DIRECCION GENERAL DE ADMINISTRACION Y FINANZAS

DIRECCION ADMINISTRATIVA

Asunción, 23 de Junio de 2023

NOTA D.A. N° 167 /2023.

C.P Patricia González Burgos, Directora
Dirección Operativa de Contrataciones
Ministerio de Salud Pública y Bienestar Social
Presente:

Me dirijo a Ud., en referencia al Contrato N° 117/2023 de la LPN N° 36/2023- Adquisición de Renovación de Software de Seguridad, Control de Punto Final, Detección y Respuesta ante Incidentes y Protección de Correo Electrónico para el MSP y BS-Plurianual- ID N° 422.466 adjudicado a la firma Corporación Sekiura SACEI

Fundamento:

Que, la Dirección Administrativa en su carácter del Administrador del Contrato suscripto con la firma Sekiura SACEI, en fecha 15 de Junio/2023, solicita Adenda al Contrato, en el **Punto N° 5**- Precio Unitario y el Importe totala pagar por los bienes .

Donde dice:

ITEM	DESCRIPCION DEL BIEN	U.DE MEDIDA	PRESENTACION	CANT	MARCA	PROCED	PRECIO UNITARIO IVA INCLUIDO	MONTTOTAL-IVA INCLUIDO
1	ANTIVIRUS CORPORATIVO CON ANTISPYWARE Y ANTISPAM	UNIDAD	UNIDAD	2.000	KASPERSKY	REINO UNIDO	1.798.863	1.435.000.000
2	SERVICIO TECNICO DE SOPORTE PARA EQUIPOS INFORMATICOS	UNIDAD	UNIDAD	1	SEKIURA	PARAGUAY	16.671465	1.200.000.000
			MONTO TOTAL-IVA INCLUIDO					2.635.000.000

Debe decir:

ITEM	DESCRIPCION DEL BIEN	U.DE MEDIDA	PRESENTACION	CANT	MARCA	PROCED	PRECIO UNITARIO IVA INCLUIDO	MONTTOTAL-IVA INCLUIDO
1	ANTIVIRUS CORPORATIVO CON ANTISPYWARE Y ANTISPAM	UNIDAD	UNIDAD	2.000	KASPERSKY	REINO UNIDO	717.500	1.435.000.000
2	SERVICIO TECNICO DE SOPORTE PARA EQUIPOS INFORMATICOS	UNIDAD	UNIDAD	1	SEKIURA	PARAGUAY	1.200.000.000	1.200.000.000
			MONTO TOTAL-IVA INCLUIDO					2.635.000.000

Teniendo en cuenta el error visualizado en los precios unitarios y totales de lo Items adjudicados, se realiza la presente solicitud.
Lo solicitado no afecta derechos de terceros, considerando que el presente proceso fue producto de un llamado que ha cumplido con cada una de las formalidades prevista en la Ley N° 2051/03, sus modificaciones y decretos reglamentarios.

Que, no se alteran la naturaleza ni finalidad del Contrato.
Para los fines pertinentes.

MINISTERIO DE SALUD PÚBLICA Y BIENESTAR SOCIAL DIRECCIÓN ADMINISTRATIVA REPÚBLICA DEL PARAGUAY

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa - D.G.A.F.

Teléf.: 201-509
Central 204-601/3 Interno N° 310
Brasil N° 1288 y Silvio Pettirossi

SEKIURA
Expertos en seguridad informatica

CORPORATION SEKIURA S.A.C.E.I.
Tel.: (+595) 21 608 515 R.A.
www.sekiura.com.py

Asunción, 23 de junio de 2023

Señores:
Ministerio de Salud Pública y Bienestar Social
Atención: Abg. Héctor Fernández
Jefe del Departamento de Ejecución de Contratos y Garantías – D.A.
Presente

De nuestra mayor consideración, nos dirigimos a ustedes, con el fin de dar respuesta a la NOTA DEC Nº 81/2023 en el marco de LPN Nº 36/2023 "ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCION DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM - PLURIANUAL" ID Nº 422.466, por lo tanto, manifestamos nuestra conformidad para la adenda al Contrato en el punto 5.

Se expide esta nota a pedido del interesado, para lo que hubiere lugar.

Desde ya muchas gracias y sin otro particular me despido cordialmente. -

Nélida Rafaela Aponte de Fischer
Representante Legal
Corporation Sekiura S.A.C.E.I.
C.I Nº 397.359

CORPORATION SEKIURA S.A.C.E.I. RUC Nº 80070689-0

Ministerio de Salud Pública y Bienestar Social
Dirección Administrativa
DEPARTAMENTO DE EJECUCION DE CONTRATOS
Nº..... Fecha: 23 JUN 2023
Hora: 9:17 Firma:

Elsa R. Cáceres
Dpto. de Ejecución de Contratos
M.S.P. y B.S.

DPTO. DE EJECUCIÓN DE CONTRATOS
DERIVAR A:
☑ SECCION GESTION DE CONTROL DE ORDENES
☐ SECCION DE VERIFICACION
☐ SECCION DE CUMPLIMIENTO CONTRACTUAL
PARA SEGUIR PROCESO

Abg. Héctor Fernández, Jefe
Dpto. de Ejecución de Contratos - D.A.
M.S.P. y B.S.

kaspersky WatchGuard Barracuda SONICWALL IBM NETSCOUT ENDPOINT PROTECTOR imperva
FORCEPOINT TREND MICRO Extreme ipswitch WhatsUpGold Ruckus VERTIV. VEEAM CYBERARK

Escaneado con CamScanner

Asunción, 23 de Junio de 2023

NOTA DEC N° 81/2023

Señores
Corporación Sekiura SACEI
Avda. Boggiani c/ R.I 5 Gral. Diaz
Asunción

De mi Mayor Consideración:

Me dirijo a Uds. En referencia a su adjudicación en el marco de la LPN N° 36/2023 – Adquisición de Renovación de Software de Seguridad, Control de Punto Final, Detección y respuesta ante incidentes y protección de Correo Electrónico para el MSP y BS- ID N° 422.466, a los efectos de solicitar su Nota de Conformidad para Adenda al Contrato

***Punto 5* del Contrato- Precio Unitario y El importe a pagar por los bienes**

Items adjudicados N° 1 y 2- Se visualiza error en los precios unitarios y totales.

