deberán constituir domicilio legal y especial en la Ciudad Autónoma de Buenos Aires de la República Argentina o en la Provincia de Buenos Aires, indicando número de teléfono/fax y dirección de e-mail, y quedarán sometidos a los TRIBUNALES FEDERALES con asiento en esta ciudad.

...ARIEZ
...A

f- Para el supuesto de Sociedades constituidas en el extranjero:

- Acreditar la existencia de la sociedad con arreglo a las leyes de su país.
- Fijar un domicilio en la República Argentina donde le serán válidas todas las notificaciones judiciales y/o extrajudiciales.
- Designación de uno o más representantes con facultades amplias y suficientes para representar al oferente sin limitación alguna, y para obligar a los mandantes durante el proceso licitatorio, en el supuesto en que la persona designada no fuera el representante legal del oferente.
- Si se tratare del representante legal, bastará que el acta de directorio contenga, de manera expresa, las facultades requeridas anteriormente.

NOTA: Toda la documentación, procedente del extranjero, destinada a acreditar requisitos establecidos en este pliego, debe estar apostillada de acuerdo a la normas de la Convención de la Haya. En caso de que provengan de un país que no la hubiese suscripto, deberá respetar la reglamentación de la República Argentina en materia consular.

g- Para el supuesto de Uniones Transitorias de Empresas:

- Constitución o Compromiso U.T.E., su objeto y la constancia de su respectiva inscripción registral o constancia de iniciación del trámite respectivo.
- Identificación de las personas físicas o jurídicas que las integran e identificación de las personas físicas que integran cada empresa.
- Declaración de solidaridad de sus integrantes por todas las obligaciones emergentes de la presentación de la oferta, de la adjudicación y de la ejecución del contrato.

Se entenderá cumplida la obligación de acompañar la documentación del Anexo II si la misma hubiese sido debidamente presentada con anterioridad; siempre y cuando se encontrare vigente y actualizada en caso de corresponder.

ANEXO N° III

ASPECTOS ECONÓMICO - FINANCIEROS

A los efectos de acreditar su capacidad económica financiera el oferente deberá presentar:

a) Solo deberá ser presentado cuando se trate de provisión de **SERVICIOS,** Estados Contables de los dos (2) últimos ejercicios anuales con dictamen del profesional en Ciencias Económicas con certificación de firma por el Consejo Profesional, y copia certificada del Acta de Asamblea aprobatoria de dichos estados.

ASPECTOS PREVISIONALES

Deberán presentar:

b) En caso de no contar con Certificado Fiscal para Contratar deberá acompañar declaración jurada y fotocopia de constancia de inscripción y comprobante de pago de los últimos tres (3) meses de aportes previsionales (F-931) de AFIP.

PARA LAS EMPRESAS DEL EXTERIOR:

A los efectos de acreditar su capacidad económica financiera el oferente deberá presentar, de acuerdo a las leyes de su país:

a) Documentación relativa a los dos últimos períodos fiscales.

Se entenderá cumplida la obligación de acompañar la documentación del Anexo III siempre que la misma haya sido presentada y no supere el año a partir de la fecha de apertura del presente llamado.

ANEXO N° IV

ASPECTOS TÉCNICOS

A los efectos de acreditar su capacidad técnica el oferente deberá presentar:

a) Nómina de las empresas a las que provean productos/servicios similares al solicitado en la presente, nombre y datos de las mismas y cualquier otro dato considerado importante para la mejor evaluación de la capacidad técnica de la empresa, adjuntando Certificados de satisfacción. (ver MODELO ADJUNTO).

b) Declaración Jurada de habilidad para contratar con el Estado Nacional.

c) Declaración Jurada de todos los juicios que mantengan con el Estado Argentino ó particulares (en caso de ser parte en algún un juicio se debe mencionar: carátula, número de expediente, juzgado y secretaría).

d) En caso de poseerlo podrán presentar copia del Certificado de Norma de Calidad ISO, igual o superior al N° 9000 o en su defecto documentación que acredite que la empresa se encuentra oficialmente en proceso de Certificación de esta Norma en relación con el proceso de producción del producto y/o servicio de que se trata.

ANEXO N° 4 - MODELO REFERENCIAS COMERCIALES

	EMPRESA/ ORGANISMO CONTRATANTE	DENOMINACIÓN DEL SERVICIO/ PRODUCTO	DURACIÓN /CANTIDAD	FECHA	OBSERVACIONES	CONTACTO
1						
2						
3						
4						
5						
6						

CLÁUSULAS GENERALES.

No será necesario firmar ni acompañar las presentes Cláusulas Generales. La presentación de la oferta implica la aceptación total y la absoluta conformidad con el contenido del pliego.

