CONTRATO INE N° 05/2021

Entre Instituto Nacional de Estadística (INE) Ex-DGEEC Ley 6670/20; dependiente de la Presidencia de la República, domiciliada en las calles Naciones Unidas esquina Centeno, de la ciudad de Fernando de la Mora – Zona Norte, República del Paraguay, representada para este acto por el Lic. Iván Mauricio Ojeda Aguilera, con Cédula de Identidad N° 1.282.752 en su carácter de Director Nacional, nombrado conforme al Decreto N° 4787, denominada en adelante la contratante, por una parte, y, por la otra, la firma CORPORATION SEKIURA S.A.C.E.I, con RUC N° 80070889-0, representada para este acto por la Sra. Nélida Rafaela Aponte de Fischer con cedula de Identidad Nº 397.359, en su carácter de Representante Legal, con domicilio en la Avenida Boggiani N° 6212 c/R.I. 5 Gral. Díaz. Asunción - República del Paraguay, denominada en adelante el proveedor, identificadas en conjunto como "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente contrato del **ID N° 398872 - Contratación Directa N° 08/2021 "RENOVACIÓN DE LICENCIAS ANTIVIRUS KASPERSKY"**, el cual estará sujeto a las siguientes cláusulas y condiciones:

1. OBJETO.

Constituye el objeto del presente Contrato, establecer las obligaciones y los derechos de las partes contratantes con relación al llamado **ID N° 398872 - Contratación Directa N° 08/2021 "RENOVACIÓN DE LICENCIAS ANTIVIRUS KASPERSKY".**

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) La carta de Invitación y sus Adendas o modificaciones;
c) Los datos cargados en el SICP;
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, siempre que no contradigan las disposiciones del Pliego de Bases y Condiciones, en cuyo caso prevalecerá lo dispuesto en este.

3. DOCUMENTOS ADICIONALES DEL CONTRATO

Los documentos adicionales del contrato son: **No Aplica.**

4. 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° 398872.**

5. PROCEDIMIENTO DE CONTRATACIÓN (Art. 37, b de la Ley N° 2051)

El presente contrato es el resultado del procedimiento de la **Contratación Directa N° 08/2021 con ID N° 398872** para la **"RENOVACIÓN DE LICENCIAS ANTIVIRUS KASPERSKY"** convocado por el Instituto Nacional de Estadística (INE). Y adjudicación fue realizada por **Resolución INE N° 461 /2021.-**

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

6. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES y/o SERVICIOS.

Nro. Ítem	Descripción	Marca	Procedencia	Unidad de Medida	Cantidad	Precio Unitario	Monto Total
1	*Renovación Licencia de Software Antivirus Kaspersky*	*Kaspersky*	*RUSIA*	*UNIDAD*	*327*	*185.000*	*60.495.000*

Total: ***60.495.000***

El monto total del presente contrato asciende a la suma de: **guaraníes sesenta millones cuatrocientos noventa y cinco mil.**

El Proveedor se compromete a proveer los Bienes al 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 la Carta de Invitación.

7. VIGENCIA DEL CONTRATO

El plazo de vigencia de este Contrato es hasta el cumplimiento total de las obligaciones.

8. PLAZO, LUGAR Y CONDICIONES DE ENTREGA (ART. 37 DE LA LEY N° 2051)

Los bienes deben ser entregados dentro de los plazos establecidos en el Cronograma de Entregas de la Carta de Invitación.

9. ADMINISTRACIÓN DEL CONTRATO.

La administración del contrato estará a cargo de la Dirección de Informática.

10. FORMA Y TÉRMINOS PARA GARANTIZAR EL CUMPLIMIENTO DEL CONTRATO.

La garantía para el fiel cumplimiento del contrato se regirá por lo establecido en la Carta de Invitación, la cual se presentará a más tardar dentro de los 10 (días) calendarios siguientes a la firma del contrato.