Esperando una respuesta favorable.

Atentamente

MINISTERIO DE SALUD PÚBLICA Y BIENESTAR SOCIAL
DEPARTAMENTO DE EJECUCIÓN DE CONTRATOS

Ing. Hector Fernández, Jefe
Depto. de Ejecución de Contratos-D.A

NDGAF – D.A

CONTRATO Nº 117/2023

LPN N° 36/2023 "ADQUISICIÓN DE RENOVACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRONICO PARA EL MSPYBS" – PLURIANUAL – ID N° 422.466

ENTRE EL MINISTERIO DE SALUD PÚBLICA Y BIENESTAR SOCIAL Y FIRMA CORPORATION SEKIURA S.A.C.E.I.

Entre el MINISTERIO DE SALUD PUBLICA Y BIENESTAR SOCIAL, domiciliado en Brasil e/ Pettirossi de la ciudad de Asunción, República del Paraguay, representado para este acto por el **Sr. Rodrigo Marcial Sánchez Araujo**, con Cédula de Identidad N° 1.589.364, Director de la Dirección Administrativa, dependiente de la Dirección General de Administración y Finanzas, nombrado por Resolución D.G.RR.HH Nº 04, de fecha 10 de Marzo de 2021, facultado a suscribir el presente contrato por Resolución D.G.A.F. Nº 320, de fecha 28 de Febrero de 2023, denominado en adelante la **CONTRATANTE,** por una parte y por la otra la Firma **CORPORATION SEKIURA S.A.C.E.I., RUC 80070889-0,** domiciliada en Avda. Boggiani 6212 c/ RI5 Gral. Díaz, ciudad de Asunción, República del Paraguay, representado para este acto por la **Sra. Nélida Rafaela Aponte de Fischer**, con Cédula de Identidad N° 397.359, según Constitución de Sociedad otorgado por el Escribano Edgar Caballero Recalde con Reg. N° 621, Esc. N° 29 y Acta de asamblea General N° 11, denominada en adelante la CONTRATISTA, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente contrato para la ADQUISICIÓN DE RENOVACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRONICO PARA EL MSPYBS – PLURIANUAL, el cual estará sujeto a las siguientes cláusulas y condiciones.

1. OBJETO.
"ADQUISICIÓN DE RENOVACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRONICO PARA EL MSPYBS - PLURIANUAL".-

2. DOCUMENTOS INTEGRANTES DEL CONTRATO
Los documentos contractuales firmados por las partes y que forman parte integral del contrato son los siguientes:
a) Contrato;
b) El Pliego de Bases y Condiciones, sus adendas y modificaciones;
c) Los datos cargados en el SICP (IAO);
d) La oferta del proveedor;
e) La resolución de adjudicación del contrato emitida por la convocante y su respectiva notificación;

Los documentos que forman parte del Contrato deberán considerarse mutuamente explicativos; en caso de contradicción o diferencia entre los mismos, la prioridad de los mismos será en el orden enunciado anteriormente.

3. IDENTIFICACIÓN DEL CRÉDITO PRESUPUESTARIO PARA CUBRIR EL COMPROMISO DERIVADO DEL CONTRATO.
El crédito presupuestario para cubrir el compromiso derivado del presente Contrato está previsto conforme al Certificado de Disponibilidad Presupuestaria vinculado al Programa Anual de Contrataciones (PAC) con el **ID N° 422.466.-**

El saldo estará supeditado al Presupuesto General de Gastos de la Nación, asignado al Ministerio de Salud Pública y Bienestar Social para el Ejercicio Fiscal 2024.-

4. PROCEDIMIENTO DE CONTRATACIÓN
El presente Contrato es el resultado del procedimiento de la LPN N° 36/2023 "ADQUISICIÓN DE RENOVACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRONICO PARA EL MSPYBS - PLURIANUAL", convocado por la Dirección Operativa de Contrataciones. La adjudicación fue realizada según Resolución D.G.A.F. Nº 320, de fecha 28 de Febrero de 2023.

5. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES.
El importe total a pagar por los bienes, conforme a la Resolución de Adjudicación y a la oferta presentada asciende a un monto total de **G. 2.635.000.000** (Guaraníes Dos Mil Seiscientos Treinta y Cinco Millones), según el siguiente cuadro:

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

Nélida R. Aponte de Fischer
CORPORATION SEKIURA S.A.C.E.I.
RUC Nº 80070889-0

ÍTEM	DESCRIPCIÓN DEL BIEN	UNIDAD DE MEDIDA	PRESENTACIÓN	CANT.	MARCA	PROCED.	PRECIO UNITARIO (IVA INCLUÍDO)	MONTO TOTAL – IVA INCLUIDO
1	ANTIVIRUS CORPORATIVO CON ANTISPYWARE Y ANTISPAM	UNIDAD	UNIDAD	2.000	KASPERSKY	REINO UNIDO	1.798.863	1.435.000.000
2	SERVICIO TÉCNICO/ SOPORTE PARA EQUIPOS INFORMÁTICOS	UNIDAD	UNIDAD	1	SEKIURA	PARAGUAY	16.671.465	1.200.000.000
MONTO TOTAL – IVA INCLUIDO								2.635.000.000

ESPECIFICACIONES TÉCNICAS: Los bienes deberán cumplir con las siguientes Especificaciones Técnicas y Normas:

ITEM	DESCRIPCIÓN
1	LICENCIAS ANTIVIRUS KASPERSKY CON SUPORTE TÉCNICO 24/7 X 3 AÑOS UPS - VER ESPECIFICACIONES TÉCNICAS
2	SERVICIO TÉCNICO PARA LA INSTALACIÓN, IMPLEMENTACIÓN Y DESPLIEGUE DE LA SOLUCIÓN, 1 EN EL MSPBS Y EN 5 HOSPITALES REGIONALES DEL MSPBS SWITCH - VER ESPECIFICACIONES TÉCNICAS

ÍTEM 1 UPS	ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS
MARCA	Kaspersky
CANTIDAD	2000 (dos mil)
VIGENCIA	El proveedor deberá entregar licencias con vigencia de 36 meses.