Plazos	Se contarán en días hábiles administrativos, salvo en los casos en que se aclare expresamente lo contrario. Cuando se fije en semanas se contarán por períodos de 7 días corridos. Cuando se fije en meses o años, será conforme lo dispuesto en el Código Civil y Comercial de la Nación.
Oferente o Proponente	Persona humana o jurídica que presenta su oferta en un procedimiento de selección iniciado por SECM.
SECM	Sociedad del Estado Casa de Moneda

1. Normativa aplicable – Orden de prelación:

Todos los documentos que integran la contratación serán considerados como recíprocamente explicativos, según corresponda.

En caso de existir discrepancias, se seguirá el siguiente orden de prelación:

a) El Reglamento de Contrataciones de SECM.
b) El Pliego de Bases y Condiciones Generales.
c) El Pliego de Bases y Condiciones Particulares.
d) Las Circulares Con Consulta y/o Sin Consulta.
e) La Oferta y las Muestras que se hubieren acompañado.
f) La Adjudicación.
g) La Orden de Compra o Contrato.

La presente contratación se encontrará alcanzada por las previsiones de la Ley Nacional N° 27.437 "LEY DE COMPRE ARGENTINO Y DESARROLLO DE PROVEEDORES", y su normativa complementaria y/o modificatoria", en los casos previstos en el artículo 2 de la citada norma.

2. Requisitos para ser Proveedor:

Podrán contratar con SECM todas las personas humanas o jurídicas con capacidad para obligarse, que acrediten su solvencia económica y financiera y su idoneidad técnica y profesional.

No podrán contratar con SECM ni inscribirse en el registro de proveedores:

a) Las personas humanas o jurídicas que se encuentren suspendidas o inhabilitadas para contratar con SECM.
b) Los agentes al servicio de SECM y hasta un año a partir de su desvinculación, como así tampoco las sociedades en las cuales aquellos tengan participación, ya sea como accionista, administrador, director, síndico o gerente.
c) Los fallidos, interdictos y concursados, salvo que estos últimos presenten la correspondiente autorización judicial y se trate de contratos donde resulte intrascendente la capacidad económica del oferente.
d) Los condenados por delitos dolosos.

e) Las personas que se encontraren condenadas por delitos contra la propiedad, o contra la Administración Pública, o contra la fe pública o por delitos comprendidos en la Convención Interamericana contra la Corrupción, Ley Nº 24.759.
f) Los evasores y deudores morosos tributarios de orden Nacional o local, previsionales, alimentarios, declarados tales por autoridad competente.
g) Las personas humanas o jurídicas que registren una sanción grave y vigente en cualquier repartición pública.

3. Forma de Presentación de la Oferta:

a) Redactada en idioma nacional.
b) Presentada por escrito en papel o en forma electrónica, según corresponda.
c) Deberá contener la propuesta económica.
d) El precio unitario y cierto, en números, con referencia a la unidad de medida establecida.
e) El precio total del renglón, en números, y el total general de la oferta, expresado en letras y números.
f) Deberá indicarse la moneda de cotización, a excepción de que el pedido de cotización establezca la misma.
g) Si el precio fuese gravado con IVA, deberá discriminarse su monto y declararse su alícuota porcentual.
h) Si se tratara de productos con envase y/o embalados, la cotización deberá efectuarse por cantidades netas y libres de envase y de gastos de embalaje, salvo que se previera lo contrario.
i) Las muestras deberán presentarse acompañadas de remito, en el caso que hubieran sido solicitadas, indicando el procedimiento de selección al que corresponden, en un rótulo debidamente fechado, firmado y sellado por el oferente, ubicado en parte visible.
j) La garantía pertinente, cuando corresponda.
k) Descripción del bien o servicio ofertado y catálogo y/o folletos ilustrativos si así correspondiese.
l) El recibo de la muestra cuando hubiese sido presentada por separado.
m) El plazo de entrega, en el supuesto en que difiera del fijado en el Pliego de Bases y Condiciones Particulares.
n) Estructura de costos en la que se detallen los componentes nacionales e importados del producto/servicio ofrecido.

El proponente podrá formular oferta por todos los renglones o por algunos de ellos, según se establezca en el Pliego de Bases y Condiciones Particulares.

Como alternativa, después de haber cotizado por renglón, podrá efectuar un descuento en el precio, por el total de los renglones o por grupo de renglones, sobre la base de su adjudicación íntegra.

Cuando la cotización se hiciere en moneda extranjera, a todos los efectos de este Reglamento se calcularán los importes, sobre la base del tipo de cambio vendedor del Banco de la Nación Argentina vigente al cierre del día anterior a la fecha de:

1. La constitución de la garantía.
2. La apertura de ofertas, para la comparación de precios.

Gastos por cuenta de los oferentes

a) Costo del despacho, derechos y servicios aduaneros y demás, por cualquier concepto en el caso de rechazo de las mercaderías importadas con cláusulas de entrega en el país.
b) Gastos de protocolización del contrato cuando se previera en el Pliego de Bases y Condiciones Particulares.
c) Reparación o reposición, según proceda, de los elementos destruidos total o parcialmente, a fin de determinar si se ajusta en su composición o construcción a lo contratado cuando por ese medio se comprueben defectos o vicios en los materiales o en su estructura. En caso contrario los gastos pertinentes estarán a cargo de la SECM.