11. CONSTANCIA DE PRESENTACIÓN DE DECLARACIÓN JURADA

El adjudicado deberá en el plazo de quince (15) días calendario desde la firma del presente contrato, presentar ante el administrador de contrato, la constancia o constancias de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, de todos los sujetos obligados en el marco de la Ley N° 6355/19.
En el mismo plazo indicado en el párrafo anterior, se deberá remitir a la convocante la actualización de la mencionada declaración jurada, una vez finalizada la ejecución del presente contrato

12. MULTAS.

Las multas y otras penalidades que rigen en el presente contrato serán aplicadas conforme a la Carta de Invitación. 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.

CORPORATION SEKURA S.A.C.E.I. RUC N° 80079828-0

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", modificado por Ley N° 6716/2021.

13. 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 la Carta de Invitación.

14. 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 la Carta de Invitación.

15. 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 DNCP, debiendo asumir LAS PARTES las responsabilidades y obligaciones derivadas de lo ejecutado del contrato.

Para la ejecución del laudo arbitral o para dirimir cuestiones que no sean arbitrables, las Partes establecen la competencia de los tribunales de la ciudad de Asunción, República del Paraguay".

En prueba de conformidad se suscriben 2 (dos) ejemplares de un mismo tenor y a un solo efecto en la Ciudad de Fernando de la Mora, República del Paraguay, a los 19 días del mes de julio de 2021.

Nélida R. Aponte de Fischer.-

Sra. Nélida Rafaela Aponte de Fischer
Representante Legal
CORPORATION SEKIURA S.A.C.E.I –
RUC N° 80070889-0

Lic. Iván Mauricio Ojeda Aguilera
Director Nacional
Instituto Nacional de Estadística.

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

ANEXO AL CONTRATO N° 05/2021

ESPECIFICACIÓN TÉCNICA DEL BIEN

ID N° 398872 Contratación Directa N° 08/2021

"RENOVACIÓN DE LICENCIAS ANTIVIRUS KASPERSKY"

Nro. de Ítem 1 – **Código** 43231512-9992
Nombre: Renovación de ANTIVIRUS KASPERSKY de Seguridad y Control de Punto Final
Cantidad: 327 **Unidad de Medida:** Unidad **Presentación:** UNIDAD

1. Servidor de Administración y Consola Administrativa
   1.1. Compatibilidad:
      1.1.1. Microsoft Windows 10 20H2 32 bits o 64 bits (versiones 12.2 en adelante).
      1.1.2. Microsoft Windows 10 20H1 32 bits o 64 bits (versiones 12.1 en adelante).
      1.1.3. Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits.
      1.1.4. Microsoft Windows 10 Enterprise 2016 LTSB 32 bits / 64 bits.
      1.1.5. Microsoft Windows 10 Enterprise 2015 LTSB 32 bits / 64 bits.
      1.1.6. Microsoft Windows 10 Pro RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
      1.1.7. Microsoft Windows 10 Pro para estaciones de trabajo RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
      1.1.8. Microsoft Windows 10 Enterprise RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
      1.1.9. Microsoft Windows 10 Education RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
      1.1.10. Microsoft Windows 10 Pro 19H1 32 bits / 64 bits.
      1.1.11. Microsoft Windows 10 Pro for Workstations 19H1 32 bits / 64 bits.
      1.1.12. Microsoft Windows 10 Enterprise 19H1 32 bits / 64 bits.
      1.1.13. Microsoft Windows 10 Education 19H1 32 bits / 64 bits.
      1.1.14. Microsoft Windows 10 Pro 19H2 32 bits / 64 bits.
      1.1.15. Microsoft Windows 10 Pro for Workstations 19H2 32 bits / 64 bits.
      1.1.16. Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits.
      1.1.17. Microsoft Windows 10 Education 19H2 32 bits / 64 bits.
      1.1.18. Microsoft Windows 8.1 Pro 32 bits / 64 bits.
      1.1.19. Microsoft Windows 8.1 Enterprise 32 bits / 64 bits.
      1.1.20. Microsoft Windows 8 Pro 32 bits / 64 bits.
      1.1.21. Microsoft Windows 8 Enterprise 32 bits / 64 bits.
      1.1.22. Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores 32 bits / 64 bits.
      1.1.23. Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 y versiones posteriores 32 bits / 64 bits.
      1.1.24. Windows Server 2019 Standard 64 bits.
      1.1.25. Windows Server 2019 Core 64 bits.
      1.1.26. Windows Server 2019 Datacenter 64 bits.
      1.1.27. Windows Server 2016 Server Standard RS3 (v1709) (LTSB / CBB) 64 bits.
      1.1.28. Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB / CBB) 64 bits.
      1.1.29. Windows Server 2016 Server Core RS3 (v1709)
      1.1.30. Windows Server 2016 Standard (LTSB) 64 bits.
      1.1.31. Windows Server 2016 Server Core
      1.1.32. Windows Server 2016 Datacenter (LTSB) 64 bits.

