CONTRATO Nº 050/2023

LICITACIÓN POR CONCURSO DE OFERTAS N° 17/2023 para "ADQUISICIÓN DE LICENCIA DE ANTIVIRUS PARA LOS SERVIDORES".

Entre el Servicio Nacional de Calidad y Sanidad Vegetal y de Semillas-SENAVE, domiciliado en Luis Alberto Herrera 195 esq. Yegros, Edificio Inter Express, Piso 5, Asunción, República del Paraguay, representado para este acto por su Encargado de Despacho de la Presidencia, el señor **MIGUEL ÁNGEL BÁEZ**, conforme a la Resolución Senave N° 388/23 del 27 de noviembre de 2023, con Cédula de Identidad N° 1.043.964, denominado en adelante, el **CONTRATANTE**, por una parte, y, por la otra, la firma **CELEXX S.A.,** con RUC Nº 80027703-1 domiciliada en la calle Avda. Guido Boggiani 5832 casi Alas Paraguayas, de la Ciudad de Asunción, República del Paraguay, con teléfono Nº (021) 504.444, con correo: licitaciones@celexx.la representada para este acto por **MARCO ESTEBAN DOMANICZKY GARCIA DE ZUÑIGA** , con C.I. Nº 958.501 en su carácter de Representante Legal, denominada en adelante **EL PROVEEDOR**, denominadas en conjunto "LAS PARTES" e, individualmente, "PARTE", acuerdan celebrar el presente contrato de ***"ADQUISICIÓN DE LICENCIA DE ANTIVIRUS PARA LOS SERVIDORES",*** el cual estará sujeto a las siguientes cláusulas y condiciones:

1. OBJETO.

El presente Contrato tiene por objeto establecer los derechos y obligaciones que asumen el CONTRATANTE y el PROVEEDOR, las partes con relación a la **LICITACIÓN POR CONCURSO DE OFERTAS *LCO N° 17/2023*** para la ***"ADQUISICIÓN DE LICENCIA DE ANTIVIRUS PARA LOS SERVIDORES".***

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 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 Contratante y su respectiva notificación;
(f) Garantía de Fiel Cumplimiento de Contrato.

Los documentos que forman parte del Contrato deberán considerarse mutuamente explicativos; en caso de contradicción o diferencia entre los documentos que forman parte integral del Contrato, la prioridad de los mismos será en el orden enunciado anteriormente, siempre y cuando no contradigan las disposiciones del Pliego de Bases y Condiciones, en cuyo caso prevalecerá lo dispuesto en el P.B.C.

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 Nº 428.477.**

4. PROCEDIMIENTO DE CONTRATACIÓN

El presente Contrato es el resultado del procedimiento de la ***LICITACIÓN POR CONCURSO DE OFERTAS LCO N° 17/2023*** para ***"ADQUISICIÓN DE LICENCIA DE ANTIVIRUS PARA LOS SERVIDORES"***, convocado por el Servicio Nacional de Calidad y Sanidad Vegetal y de Semillas-SENAVE. La adjudicación fue realizada según **Resolución Nº 321, de fecha 14 de noviembre de 2023.**

5. PRECIO UNITARIO Y EL IMPORTE TOTAL A PAGAR POR LOS BIENES.

ítem	Descripción	Unidad de Medida	Presentación	Cantidad	Marca	Procedencia	Precio Unitario	Precio Total
1	software antivirus para servidores	Unidad	Unidad	450	FORTINET	USA	1.098.000	494.100.000
TOTAL								**494.100.000**

El Monto del presente contrato asciende a la suma de ***GUARANIES CUATROCIENTOS NOVENTA Y CUATRO MILLONES CIEN MIL (GS. 494.100.000) IVA INCLUIDO.-***

C. MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

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 la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en las Condiciones Contractuales.

El pago será realizado luego de la entrega de los Bienes a satisfacción del SENAVE; con recursos institucionales (FF-30). Para el pago, el proveedor deberá presentar una solicitud de pago por escrito acompañando la factura correspondiente. El pago será efectivizado dentro de los 60 días calendario contados a partir de la fecha de presentación de la solicitud respectiva.