Cotizaciones por productos a importar

Las cotizaciones por productos a importar, deberán hacerse bajo las siguientes condiciones:

a) En moneda extranjera, cuando así se hubiera previsto en las Pliego de Bases y Condiciones Particulares, correspondiente al país de origen del bien ofrecido u otra usual en el comercio internacional.
b) De no estipularse lo contrario las cotizaciones se establecerán en condiciones C.I.F. o C.I.P.
c) En las cotizaciones en condiciones C.I.F. o C.I.P., se deberá discriminar el valor FOB y el costo de flete y seguros.
d) En aquellos casos especiales en que se establezca la condición F.O.B. para las cotizaciones, la SECM deberá calcular el costo para los seguros y fletes a los fines de realizar la comparación de ofertas.
e) En las cotizaciones será condición de preferencia consignar los gastos por los siguientes conceptos:
    1. Recargos y derechos aduaneros.
    2. Otros gastos o gravámenes, si los hubiere.
f) Salvo convención en contrario, los plazos de entrega se entenderán cumplidos cuando la SECM reciba los bienes en el lugar que indique el Pliego de Bases y Condiciones Particulares.
g) Cuando la mercadería adquirida deba ser entregada y se trate de elementos a instalar y recibir en funcionamiento, el oferente deberá consignar por separado los plazos para dar cumplimiento a esta última obligación. A tal efecto, los mismos comenzarán a computarse a partir de la comunicación por parte de la SECM del arribo de la mercadería a su destino definitivo.
h) Se respetarán las normas del comercio internacional, las habituales establecidas y aceptadas por nuestro país.
i) Las empresas del exterior deberán informar lo siguiente, para el total de la provisión:
    - Volumen
    - Peso neto en kilos
    - Peso bruto en kilos
    - Cantidad de cajones y dimensiones
    - Cobertura del seguro
    - Posición arancelaria en el NCM (Nomenclador Común del MERCOSUR)

j) Toda materia prima, material o elemento, simple o compuesto, que constituya un reconocido riesgo a la salud o al medio ambiente, deberá ser provisto en sus respectivos envases con las debidas indicaciones en sus rótulos aclaratorios, y acompañados por la hoja de datos correspondiente, tal cual la exigencia de normas legales en vigencia. Esta restricción es de carácter obligatorio, en el caso de no cumplimiento de este requisito dará motivo al rechazo en la recepción de mercadería.

4. Mantenimiento de la oferta:

Las ofertas presentadas serán válidas para SECM por el término de 60 (sesenta) días corridos contados a partir de la fecha límite para presentarla. Si el oferente no manifestara en forma fehaciente su voluntad de no renovar la oferta con una antelación mínima de 10 (diez) días corridos al vencimiento del plazo, aquélla se considerará prorrogada automáticamente por un lapso de 30 (treinta) días corridos y así sucesivamente, salvo disposición en contrario, hasta un plazo máximo de 180 (ciento ochenta) días corridos.

5. Muestras:

a) En caso de que se requieran muestras del producto ofertado, las mismas deberán individualizarse indicando el procedimiento de selección a la cual corresponden, en un rótulo debidamente fechado, firmado y sellado por el oferente, ubicado en parte visible.
b) Si existiera muestra patrón, bastará al oferente manifestar en su propuesta que lo ofertado se ajusta a la misma.
c) Las muestras presentadas por aquéllos oferentes que no hayan sido adjudicados y que no haya sido necesario someterlas a un proceso destructivo para su examen, serán retiradas por sus propietarios en el plazo de 2 (dos) meses de concluido el procedimiento. Transcurrido dicho plazo las muestras pasarán a ser propiedad de SECM, sin cargo.
d) Las muestras correspondientes a los artículos adjudicados quedarán en poder de SECM para contralor de los que fuesen provistos, salvo que sus características no permitan su retención. Una vez cumplido el contrato las muestras serán devueltas conforme a lo previsto en el apartado anterior.

6. Garantías:

6.1 Garantía de mantenimiento de oferta.

Cuando sea exigida en las Cláusulas Particulares, deberá constituirse por un importe no inferior al 5% (cinco por ciento) del monto total cotizado incluyendo el IVA, debiendo acompañar la misma en su propuesta. En el caso de cotizar con alternativas, la garantía se calculará sobre el mayor valor propuesto. La garantía deberá tener plena vigencia por todo el término de mantenimiento de la propuesta.
La no presentación de la misma implicará la desestimación de la oferta

6.2 Garantía de adjudicación.

El adjudicatario deberá constituir dentro de los 10 (diez) días subsiguientes al perfeccionamiento del contrato, una garantía por un importe del 15% (quince por ciento) del monto total adjudicado, la que deberá cubrir el período que va desde la fecha de emisión de la Orden de Compra hasta la recepción definitiva y la totalidad de las obligaciones del adjudicatario.