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

1.1.33. Windows Server 2012 R2 Standard 64 bits.
1.1.34. Windows Server 2012 R2 Server Core 64 bits.
1.1.35. Windows Server 2012 R2 Foundation 64 bits.
1.1.36. Windows Server 2012 R2 Essentials 64 bits.
1.1.37. Windows Server 2012 R2 Datacenter 64 bits.
1.1.38. Windows Server 2012 Standard 64 bits.
1.1.39. Windows Server 2012 Server Core 64 bits.
1.1.40. Windows Server 2012 Foundation 64 bits.
1.1.41. Windows Server 2012 Essentials 64 bits.
1.1.42. Windows Server 2012 Datacenter 64 bits.
1.1.43. Windows Storage Server 2016 64 bits.
1.1.44. Windows Storage Server 2012 R2 64 bits.
1.1.45. Windows Storage Server 2012 64 bit

2. Características:

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 disponibilidad
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

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

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 características 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 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;

CORPORATION SEKUFA S.A.C.E.I. RUC N° 80070853-0

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 paquetes 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 compatibilidad con Cisco Network Admission Control (NAC);
2.1.35. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo).
2.1.36. 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);
2.1.37. 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);
2.1.38. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;
2.1.39. Capacidad de reportar vulnerabilidades de software presentes en las computadoras.
2.1.40. Capacidad de realizar inventario de hardware de todas las máquinas clientes;
2.1.41. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;
2.1.42. 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, Service Pack 1 o superior
   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)

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

3.2.1.7. Control de dispositivos externos
3.2.1.8. Control de acceso a sitios por categoría
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 la 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:

CORPORATION SEKURIR S.A.C.E.E. RUC N° 80076825-0

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;
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:

CORPORATION SEKURA S.A.C.E.I. RUC N° 80070600-0

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.

4. Estaciones y Servidores Mac OS X –

4.1. Compatibilidad:

4.1.1. Mac OS X 10.12 o superior

CORPORATION SEKURA S.A.C.E.I. RUC N° 80076882-0

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

CORPORATION SEKIURA S.A.C.E.I. RUC N° 80076669-0

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 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

CORPORATION SEKURA S.A.C.E.I. RUC N° 80070000-0

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;

CORPORATION SEKUPA S.A.C.E.I. RUC N° 80078883-0

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 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 –

6.1. Compatibilidad:

6.1.1. CentOS 6.7 o superior, x86 / x64

6.1.2.Red Hat® Enterprise Linux® 6.7 o superior, x64

6.1.3.Oracle Linux 7.3 o superior, x64

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. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

6.2.2.Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:

6.2.2.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);

CORPORATION SEKUNA S.A.C.E.I. RUC N° 80070020-0

6.2.2.2. 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;

6.2.2.3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;

6.2.2.4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.

6.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software;

6.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

6.2.5. 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;

6.2.6. Capacidad de verificar objetos usando heurística;

6.2.7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán

6.2.8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena

6.2.9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)

7. Smartphones y tablets-

7.1. Compatibilidad:

7.1.1. Apple iOS 10.0 o superior

7.1.2. Android OS 4.2 o superior

7.2. Características:

7.2.1. Debe proporcionar las siguientes protecciones:

7.2.1.1. Protección en tiempo real del sistema de archivos del dispositivo — interceptación y verificación de:

7.2.1.1.1. 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.