1. SERVIDOR DE ADMINISTRACIÓN Y CONSOLA ADMINISTRATIVA	1. Compatibilidad: 1. Microsoft Windows 10 20H2 32 bits o 64 bits (versiones 12.2 en adelante). 2. Microsoft Windows 10 20H1 32 bits o 64 bits (versiones 12.1 en adelante). 3. Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits. 4. Microsoft Windows 10 Enterprise 2016 LTSB 32 bits / 64 bits. 5. Microsoft Windows 10 Enterprise 2015 LTSB 32 bits / 64 bits. 6. Microsoft Windows 10 Pro RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 7. Microsoft Windows 10 Pro para estaciones de trabajo RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 8. Microsoft Windows 10 Enterprise RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 9. Microsoft Windows 10 Education RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 10. Microsoft Windows 10 Pro 19H1 32 bits / 64 bits. 11. Microsoft Windows 10 Pro for Workstations 19H1 32 bits / 64 bits. 12. Microsoft Windows 10 Enterprise 19H1 32 bits / 64 bits 13. Microsoft Windows 10 Education 19H1 32 bits / 64 bits. 14. Microsoft Windows 10 Pro 19H2 32 bits / 64 bits. 15. Microsoft Windows 10 Pro for Workstations 19H2 32 bits / 64 bits. 16. Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits. 17. Microsoft Windows 10 Education 19H2 32 bits / 64 bits. 18. Microsoft Windows 8.1 Pro 32 bits / 64 bits. 19. Microsoft Windows 8.1 Enterprise 32 bits / 64 bits. 20. Microsoft Windows 8 Pro 32 bits / 64 bits. 21. Microsoft Windows 8 Enterprise 32 bits / 64 bits. 22. Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores 32 bits / 64 bits. 23. Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 y versiones posteriores 32 bits / 64 bits. 24. Windows Server 2019 Standard 64 bits. 25. Windows Server 2019 Core 64 bits. 26. Windows Server 2019 Datacenter 64 bits. 27. Windows Server 2016 Server Standard RS3 (v1709) (LTSB / CBB) 64 bits. 28. Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB / CBB) 64 bits. 29. Windows Server 2016 Server Core RS3 (v1709) 30. Windows Server 2016 Standard (LTSB) 64 bits. 31. Windows Server 2016 Server Core 32. Windows Server 2016 Datacenter (LTSB) 64 bits. 33. Windows Server 2012 R2 Standard 64 bits. 34. Windows Server 2012 R2 Server Core 64 bits. 35. Windows Server 2012 R2 Foundation 64 bits. 36. Windows Server 2012 R2 Essentials 64 bits. 37. Windows Server 2012 R2 Datacenter 64 bits. 38. Windows Server 2012 Standard 64 bits.

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

CORPORATION SEKIURA S.A.C.E.I.
RUC N° 80070889-0

	39. Windows Server 2012 Server Core 64 bits. 40. Windows Server 2012 Foundation 64 bits. 41. Windows Server 2012 Essentials 64 bits. 42. Windows Server 2012 Datacenter 64 bits. 43. Windows Storage Server 2016 64 bits. 44. Windows Storage Server 2012 R2 64 bits. 45. Windows Storage Server 201
2.CARACTERISTICAS	2.1.1. Se debe acceder a la consola vía WEB (HTTPS) o MMC; 2.1.2. Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidades 2.1.3. Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus; 2.1.4. Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory; 2.1.5. Capacidad de instalar remotamente la solución de seguridad en smartphones y Android, utilizando estaciones como intermediadoras; 2.1.6. Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets de sistema iOS; 2.1.7. Capacidad de instalar remotamente cualquier app en smartphones y tablets de sistema iOS; 2.1.8. Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus; 2.1.9. Capacidad de gestionar smartphones y tablets (tanto Symbian como Windows Mobile, BlackBerry, Android y iOS) protegidos por la solución antivirus; 2.1.10. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto; 2.1.11. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas; 2.1.12. Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes; 2.1.13. Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes; 2.1.14. Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores; 2.1.15. Capacidad de importar la estructura de Active Directory para encontrar máquinas; 2.1.16. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección; 2.1.17. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección; 2.1.18. Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente; 2.1.19. Capacidad de agrupamiento de máquinas por caracteristicas comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.; 2.1.20. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos; 2.1.21. Debe proporcionar las siguientes informaciones de las computadoras: 2.1.21.1. Si el antivirus está instalado; 2.1.21.2. Si el antivirus ha iniciado; 2.1.21.3. Si el antivirus está actualizado; 2.1.21.4. Minutos/horas desde la última conexión de la máquina con el servidor administrativo; 2.1.21.5. Minutos/horas desde la última actualización de vacunas 2.1.21.6. Fecha y horario de la última verificación ejecutada en la máquina; 2.1.21.7. Versión del antivirus instalado en la máquina; 2.1.21.8. Si es necesario reiniciar la computadora para aplicar cambios; 2.1.21.9. Fecha y horario de cuando la máquina fue encendida; 2.1.21.10. Cantidad de virus encontrados (contador) en la máquina; 2.1.21.11. Nombre de la computadora; 2.1.21.12. Dominio o grupo de trabajo de la computadora; 2.1.21.13. Fecha y horario de la última actualización de vacunas; 2.1.21.14. Sistema operativo con Service Pack; 2.1.21.15. Cantidad de procesadores; 2.1.21.16. Cantidad de memoria RAM; 2.1.21.17. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory) 2.1.21.18. Dirección IP; 2.1.21.19. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido. 2.1.21.20. Actualizaciones de Windows Updates instaladas. 2.1.21.21. Información completa de hardware conteniendo: procesadores, memoria, adaptadores