6.3 Formas de las garantías

Las garantías podrán constituirse de las siguientes formas o combinaciones de ellas:

a) Mediante depósito o transferencia bancaria efectuado en la cuenta que la SECM indique, u otro medio que ésta establezca, siempre con expresa indicación de la imputación a la contratación de que se trate.

b) Con pagarés a la vista, suscriptos por quienes tengan el uso de la firma social o actuaren con poderes suficientes, siempre y cuando, la garantía no supere los $ 250.000 (Pesos doscientos cincuenta mil), pagaderos en la Ciudad Autónoma de Buenos Aires.

c) Mediante aval u otra fianza bancaria a satisfacción de la SECM, constituyéndose el fiador en deudor solidario, liso y llano y principal pagador con renuncia a los beneficios de división y excusión en los términos de los Artículos 1584 y 1589 del Código Civil y Comercial de la Nación, así como al beneficio de interpelación judicial previa.

d) Mediante seguro de caución a través de pólizas emitidas por compañías de seguros autorizadas por la Superintendencia de Seguros de la Nación, extendidas a favor de la SECM. Las mismas serán incondicionales, irrevocables y renovables.

e) Cualquier otra garantía que la SECM considere satisfactoria.

La elección de la forma de garantía, en principio, queda a opción del oferente o adjudicatario, con excepción de lo establecido en el Artículo 18 inciso b), y si nada se expresa en el Pliego de Bases y Condiciones Particulares, Orden de Compra y/o Contrato, según corresponda, respecto de la presentación de algún tipo de garantía en especial.

Todas las garantías, deberán cubrir los plazos previstos en el Pliego de Bases y Condiciones Particulares, garantizarán el total cumplimiento de las obligaciones contraídas, debiendo constituirse en forma independiente para cada contratación.

Las garantías constituidas podrán ser sustituidas por otras de igual magnitud, a pedido del oferente o adjudicatario, previa aprobación por parte de la SECM.

La SECM no abonará intereses por los depósitos en garantía.

7. Recepción y Apertura de ofertas:

El Acto de Apertura de Ofertas ocurrirá en el lugar, día y hora determinados en el Pliego de Bases y Condiciones, que será el límite para la presentación de ofertas. Se procederá a abrir las ofertas en presencia de los funcionarios de SECM que se designen a tal efecto y de todos aquellos que desearan presenciarlo.

Si el día señalado para la apertura de las ofertas deviniera inhábil, el acto tendrá lugar el día hábil siguiente y a la misma hora.

8. Causales de desestimación no subsanables:

Será desestimada total o parcialmente, la oferta en los siguientes supuestos:

a) Cuando no estuviere firmada la oferta económica, en ninguna foja, cuando sean presentadas en papel.
b) Cuando no se presente la garantía exigida o cuando no cubra al menos el 75% (setenta y cinco por ciento) del monto requerido.
c) Cuando no se presenten las muestras solicitadas en la documentación que rija el procedimiento de selección.
d) Cuando fuera formulada por personas inhabilitadas o suspendidas para contratar con SECM.
e) Cuando las propuestas se encuentren condicionadas o se aparten de la documentación que rija el procedimiento de selección, salvo aquellas que contengan defectos de forma que no constituyan impedimentos para su aceptación, tales como errores evidentes en los cálculos, falta de totalización de las propuestas, error en las especificaciones del monto de la garantía u otros aspectos que no impidan su completa, integral y equitativa comparación con las demás ofertas.
f) Cuando fuere ilegible, tuviere raspaduras, enmiendas o interlíneas en el precio, cantidad, plazo de entrega o alguna otra parte que hiciere a la esencia del contrato, y no estuvieren debidamente salvadas.
g) Cuando las ofertas contengan algún tipo de condición que afecte su validez o vigencia o formulen reservas de modificación a futuro.

9. Errores de Cotización:

Si el total cotizado por cada renglón no correspondiera al precio unitario se tomará éste último como precio cotizado.

Todo otro error en el monto cotizado, ya sea denunciado por el oferente o detectado por la SECM podrá ser desestimado de la oferta en los renglones pertinentes. La autoridad competente evaluará si correspondiera aplicar la pérdida de la garantía de mantenimiento de oferta, en la proporción que corresponda.

10. Precio vil o no serio:

La oferta será desestimada cuando de los informes técnicos de evaluación surja que no podrá ser cumplida en forma debida por tratarse de precios excesivamente bajos de acuerdo a criterios objetivos que surjan de los precios de mercado y de la evaluación de la capacidad económica del oferente.

11. Desempate de ofertas:

En caso de igualdad en el orden de mérito de las ofertas, se solicitará mediante comunicación fehaciente a los respectivos oferentes, que por el mismo medio que remitieran la oferta y dentro del término del plazo común que se les fije, formulen una mejora de ofertas.