7.2.1.1.2. Archivos abiertos en el smartphone

7.2.1.1.3. Programas instalados usando la interface del smartphone

7.2.1.2. 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;

7.2.2. Deberá aislar en área de cuarentena los archivos infectados;

7.2.3. Deberá actualizar las bases de vacunas de modo agendado;

7.2.4. Deberá bloquear spam de SMS a través de Black lists (listas negras);

7.2.5. Deberá tener función de bloqueo del aparato en caso de que la SIM CARD sea cambiada por otra no autorizada;

7.2.6. Deberá tener función de limpieza de datos personales a distancia, en caso de robo, por ejemplo.

7.2.7. Deberá tener firewall personal;

7.2.8. Posibilidad de instalación remota utilizando Microsoft System Center Mobile Device Manager 2008 SP1

7.2.9. Posibilidad de instalación remota utilizando SybaseAfaria 6.5

7.2.10. Capacidad de detectar Jailbreak en dispositivos iOS

CORPORATION SEKURA S.A.C.E.I. RUC N° 80078424-0

7.2.11. Capacidad de bloquear el acceso a sitios por categoría en dispositivos
7.2.12. Capacidad de bloquear el acceso a sitios phishing o maliciosos
7.2.13. Capacidad de crear contenedores de aplicativos, separando datos corporativos de datos personales
7.2.14. Capacidad de configurar white y blacklist (listas blancas y listas negras) de aplicativos

8. Manejo de dispositivos móviles (MDM):
8.1. Compatibilidad:
8.1.1. Dispositivos conectados a través de Microsoft Exchange ActiveSync
8.1.1.1. Apple iOS
8.1.1.2. Android
8.1.2. Dispositivos con soporte a Apple Push Notification (APNs) service
8.1.2.1. Apple iOS 11.0 o superior
8.2. Características:
8.2.1. Capacidad de aplicar políticas de ActiveSync a través del servidor Microsoft Exchange
8.2.2. Capacidad de ajustar las configuraciones de:
8.2.2.1. Sincronización de correo electrónico
8.2.2.2. Uso de aplicativos
8.2.2.3. Contraseña del usuario
8.2.2.4. Cifrado de datos
8.2.2.5. Conexión de medios extraíbles
8.2.3. Capacidad de instalar certificados digitales en dispositivos móviles
8.2.4. Capacidad de, en forma remota, resetear la contraseña de dispositivos iOS
8.2.5. Capacidad de, en forma remota, borrar todos los datos de dispositivos iOS
8.2.6. Capacidad de, en forma remota, bloquear un dispositivo iOS

COMO MINIMO DEBERA CONTAR:

8.3. Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto
8.4. contar como mínimo con 2 técnicos con certificaciones de cifrado
8.5. Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam
8.6. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS
8.7. contar como mínimo con 3 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.
8.8. contar con al menos 10 contratos o facturas de la provisión del Software ofertado entre los años 2018, 2019 y 2020.
8.9. implementación de todos los módulos de la herramienta en todo el parque de equipos.
8.10. capacitación de la herramienta a todas las personas involucradas en el departamento de tecnología.
8.11. soporte técnico incluido durante todo el periodo de licenciamiento.
8.12. cantidad de tickets de soporte ilimitados.
8.13. El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local.
8.14. El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.
8.15. El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado

CORPORATION SEKURA S.A.C.E.I. RUC N° 80010285-0

Misión: ***Regir y conducir la producción de la estadística oficial que describa al Paraguay.***

8.16. 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.

8.17. 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

8.18. la convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta

Nélida R. Aponte de Fischer.-

Sra. Nélida Rafaela Aponte de Fischer
Representante Legal
CORPORATION SEKIURA S.A.C.E.I –
RUC N° 80070889-0

Lic. Iván Mauricio Ojeda Aguilera
Director Nacional
Instituto Nacional de Estadística.

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