CORPORATION SEKUAA S.A.C.E.I. RUC N° 80070839-0

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

	de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD 2.1.21.22. Vulnerabilidades de aplicativos instalados en la máquina 2.1.22. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas; 2.1.23. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como: 2.1.23.1. Cambio de gateway; 2.1.23.2. Cambio de subnet DNS; 2.1.23.3. Cambio de dominio; 2.1.23.4. Cambio de servidor DHCP; 2.1.23.5. Cambio de servidor DNS; 2.1.23.6. Cambio de servidor WINS; 2.1.23.7. Aparición de nueva subnet; 2.1.24. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet; 2.1.25. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes; 2.1.26. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus; 2.1.27. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos; 2.1.28. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paqueles de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red; 2.1.29. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo. 2.1.30. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML. 2.1.31. Capacidad de generar traps SNMP para monitoreo de eventos; 2.1.32. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento; 2.1.33. Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server; 2.1.34. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo). 2.1.35. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor); 2.1.36. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo); 2.1.37. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes; 2.1.38. Capacidad de reportar vulnerabilidades de software presentes en las computadoras. 2.1.39. Capacidad de realizar inventario de hardware de todas las máquinas clientes; 2.1.40. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes; 2.1.41. Capacidad de diferenciar máquinas virtuales de máquinas físicas;
3. ESTACIONES WINDOWS	3.1. Compatibilidad: 3.1.1. Windows 10 3.1.2. Windows 8.1 3.1.3. Windows 8 3.1.4. Windows 7 todas las versiones con o sin Service Pack 1 o superior 3.1.5. Windows XP Embedded SP3 (32 bits) 3.1.6. Windows Embedded POSReady 2009 (32 bits) 3.1.7. Windows Embedded Standard 7 SP1 (32 bits, 64 bits) 3.1.8. Windows Embedded Enterprise 7 SP1 (32 bits, 64 bits) 3.1.9. Windows Embedded POSReady 7 (32 bits, 64 bits) 3.1.10. Estándar de Windows Embedded 8.0 (32 bits, 64 bits) 3.1.11. Windows Embedded 8.1 Industry Professional/Empresarial (32 bits, 64 bits) 3.1.12. Windows 10 IoT Enterprise (32 bits, 64 bits) 3.1.13. Windows XP Professional SP2 / SP3 (32 bits) 3.2. Características: 3.2.1. Debe proporcionar las siguientes protecciones: 3.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías, etc.) que verifique cualquier archivo creado, accedido o modificado; 3.2.1.2. Antivirus de web (módulo para verificación de sitios y downloads contra virus) 3.2.1.3. Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) 3.2.1.4. Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc.) 3.2.1.5. Firewall con IDS 3.2.1.6. Autoprotección (contra ataques a los servicios/procesos del antivirus) 3.2.1.7. Control de dispositivos externos 3.2.1.8. Control de acceso a sitios por categoría.

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

SEKIURA CORPORATION S.A.C.E.I. RUC Nº 80070889-0

3.2.1.9. Control de ejecución de aplicativos
3.2.1.10. Control de vulnerabilidades de Windows y de los aplicativos instalados
3.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en instalación remota;
3.2.3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
3.2.4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución;
3.2.5. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
3.2.6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;
3.2.7. Capacidad de agregar aplicativos a una lista de aplicativos confiables, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;
3.2.8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
3.2.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
3.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
3.2.11. Capacidad de verificar solamente archivos nuevos y modificados;
3.2.12. Capacidad de verificar objetos usando heurística;
3.2.13. Capacidad de agendar una pausa en la verificación;
3.2.14. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
3.2.15. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
3.2.15.1. Preguntar qué hacer, o;
3.2.15.2. Bloquear el acceso al objeto;
3.2.15.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
3.2.15.2.2. Caso positivo de desinfección:
3.2.15.2.2.1. Recuperar el objeto para uso;
3.2.15.2.3. Caso negativo de desinfección:
3.2.15.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
3.2.16. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
3.2.17. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
3.2.18. Capacidad de verificar tráfico de ICQ, MSN, AIM y IRC contra virus y enlaces phishings;
3.2.19. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings;
3.2.20. Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Firefox y Opera;
3.2.21. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;
3.2.22. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
3.2.22.1. Preguntar qué hacer, o;
3.2.22.2. Bloquear el correo electrónico;
3.2.22.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
3.2.22.2.2. Caso positivo de desinfección:
3.2.22.2.2.1. Recuperar el correo electrónico al usuario;
3.2.22.2.3. Caso negativo de desinfección:
3.2.22.2.3.1. Mover a cuarentena o borrar el objeto (de acuerdo con la configuración preestablecida por el administrador);
3.2.23. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
3.2.24. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
3.2.25. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
3.2.26. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.) usando heurísticas;
3.2.27. Debe tener soporte total al protocolo IPv6;
3.2.28. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico;
3.2.29. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
3.2.29.1. Preguntar qué hacer, o;
3.2.29.2. Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o;
3.2.29.3. Permitir acceso al objeto;
3.2.30. El antivirus de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:
3.2.30.1. Verificación on-the-fly, donde los datos se verifican mientras son recibidos en tiempo real, o;