El silencio por parte del oferente invitado a mejorar se considerará como que mantiene su oferta.

De subsistir el empate, se procederá al sorteo público de las ofertas empatadas. Para ello se deberá fijar día, hora y lugar del sorteo público y notificarse por medio fehaciente a los oferentes llamados a desempatar. El sorteo se realizará en presencia de los interesados, si asistieran, y se labrará el acta correspondiente.

12. Mejora de ofertas:
SECM se reserva el derecho de solicitar **mejora de precios**:

a) Al oferente que haya formulado la oferta más económica y a los siguientes, cuando la diferencia entre ellos esté comprendida en un 3 % (tres por ciento).
b) Al oferente que reciba el primer orden de mérito, o al oferente único en su caso cuando existan motivos para considerar su oferta onerosa en comparación con la valuación estimada y/o anteriores órdenes de compra.

SECM se reserva el derecho de solicitar **mejora de plazos** cuando al oferente que se encuentre primero en orden de mérito, cuando no cubra la fecha de necesidad del insumo y/o servicio requerido.
Las nuevas ofertas serán abiertas en el lugar, día y hora establecidos en el requerimiento, labrándose el Acta respectiva.
El silencio por parte del oferente invitado a mejorar se considerará como que mantiene su oferta.

13. Consultas:
Los interesados que deseen efectuar consultas al presente llamado o aclaraciones al pliego de orden técnico y/o administrativo, podrán realizarlas hasta la fecha fijada en las condiciones particulares por nota dirigida al ÁREA DE COMPRAS NACIONALES o ÁREA DE COMPRAS AL EXTERIOR, según corresponda, de CASA DE MONEDA, Av. Antártida Argentina N° 2085 – C1104ACH – Ciudad Autónoma de Buenos Aires – República Argentina o vía correo electrónico a cmcompras@casademoneda.gob.ar o importaciones@casademoneda.gob.ar.

14. Vista del expediente:
Podrá solicitarse la vista del expediente licitatorio en cualquier momento del procedimiento, salvo durante la etapa de evaluación de ofertas, que comprende desde el segundo día de la apertura de ofertas hasta el dictamen de pre-adjudicación. La toma de vista en ningún caso dará lugar a la suspensión de los trámites o demoras en el procedimiento licitatorio.

15. Facultades de S.E.C.M.:
a) SECM se reserva el derecho de solicitar documentación y/o muestras complementarias que considere pertinente.
b) SECM se reserva el derecho de solicitar mejora de condiciones, precios y plazos, luego de realizada la apertura de sobres.
c) SECM podrá dejar sin efecto el procedimiento de contratación en cualquier momento anterior al perfeccionamiento del contrato, sin lugar a reintegro de gastos e indemnización alguna en favor de los interesados u oferentes.
d) SECM verificará si el oferente se encuentra incorporado al Registro Público de Empleadores con Sanciones Laborales (REPSAL), reservándose el derecho de proceder a la adjudicación de quien se encuentre alcanzado por lo establecido en el Artículo 13 de la Ley N° 26.940 cuando razones de interés público debidamente justificadas así lo determinen.

16. Criterio para adjudicar:
La adjudicación deberá realizarse a favor de la oferta más conveniente para la SECM, teniendo en cuenta el precio, la calidad, la idoneidad del oferente y demás condiciones de la oferta, de acuerdo

con los criterios y parámetros de evaluación previstos en la documentación que rigió el procedimiento de selección.
Cuando se trate de la compra de un bien o de la contratación de un servicio estandarizado o uno de uso común cuyas características técnicas puedan ser inequívocamente especificadas e identificadas, se entenderá, en principio, por oferta más conveniente aquella de menor precio.
La adjudicación podrá realizarse por todos los renglones o por algunos de ellos, según lo que establezca el Pliego de Bases y Condiciones Particulares.
Cuando así se especifique en las Cláusulas Particulares, en la evaluación de las ofertas se tomará como criterio de preferencia las pautas establecidas en la Ley N° 27.437 de "Compre Argentino y Desarrollo de Proveedores.
La adjudicación será resuelta en forma fundada por la autoridad competente para aprobar la contratación y será notificada fehacientemente al adjudicatario y demás oferentes. Si se hubieran formulado impugnaciones contra el dictamen de evaluación de las ofertas, éstas serán resueltas en el mismo acto que disponga la adjudicación. La decisión sobre las impugnaciones no podrá volver a ser impugnada ante la SECM. Podrá adjudicarse aún cuando se haya presentado una sola oferta.

17. Perfeccionamiento del contrato:
Las contrataciones quedarán perfeccionadas mediante la notificación fehaciente de la Orden de Compra al adjudicatario, y/o la Suscripción del Contrato respectivo, según corresponda.
Si el adjudicatario no retirase la orden de compra, la rechazase o no suscribiese el contrato respectivo cuando así correspondiera, dentro de los 3 (tres) días de notificado, la SECM podrá adjudicar la contratación al oferente que siga en el orden de mérito y así sucesivamente, sin perjuicio de la aplicación de las penalidades respectivas.

18. Erogaciones a cargo del adjudicatario:
Será por cuenta del adjudicatario, el impuesto a los sellos de la Orden de Compra y/o contrato por el importe pertinente.

19. Entrega – Recepción:
a) Los adjudicatarios cumplirán la prestación en la forma, plazo o fecha, lugar y demás condiciones establecidas en los documentos que integran la contratación. Los plazos de entrega se computarán en días corridos a partir del día siguiente a la fecha de perfeccionamiento del contrato.
b) La recepción de los bienes y servicios tendrá carácter provisional y los recibos o remitos que firmen los funcionarios de SECM, quedarán sujetos a la recepción definitiva.
c) La recepción definitiva se otorgará dentro del plazo de 3 (tres) días, a contar de la fecha de entrega, salvo que la orden de compra y/o contrato especifiquen un plazo mayor.
d) La recepción definitiva no libera al adjudicatario de las responsabilidades emergentes de defectos de origen o vicios de fabricación que se adviertan con motivo del uso de los elementos entregados, durante un plazo de 6 (seis) meses contados a partir de la recepción definitiva. Salvo que por la índole de la contratación se fijara un término mayor en las cláusulas particulares o en las ofertas. En estos casos, el adjudicatario queda obligado a la reposición de los elementos en el plazo y lugar que se le indique.

e) Cuando se trate de mercaderías rechazadas, el adjudicatario será intimado a retirarlas dentro del plazo que se fije en cada oportunidad. Vencido el término establecido, quedarán en propiedad de SECM, sin derecho a reclamación alguna y sin cargo.
f) La conformidad se tendrá por prestada con la firma del funcionario de la dependencia interviniente, y ello implica que la adjudicataria ha dado cumplimiento al contrato.

20. Facturas y Pagos:

SECM establece como principio la modalidad de pago a 30 (treinta) días de recibida la factura y de la conformidad que corresponda. El plazo se interrumpirá si existieran observaciones sobre la documentación u otros trámites a cumplir, imputables al proveedor.

a) Los plazos se comenzarán a contar a partir del día siguiente al que se produzca la conformidad definitiva.
b) Si las facturas fueran presentadas con posterioridad a la fecha de conformidad definitiva, el plazo para el pago será computado desde la presentación de las mismas.
c) Los plazos de pago de órdenes de venta, se comenzarán a contar a partir de la fecha de la recepción de la comunicación pertinente y deberá ser en todo momento anterior al retiro de los elementos.
d) En caso de haberse aceptado el pago anticipado, deberá ser indefectiblemente avalado por una Póliza de Seguro de Caución o aval bancario que cubra el importe correspondiente más el IVA incluido, en caso de corresponder.
e) Los horarios de atención para el pago a proveedores en la Oficina de Tesorería son:
   Proveedores : lunes y jueves, 11:00 a 14:00 hs, interno 3452, mail cmproveedores@casademoneda.gob.ar
   Tesorería : lunes, miércoles y viernes, 11:00 a 15:00 hs, interno 3468, mail cmtesoreria@casademoneda.gob.ar

   Deberán presentar Certificado de Cuenta que deberá incluir:
   - Nombre del Banco donde esté radicada la cuenta
   - Denominación de cuenta
   - Tipo y número de cuenta
   - Sucursal.
   - C.U.I.T.
   - C.B.U.

   DE NO CONTAR CON ESTA INFORMACIÓN NO SE PODRÁN EFECTUAR LOS PAGOS.

Deberán emitir **Factura Electrónica** de acuerdo a lo normado por la R.G N° 4291/18 AFIP en la que conste:

a) número y fecha de la Orden de Compra o contrato a que corresponda;
b) número de expediente;
c) número y fecha de remitos de entrega;
d) número, especificación e importe de cada renglón facturado;
e) importe total bruto de la factura;
f) IVA y otros impuestos;
g) monto y tipo de descuentos, si correspondieran;
h) importe neto de la factura;

i) todo otro dato de interés que pueda facilitar su tramitación.
j) Las facturas presentadas en moneda extranjera serán liquidadas en pesos según cotización del Banco de la Nación Argentina tipo vendedor del día anterior al efectivo pago.
k) Deberán emitir Factura Electrónica **en la misma moneda de la Orden de Compra**.
l) Las facturas deberán ser entregadas en Mesa de Entradas o enviadas vía e-mail a cmproveedores@casademoneda.gob.ar para que se considere válida su recepción.