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

CORPORATION SEKIURA S.A.C.E.I.
RUC Nº 80070889-0

	3.2.30.2. Verificación de buffer, donde los datos se reciben y son almacenados para posterior verificación. 3.2.31. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web. 3.2.32. Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas. 3.2.33. Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa. 3.2.34. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas. 3.2.35. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-PhishingWorkingGroup (http://www.antiphishing.org/). 3.2.36. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica; 3.2.37. Debe tener módulo IDS (IntrusionDetectionSystem) para protección contra portscans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas. 3.2.38. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas: 3.2.38.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas; 3.2.38.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. 3.2.39. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo: 3.2.39.1. Discos de almacenamiento locales 3.2.39.2. Almacenamiento extraíble 3.2.39.3. Impresoras 3.2.39.4. CD/DVD 3.2.39.5. Drives de disquete 3.2.39.6. Modems 3.2.39.7. Dispositivos de cinta 3.2.39.8. Dispositivos multifuncionales 3.2.39.9. Lectores de smart card 3.2.39.10. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.) 3.2.39.11. Wi-Fi 3.2.39.12. Adaptadores de red externos 3.2.39.13. Dispositivos MP3 o smartphones 3.2.39.14. Dispositivos Bluetooth 3.2.40. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario. 3.2.41. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario. 3.2.42. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento. 3.2.43. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID 3.2.44. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento. 3.2.45. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc.). 3.2.46. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo. 3.2.47. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo. 3.2.48. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web. 3.2.49. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web. 3.2.50. Capacidad de funcionar de forma eficaz incluso con hardware de gama baja (desde 256 MB de RAM y CPU Pentium III) y software antiguo (desde Windows XP) sin riesgo de sobrecargar los sistemas 3.2.51. Supervisión de la integridad del sistema. 3.2.52. Supervisión de la integridad de archivos: Capacidad de realizar el seguimiento de las acciones llevadas a cabo por los archivos y las carpetas especificados dentro de un marco determinado. Además, de poder configurarse que se realice el seguimiento de las modificaciones durante los períodos en los que la supervisión se interrumpe. 3.2.53. Inspección de registros: Capacidad de supervisar las posibles infracciones en relación con la protección mediante la inspección de los registros de eventos de Windows. Posibilidad de que la aplicación envíe una notificación al administrador cuando detecte comportamientos anormales que

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

CORPORATION SEKIURA S.A.C.E.I
RUC N° 80070589-0

	pueden indicar un intento de ciberataque
4. ESTACIONES Y SERVIDORES MAC OS X	4.1. Compatibilidad: 4.1.1. Mac OS X 10.12 o superior 4.1.2. Mac OS X Server 10.9 o superior 4.2. Características: 4.2.1. Debe proporcionar protección residente para archivos (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado; 4.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota; 4.2.3. La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione en toda su capacidad; 4.2.4. Debe contar con soportes a notificaciones utilizando Growl; 4.2.5. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo). 4.2.6. Capacidad de volver a la base de datos de la vacuna anterior; 4.2.7. Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas; 4.2.8. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado; 4.2.9. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks); 4.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 4.2.11. Capacidad de verificar solamente archivos nuevos y modificados; 4.2.12. Capacidad de verificar objetos usando heurística; 4.2.13. Capacidad de agendar una pausa en la verificación; 4.2.14. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 4.2.14.1. Preguntar qué hacer, o; 4.2.14.2. Bloquear el acceso al objeto; 4.2.14.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 4.2.14.2.2. Caso positivo de desinfección: 4.2.14.2.2.1. Recuperar el objeto para uso; 4.2.14.2.3. Caso negativo de desinfección: 4.2.14.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 4.2.15. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto; 4.2.16. Capacidad de verificar archivos de formato de correo electrónico; 4.2.17. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antivirus e iniciar el antivirus por la línea de comando; 4.2.18. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión;
5. ESTACIONES DE TRABAJO LINUX	5.1. Compatibilidad: 5.1.1. Debian GNU / Linux 8.9 o superior, x86 / x64 5.1.2. Ubuntu 16.04 LTS o superior, x86 / x64 5.1.3. Linux Mint 18.2 o superior, x86 / x64 5.1.4. ALT, x86 / x64 5.1.5. GosLinux 6.6 o superior, x86 / x64 5.1.6. Mageia 4, x86 5.1.7. Amazon Linux AMI, x64 5.1.8. Astra Linux, x64 5.1.9. OS ROSA Cobalt, x64 5.1.10. AlterOS 7.5 o superior, x64 5.1.11. Pardus OS 19.1 o superior, x64 5.2. Características: 5.2.1. Debe proporcionar las siguientes protecciones: 5.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 5.2.1.2. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 5.2.2. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 5.2.2.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 5.2.2.2. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes; 5.2.2.3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena; 5.2.2.4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado), análisis de archivos; desinfección o eliminación de objetos

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

CORPORATION SEKURA S.A.C.E.I. RUC N° 80070589-0

	infectados. 5.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software; 5.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 5.2.5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 5.2.6. Capacidad de verificar objetos usando heurística; 5.2.7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 5.2.8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 5.2.9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)
6. SERVIDORES WINDOWS	6.1. Compatibilidad: 6.1.1. Windows Server 2019 todas las versiones 6.1.2. Windows Server 2016 todas las versiones 6.1.3. Windows Server 2012 todas las versiones 6.1.4. Windows Server 2008 todas las versiones, Service Pack 1 o superior 6.1.5. Windows Server 2003 todas las versiones, Service Pack 2 o superior 6.1.6. Windows Storage Server 2012 o superior 6.1.7. Hyper-V Server 2012 o superior 6.1.8. Windows MultiPoint Server 2011 o superior 6.1.9. Small Business Server 2008 o superior 6.2. Características: 6.2.1. Debe proporcionar las siguientes protecciones: 6.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 6.2.1.2. Autoprotección contra ataques a los servicios/procesos del antivirus 6.2.1.3. Firewall con IDS 6.2.1.4. Control de vulnerabilidades de Windows y de los aplicativos instalados 6.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota; 6.2.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 6.2.4. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 6.2.4.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 6.2.4.2. Gerenciamiento de tarea (crear o excluir tareas de verificación) 6.2.4.3. Lectura de configuraciones 6.2.4.4. Modificación de configuraciones 6.2.4.5. Gerenciamiento de respaldo y cuarentena 6.2.4.6. Visualización de informes 6.2.4.7. Gerenciamiento de informes 6.2.4.8. Gerenciamiento de claves de licencia 6.2.4.9. Gerenciamiento de permisos (agregar/excluir permisos superiores) 6.2.5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas: 6.2.5.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas; 6.2.5.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. 6.2.6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total. 6.2.7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anormalidades (corte de energía, errores, etc.) 6.2.8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptiblePowersupply UPS) 6.2.9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software; 6.2.10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor. 6.2.11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor. 6.2.12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas aunque sean infectadas. 6.2.13. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación; 6.2.14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado; 6.2.15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos

CORPORATION SEKURA S.A.C.E.I. RUC N° 80070889-0

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

	necesiten más recursos de memoria o procesamiento; 6.2.16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 6.2.17. Capacidad de verificar solamente archivos nuevos y modificados; 6.2.18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos autodescompresores, .PST, archivos compactados por compactadores binarios, etc.) 6.2.19. Capacidad de verificar objetos usando heurística; 6.2.20. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas; 6.2.21. Capacidad de agendar una pausa en la verificación; 6.2.22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo; 6.2.23. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 6.2.23.1. Preguntar qué hacer, o; 6.2.23.2. Bloquear el acceso al objeto; 6.2.23.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 6.2.23.2.2. Caso positivo de desinfección: 6.2.23.2.2.1. Recuperar el objeto para uso; 6.2.23.2.3. Caso negativo de desinfección: 6.2.23.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 6.2.24. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. 6.2.25. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 6.2.26. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 6.2.27. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.
7. SERVIDORES LINUX	1. Compatibilidad: 2. CentOS 6.7 o superior, x86 / x64 3. Red Hat® Enterprise Linux® 6.7 o superior, x64 4. Oracle Linux 7.3 o superior, x64 5. Características: 6. Debe proporcionar las siguientes protecciones: 7. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 8. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 9. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 10. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 11. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes; 12. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena; 13. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados. 14. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software; 15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 17. Capacidad de verificar objetos usando heurística; 18. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 19. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 20. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)
8. SMARTPHONES Y TABLETS	8.1. Compatibilidad: 8.1.1. Apple iOS 10.0 o superior 8.1.2. Android OS 4.2 o superior 8.2. Características: 8.2.1. Debe proporcionar las siguientes protecciones: 8.2.1.1. Protección en tiempo real del sistema de archivos del dispositivo — interceptación y verificación de: 8.2.1.1.1. Todos los objetos trasmitidos usando conexiones wireless (puerta de infrarrojo, Bluetooth) y mensajes EMS, durante sincronismo con PC y al realizar descargas usando el browser; 8.2.1.1.2. Archivos abiertos en el smartphone

	8.2.1.1.3. Programas instalados usando la interface del smartphone 8.2.1.2. Verificación de los objetos en la memoria interna del smartphone y en las tarjetas de expansión a pedido del usuario y de acuerdo con un agendamiento; 8.2.2. Deberá aislar en área de cuarentena los archivos infectados; 8.2.3. Deberá actualizar las bases de vacunas de modo agendado; 8.2.4. Deberá bloquear spam de SMS a través de Black lists (listas negras); 8.2.5. Deberá tener función de bloqueo del aparato en caso de que la SIM CARD sea cambiada por otra no autorizada; 8.2.6. Deberá tener función de limpieza de datos personales a distancia, en caso de robo, por ejemplo. 8.2.7. Deberá tener firewall personal; 8.2.8. Posibilidad de instalación remota utilizando Microsoft System Center Mobile Device Manager 2008 SP1 8.2.9. Posibilidad de instalación remota utilizando SybaseAfaria 6.5 8.2.10. Capacidad de detectar Jailbreak en dispositivos iOS 8.2.11. Capacidad de bloquear el acceso a sitios por categoría en dispositivos 8.2.12. Capacidad de bloquear el acceso a sitios phishing o maliciosos 8.2.13. Capacidad de crear contenedores de aplicativos, separando datos corporativos de datos personales 8.2.14. Capacidad de configurar white y blacklist (listas blancas y listas negras) de aplicativos
9. MANEJO DE DISPOSITIVOS MÓVILES (MDM):	9.1. Compatibilidad: 9.1.1. Dispositivos conectados a través de Microsoft Exchange ActiveSync 9.1.1.1. Apple iOS 9.1.1.2. Android 9.1.2. Dispositivos con soporte a Apple Push Notification (APNs) service 9.1.2.1. Apple iOS 11.0 o superior 9.2. Características: 9.2.1. Capacidad de aplicar políticas de ActiveSync a través del servidor Microsoft Exchange 9.2.2. Capacidad de ajustar las configuraciones de: 9.2.2.1. Sincronización de correo electrónico 9.2.2.2. Uso de aplicativos 9.2.2.3. Contraseña del usuario 9.2.2.4. Cifrado de datos 9.2.2.5. Conexión de medios extraíbles 9.2.3. Capacidad de instalar certificados digitales en dispositivos móviles 9.2.4. Capacidad de, en forma remota, resetear la contraseña de dispositivos iOS 9.2.5. Capacidad de, en forma remota, borrar todos los datos de dispositivos iOS 9.2.6. Capacidad de, en forma remota, bloquear un dispositivo iOS
10. CIFRADO	10.1. Características: 10.1.1. El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de el usuario haya olvidado la contraseña, a través de procedimientos de recuperación. 10.1.2. Utilizar, como mínimo, un algoritmo AES con clave de 256 bits. 10.1.3. Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario. 10.1.4. Capacidad de utilizar Single Sign-On para la autenticación de preboot. 10.1.5. Permitir crear varios usuarios de autenticación preboot. 10.1.6. Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo. 10.1.7. Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones: 10.1.7.1. Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes. 10.1.7.2. Cifrar todos los archivos individualmente. 10.1.7.3. Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas. 10.1.7.4. Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña. 10.1.8. Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios. 10.1.9. Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados. 10.1.10. Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.
11. GERENCIAMIENTO DE SISTEMAS	11.1. Capacidad de crear imágenes de sistema operativo remotamente y distribuir esas imágenes para computadoras gestionadas por la solución y para computadoras bare-metal. 11.2. Capacidad de detectar software de terceros vulnerables, creando así un informe de softwares vulnerables. 11.3. Capacidad de corregir las vulnerabilidades de software, haciendo el download centralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios. 11.4. Capacidad de gestionar licencias de software de terceros. 11.5. Capacidad de registrar cambios de hardware en las máquinas gestionadas. 11.6. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra,