21. Aumentos y Prórrogas:
En oportunidad del dictamen de evaluación, al dictarse el acto de adjudicación, o durante la ejecución de la orden de compra y hasta 3 (tres) meses de cumplida la misma, SECM podrá:

a) Aumentar o disminuir el total adjudicado hasta un veinte por 20% (veinte por ciento) de su valor original en uno y otro caso, en las condiciones y precios pactados y con adecuación de los plazos respectivos. El aumento o la disminución podrá incidir sobre uno, varios o el total de los renglones de la Orden de Compra y/o Contrato, siempre y cuando el total resultante no exceda el porcentaje mencionado.

b) En los casos que resulte imprescindible para la SECM, el aumento o disminución podrá exceder el veinte 20% (veinte por ciento) y deberá requerir la conformidad del cocontratante Si esta no fuera aceptada, no generará ningún tipo de responsabilidad al adjudicatario ni será pasible de ningún tipo de penalidad o sanción.

En ningún caso las ampliaciones o disminuciones podrán exceder el 35 % (treinta y cinco por ciento) del monto total del contrato, aún con el consentimiento del cocontratante.

c) Cuando por la naturaleza de la prestación exista imposibilidad de fraccionar las unidades para entregar la cantidad exacta contratada, las entregas podrán ser aceptadas en más o en menos, según lo permita el mínimo fraccionable. Estas diferencias serán aumentadas o disminuidas del monto de la facturación correspondiente, sin otro requisito.

e) Prorrogar los contratos, en las condiciones pactadas originalmente, por un máximo de 120 (ciento veinte) días. La prórroga deberá ser comunicada al proveedor durante la vigencia del contrato.

f) A pedido de la Gerencia requirente conveniencia de SECM, la Gerencia de Compras podrá, extender la fecha de vencimiento de la orden de compra a efectos de consumir las cantidades pendientes de utilización. Si dicha extensión fuese igual o inferior a 30 (treinta) días, bastará con la comunicación al proveedor para hacerla efectiva. Si fuese superior, quedará supeditada a la aceptación del adjudicatario. En ningún caso la extensión podrá superar los 120 (ciento veinte) días.

22. Transferencia y cesión del contrato:

No podrá ser transferido ni cedido por el adjudicatario sin la previa autorización fundada de la autoridad competente. En caso contrario el contrato se podrá dar por rescindido de pleno derecho. El adjudicatario, continuará obligado solidariamente con el cesionario por los compromisos emergentes del contrato.

Dicha transferencia o cesión, de producirse, deberá seguir el mismo criterio de publicidad y difusión aplicado para la adjudicación original.

23. Rescisión contractual - Facultad de SECM:

En caso de incumplimiento total o parcial, SECM podrá optar entre exigir el cumplimiento del contrato o hacerlo ejecutar por un tercero por cuenta del adjudicatario. Este, además responderá por los daños y perjuicios que se ocasionen a la SECM.

Rescindido el contrato por culpa del adjudicatario, éste perderá la garantía, responderá por los daños y perjuicios resultantes y será pasible de las consecuencias jurídicas previstas en el Reglamento de Contrataciones de SECM y en la respectiva contratación.

La revocación, modificación o sustitución de los contratos por razones de oportunidad, mérito o conveniencia, no generará derecho a indemnización en concepto de lucro cesante, sino únicamente a la indemnización del daño emergente, que resulte debidamente acreditado.

SECM se reserva el derecho de interrumpir un contrato en cualquier momento en que se encuentre con previo aviso de la acción a realizar con 30 (treinta) días de antelación.

Se podrá rescindir el contrato de común acuerdo con el proveedor cuando el interés público comprometido al momento de realizar la contratación hubiese variado y el cocontratante prestare su conformidad. Estos casos no darán derecho a indemnización alguna para las partes, sin perjuicio de los efectos cumplidos hasta la extinción del vínculo contractual.

24. Penalidades y sanciones:

Los oferentes o cocontratantes podrán ser pasibles de las penalidades y sanciones establecidas en el Capítulo XIV del Reglamento de Contrataciones de SECM, sin perjuicio de las multas contempladas, en su caso, en las Condiciones Particulares.

ALVAREZ

DECLARACIÓN JURADA DE INTERESES - DECRETO 202/2017

Tipo de declarante: Persona Jurídica

Razón Social	
CUIT	

Vínculos a declarar

¿La persona física declarante tiene vinculación con los funcionarios enunciados en los artículos 1 y 2 del Decreto n° 202/17?

(Marque con una X donde corresponda)

SI		NO	
En caso de existir vinculaciones con más de un funcionario, se deberá repetir la información que a continuación se solicita por cada una de las vinculaciones a declarar.		La opción elegida en cuanto a la no declaración de vinculaciones implica la declaración expresa de la inexistencia de los mismos, en los términos del Decreto n° 202/17.	

Vínculo

Persona con el vínculo

(Marque con una X donde corresponda y brinde la información adicional requerida para el tipo de vínculo elegido)

Persona jurídica (si el vínculo a declarar es directo de la persona jurídica declarante)		No se exige información adicional
Representante legal		Detalle nombres apellidos y CUIT
Sociedad controlante		Detalle Razón Social y CUIT
Sociedades controladas		Detalle Razón Social y CUIT
Sociedades con interés directo en los resultados económicos o financieros de la declarante		Detalle Razón Social y CUIT
Director		Detalle nombres apellidos y CUIT
Socio o accionista con participación en la formación de la voluntad social		Detalle nombres apellidos y CUIT
Accionista o socio con más del 5% del capital social de las sociedades sujetas a oferta pública		Detalle nombres apellidos y CUIT

Información Adicional

¿Con cuál de los siguientes funcionarios?
(Marque con una X donde corresponda)

Presidente	
Vicepresidente	
Jefe de Gabinete de Ministros	
Ministro	
Autoridad con rango de ministro en el Poder Ejecutivo Nacional	
Autoridad con rango inferior a Ministro con capacidad para decidir	

(En caso de haber marcado Ministro, Autoridad con rango de ministro en el Poder Ejecutivo Nacional o Autoridad con rango inferior a Ministro con capacidad para decidir complete los siguientes campos)

Nombres	
Apellidos	
CUIT	
Cargo	
Jurisdicción	

Tipo de vínculo
(Marque con una X donde corresponda y brinde la información adicional requerida para el tipo de vínculo elegido)

Sociedad o comunidad		Detalle Razón Social y CUIT.
Parentesco por consanguinidad dentro del cuarto grado y segundo de afinidad		Detalle qué parentesco existe concretamente.
Pleito pendiente		Proporcione carátula, nº de expediente, fuero, jurisdicción, juzgado y secretaría intervinientes.
Ser deudor		Indicar motivo de deuda y monto.
Ser acreedor		Indicar motivo de acreencia y monto.
Haber recibido beneficios de importancia de parte del funcionario		Indicar tipo de beneficio y monto estimado.

Información adicional

La no declaración de vinculaciones implica la declaración expresa de la inexistencia de los mismos, en los términos del Decreto n° 202/17.

Firma

Aclaración

Fecha y lugar

DECLARACIÓN JURADA DE INTERESES - DECRETO 202/2017

Tipo de declarante: Persona física

Nombres	
Apellidos	
CUIT	

Vínculos a declarar

¿La persona física declarante tiene vinculación con los funcionarios enunciados en los artículos 1 y 2 del Decreto n° 202/17?

(Marque con una X donde corresponda)

SI		NO	
En caso de existir vinculaciones con más de un funcionario, se deberá repetir la información que a continuación se solicita, por cada una de las vinculaciones a declarar.		La opción elegida en cuanto a la no declaración de vinculaciones implica la declaración expresa de la inexistencia de los mismos, en los términos del Decreto n° 202/17.	

Vínculo

¿Con cuál de los siguientes funcionarios?

(Marque con una X donde corresponda)

Presidente	
Vicepresidente	
Jefe de Gabinete de Ministros	
Ministro	
Autoridad con rango de ministro en el Poder Ejecutivo Nacional	
Autoridad con rango inferior a Ministro con capacidad para decidir	

(En caso de haber marcado Ministro, Autoridad con rango de ministro en el Poder Ejecutivo Nacional o Autoridad con rango inferior a Ministro con capacidad para decidir complete los siguientes campos)

Nombres	
Apellidos	
CUIT	
Cargo	
Jurisdicción	

Tipo de vínculo

(Marque con una X donde corresponda y brinde la información adicional requerida para el tipo de vínculo elegido)

Sociedad o comunidad		Detalle Razón Social y CUIT.
Parentesco por consanguinidad dentro del cuarto grado y segundo de afinidad		Detalle qué parentesco existe concretamente.
Pleito pendiente		Proporcione carátula, nº de expediente, fuero, jurisdicción, juzgado y secretaría intervinientes.
Ser deudor		Indicar motivo de deuda y monto.
Ser acreedor		Indicar motivo de acreencia y monto.
Haber recibido beneficios de importancia de parte del funcionario		Indicar tipo de beneficio y monto estimado.
Amistad pública que se manifieste por gran familiaridad y frecuencia en el trato		No se exige información adicional

Información adicional

La no declaración de vinculaciones implica la declaración expresa de la inexistencia de los mismos, en los términos del Decreto n° 202/17.

Firma

Aclaración

Fecha y lugar

Complemento del Decreto N° 202/2017 –

Resolución 11-E/2017

En cumplimiento del Artículo 1, que reza, "*Las autoridades convocantes deberán informar en cada procedimiento los nombres y cargos de los funcionarios con competencia o capacidad de decisión sobre la contratación o acto correspondiente*", SECM informa:

Monto Total de la Compra / Venta (con IVA)	**Funcionarios Autorizantes**
Más de $ 15.000.000	Directorio Rodolfo Gabrielli –Andrés Vasiliadis
Más de $5.000.000 y hasta $ 15.000.000	Presidente – Rodolfo Gabrielli
Más de $2.500.000 y hasta $ 5.000.000	Gerente General de Administración Anastasia Adem
Hasta $ 2.500.000	Gerente de Compras – Andrea Lapadula