Dr. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

CORPORATION SEKURA S.A.C.E.I. RUC Nº 80070889-0

	servicetag, número de identificación y otros.
12. SERVIDORES DE CORREO ELECTRÓNICO WINDOWS	12.1. Características: 12.1.1. Debe utilizar las tecnologías VSAPI 2.0, 2.5 y 2.6; 12.1.2. Capacidad de iniciar varias copias del proceso de antivirus; 12.1.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 12.1.4. Capacidad de verificar carpetas públicas, correos electrónicos enviados, recibidos y almacenados contra virus, spywares, adwares, gusanos, troyanos y riskwares; 12.1.5. Capacidad de verificar carpetas públicas y correos electrónicos almacenados de forma agendada, utilizando las últimas vacunas y heurística; 12.1.6. El antivirus, al encontrar un objeto infectado, debe: 12.1.6.1. Desinfectar el objeto, notificando el remitente, destinatario y administradores, o 12.1.6.2. Excluir el objeto, sustituyéndolo por una notificación; 12.1.6.3. Bloquear el acceso al objeto; 12.1.6.3.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 12.1.6.3.2. Caso positivo de desinfección: 12.1.6.3.2.1. Recuperar el objeto para uso; 12.1.6.3.3. Caso negativo de desinfección: 12.1.6.3.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 12.1.7. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. 12.1.8. Capacidad de enviar notificaciones sobre virus detectados para el administrador, para el destinatario y remitente del mensaje infectado. 12.1.9. Capacidad de grabar logs de actividad de virus en los eventos del sistema y en los logs internos de la aplicación; 12.1.10. Capacidad de detectar diseminación en masa de correos infectados, informando al administrador y registrando tales eventos en los logs del sistema y de la aplicación.
13. SERVIDORES DE CORREO ELECTRÓNICO LOTUS NOTES/DOMINO	13.1. Características: 13.1.1. Capacidad de barrido de banco de datos internos del sistema Lotus Notes/Domino; 13.1.2. Capacidad de barrido en las réplicas de otros servidores Domino que no tengan el antivirus instalado; 13.1.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 13.1.4. Capacidad de barrido de virus en todos los correos electrónicos que pasan por el sistema Lotus Notes/Domino; 13.1.5. El barrido debe involucrar el texto del mensaje y los archivos adjuntos; 13.1.6. Capacidad de cura de mensajes infectados; 13.1.7. Capacidad de filtrado de archivos por tipo; 13.1.8. Capacidad de creación de cuarentena para objetos sospechosos, evitando pérdida de datos; 13.1.9. Capacidad de notificación del destinatario, remitente y administrador sobre objetos que contengan archivos maliciosos; 13.1.10. Capacidad de detección de epidemias y notificaciones de estos eventos al administrador; 13.1.11. Capacidad de actualización vía HTTP, FTP o carpeta en red local; 13.1.12. Capacidad de configurar el tamaño máximo de un archivo que será verificado;
14. SERVIDORES DE CORREO ELECTRÓNICO LINUX	14.1. Características: 14.1.1. Capacidad de verificar el tráfico SMTP del servidor contra malware en todos los elementos del correo electrónico: encabezado, cuerpo y adjunto; 14.1.2. Capacidad de notificar al administrador, al remitente y al destinatario en caso de que un archivo malicioso sea encontrado en el correo electrónico; 14.1.3. Capacidad de poner en cuarentena objetos maliciosos; 14.1.4. Capacidad de guardar respaldo de los objetos antes del intento de desinfección; 14.1.5. Capacidad de hacer barrido en el sistema de archivos del servidor; 14.1.6. Capacidad de filtrar adjuntos por nombre o tipo de archivo; 14.1.7. Capacidad de crear grupos de usuarios para aplicar reglas de verificación de correos electrónicos; 14.1.8. Debe permitir gestión vía consola WEB; 14.1.9. Debe ser actualizado de manera automática vía internet o por servidores locales, con frecuencia horaria.
15. FUNCIONALIDADES DE DETECCIÓN Y RESPUESTA DE ENDPOINT	15.1. La solución debe operar mediante una única consola tanto en entorno local como en la nube. 15.2. La solución debe incluir módulos EDR 15.3. La solución debe contar con funciones de automatización que garanticen la solución rápida de incidentes. 15.4. Capacidad de visualización de alertas de seguridad de los endpoints 15.5. Capacidad de configurar respuestas automatizadas para amenazas descubiertas en todos los endpoints basadas en exploraciones de indicadores de compromiso - IoC 15.6. Capacidad de respuesta instantánea a incidentes tras el descubrimiento 15.7. Las opciones de respuesta deben incluir: 15.7.1. aislar el host 15.7.2. poner en cuarentena el archivo 15.7.3. iniciar el análisis del host 15.7.4. impedir que se ejecute el archivo. 15.8. Capacidad de brindar información acerca de: 15.8.1. Alcance de la amenaza.

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

Velida N. Aponte de Riseher
CORPORATION SEKUAI S.A.C.E.I.
RUC Nº 80070889-0

	15.8.2. Estado de la amenaza: activo y desactivado. 15.8.3. Identificación de los hosts y cuentas de usuarios afectados. 15.8.4. Origen de la amenaza. 15.9. Capacidad de neutralizar amenazas mediante respuesta automática. 15.10. Capacidad de reacción inmediata a los incidentes detectados.
16. SOPORTE TÉCNICO QUE INCLUYA	16.1. El proveedor deberá bridar soporte técnico insitu 24/7 durante el período de licencias; además de dar un adiestramiento mínimo de 40 horas en el uso de la herramienta a 4 personas de la institución. 16.2. Cantidad de tickets de soporte ilimitados. 16.3. Actualización de la consola, agentes y endpoints. 16.4. Actualización de versiones de Sistemas Operativos. 16.5. Respuesta ante incidentes. 16.6. Administración de parches de seguridad. 16.7. Análisis forense e indicadores de compromiso. 16.8. Informes semanales de eventos de seguridad. 16.9. Implementación de todos los módulos de la herramienta en todo el parque de equipos 16.10. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada. 16.11. El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor

El Proveedor se compromete a proveer los Bienes a la Contratante y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.-

La Contratante se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en el Pliego de Bases y Condiciones.-

6. VIGENCIA DEL CONTRATO.
Este contrato tendrá vigencia, desde la firma del mismo hasta el cumplimiento total de las obligaciones.

7. PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE SERVICIOS.
PLAN DE ENTREGA DE LOS SERVICIOS

LUGAR DE ENTREGA: donde indique la orden de servicio

CRONOGRAMA DE ENTREGA:
Las órdenes de servicios serán emitidas por la **DIRECCIÓN ADMINISTRATIVA - DEPARTAMENTO DE EJECUCIÓN DE CONTRATOS,** dependiente de la Dirección Gral. de Administración y Finanzas, a solicitud de la Dirección Gral. de Tecnologías de Información y Comunicación.
Avda Pettirossi esquina Brasil - Teléfono: (021) 201.509
De Lunes a Viernes de 7:30 a 15:00hs
La orden de servicio, será emitida dentro de los 15 (quince) días corridos posteriores a la firma del contrato.

PLAZO DE ENTREGA SERÁ DE:
PARA EL ITEM 1: Se deberá entregar en un plazo máximo de 10 días corridos desde la recepción de la orden de servicio por parte del proveedor. Con presentación y aprobación del Informe Técnico de la Dirección General de Tecnología de la Información y Comunicación de la institución. Se deberá entregar el Certificado de Original de las Licencias.
PARA EL ITEM 2: Se deberá entregar 1 (una) instalación por mes a partir de la recepción de la orden de servicio.
5 hospitales en total se deberá emitir un informe por cada hospital.

La emisión de la totalidad de la orden de servicio, será hasta el Cumplimiento Total de las Obligaciones.

PLAZO DE REPOSICIÓN DE BIENES
El plazo de reposición de bienes para reparar o reemplazar será de: **05 (CINCO) DÍAS HÁBILES.**
El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.
1. La contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.
Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

Lic. Rodrigo Sánchez Araujo, Director
Dirección Administrativa
Ministerio de Salud Pública y Bienestar Social

Nélida R. Aponte de Fischer
CORPORATION SEKIURA S.A.C.E.I.
RUC N° 80070889-0

2. Si el proveedor después de haber sido notificado, no cumple con su obligación dentro del plazo establecido, la contratante tomará las medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

8. ADMINISTRACIÓN DEL CONTRATO.
La administración del contrato estará a cargo de la **DIRECCIÓN ADMINISTRATIVA – DPTO. DE EJECUCIÓN DE CONTRATOS**, quien otorgará las conformidades de recepción y se responsabilizará de la vigencia de las garantías y del cumplimiento del presente Contrato.

9. FORMA Y TÉRMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.
La Garantía de cumplimiento de Contrato deberá ser presentada por el Contratista dentro de los 10 días (Art 39 de la ley 2051/03) siguientes, a partir de la fecha de suscripción del Contrato. El plazo de vigencia de la garantía deberá ser por lo menos treinta días posteriores al plazo de entrega o ejecución del contrato. En caso de ser necesario la garantía de fiel cumplimiento de contrato deberá ser renovada y presentada al administrador del contrato, 60 días antes del vencimiento, la no aplicación de lo estipulado será causal de recisión contractual. La Garantía de Fiel Cumplimiento de Contrato se hará efectiva si la Contratante determinare la Rescisión del Contrato por causa imputable al Contratista, conforme a la Ley y al Contrato. La liberación de la Garantía de Fiel Cumplimiento de Contrato tendrá lugar: a más tardar dentro de los treinta (30) días posteriores a la fecha en que el Proveedor haya cumplido con todas sus obligaciones contractuales.

10. MULTAS.
Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme con las Condiciones Especiales y Generales del Contrato. Superado el monto equivalente a la Garantía de Fiel Cumplimiento de Contrato, la Contratante podrá aplicar el procedimiento de rescisión de contratos de conformidad al Artículo 59 inc. c) de la Ley N° 2.051/03 "De Contrataciones Públicas", caso contrario deberá seguir aplicando el monto de las multas que correspondan. La rescisión del contrato o la aplicación de multas por encima del porcentaje de la Garantía de Cumplimiento del Contrato deberá comunicarse a la DNCP a los fines previstos en el artículo 72 de la Ley N° 2051/03 "De Contrataciones Públicas".

11. CAUSALES Y PROCEDIMIENTO PARA SUSPENDER TEMPORALMENTE, DAR POR TERMINADO ANTICIPADAMENTE O RESCINDIR EL CONTRATO.
Las causales y el procedimiento para suspender temporalmente, dar por terminado en forma anticipada o rescindir el contrato, son las establecidas en la Ley N° 2.051/03, y en las Condiciones Generales y Especiales del Contrato (CGC y CEC).

12. SOLUCIÓN DE CONTROVERSIAS.
Cualquier diferencia que surja durante la ejecución de los Contratos se dirimirá conforme las reglas establecidas en la legislación aplicable y en las Condiciones Generales y Especiales del Contrato.

13. ANULACIÓN DE LA ADJUDICACIÓN
Si la Dirección Nacional de Contrataciones Públicas resolviera anular la adjudicación de la Contratación debido a la procedencia de una protesta o investigación instaurada en contra del procedimiento, y si dicha nulidad afectara al Contrato ya suscrito entre LAS PARTES, el Contrato o la parte del mismo que sea afectado por la nulidad quedará automáticamente sin efecto, de pleno derecho, a partir de la comunicación oficial realizada por la D.N.C.P., debiendo asumir LAS PARTES las responsabilidades y obligaciones derivadas de lo ejecutado del contrato.

En prueba de conformidad se suscriben 2 (dos) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de Asunción, República del Paraguay, a los 15 días del mes de junio de 2023.

Sra. Nélida Rafaela Aponte de Fischer
CONTRATISTA

Sr. Rodrigo Marcial Sánchez Araujo
CONTRATANTE

CORPORATION SEKUAA S.A.C.E.I.
RUC N° 80076889-0