Del monto total facturado, serán pasibles las retenciones correspondientes al Impuesto a la Renta y al Impuesto al Valor Agregado, según lo establecido por las disposiciones legales de la República del Paraguay.

Asimismo, independientemente de estas retenciones impositivas, se aplicará una Retención equivalente al 0,5% sobre el monto de las facturas pagadas, deducidos los impuestos reflejados en las mismas, en concepto de "Contribución" de conformidad a lo dispuesto por el Art. 41 de la Ley 3439/07 "Que modifica la Ley Nº 2051/03 de Contrataciones Públicas y establece la carta orgánica de la Dirección Nacional de Contrataciones Públicas" y el Art. 278 de la Ley N° 7050/2023. La vigencia del presente porcentaje para el Ejercicio Fiscal 2024 estará sujeta a la aprobación presupuestaria correspondiente.

Solicitud de pago de anticipo: Solo para MYPYMES, en caso de que resulte adjudicada una empresa MIPYMES se otorgara a la misma un anticipo del 10% (diez por ciento) del monto total del contrato, conforme a lo establecido en el Art. N° 188 de la Ley N° 7050/2023, y lo establecido en las bases del llamado en cuanto al apartado de anticipo.

Todos los pagos se efectuaran en Guaranies.

6. VIGENCIA DEL CONTRATO

El plazo de vigencia es desde la suscripción hasta el cumplimiento total de las obligaciones.

7. PLAZO, LUGAR Y CONDICIONES DE LA PROVISIÓN DE LOS BIENES.

ítem	Descripción	Especificaciones Técnicas	Unid medida
1	Licencia de antivirus	La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows (32-bit & 64-bit versiones) XP SP2/SP3, 7, 8, 8.1, 10 y 11	unidad
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Windows Server r 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019, y 2022			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: macOS Versiones: El Capitan (10.11),Sierra(10.12),High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x), y Monterey (12.x)			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: RedHat Enterprise Linux y CentOS 6.x, 7.x, and 8.x			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: Ubuntu LTS 16.04.x, 18.04.x, 20.04.x server, 64-bit solamente			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: Oracle Linux 7.7+ and 8.2+			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: Amazon Linux AMI 2			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Linux Versiones: SuSE SLES 15.1			
La solución propuesta debe ser compatible con los siguientes sistemas operativos: Ambientes Virtual Desktop Infrastructure (VDI) en VMware Y Citrix. VMware Horizons 6 y 7, y Citrix XenDesktop 7			
La solución propuesta debe tener un consumo máximo de 120MB de memoria RAM			
La solución propuesta debe tener un consumo promedio de menos de 2% de uso de CPU			
La solución propuesta debe tener un consumo menor a 20MB de espacio en disco			

MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

La solución propuesta debe soporta el despliegue masivo a través de herramientas como MS System Center, JAMF, y Satellite.
La solución propuesta debe tener la habilidad de actualizar el Endpoint sin interacción por parte del usuario y sin requerimiento de reinicio
La solución propuesta debe tener protección "Anti-Tamper" en el Agente
La solución propuesta debe trabajar sin depender de firmas hash locales conocidas para la detección de archivos maliciosos
La solución propuesta debe poder registrar en tiempo real información del proceso e informaciones adicionales tal como conocer el usuario asociado con los eventos
La solución propuesta debe contar con la opción de establecer contraseña para desinstalar el agente en el endpoint
La solución propuesta debe poder generar un instalador de Windows Preconfigurado. Esta configuración debe permitir la instalación sin requerir interacción ni configuración por parte de los usuarios
El colector que será instalado en los endpoint de la solución propuesta debe poder trabajar detrás de un proxy
Detección de Malware
La solución propuesta debe poder funcionar en modalidad "offline" fuera de línea sin que el Agente se encuentre conectado a la red empresarial
La solución propuesta debe poder detectar procesos en ejecución, inicios de procesos, paradas de procesos e interacciones entre procesos.
La solución propuesta debe poder detectar, eliminar y volver a su valor inicial cambios realizado por procesos maliciosos en el registro de las PC.
La solución propuesta debe poder detecta solicitudes DNS enviadas desde el dispositivo.
La solución propuesta debe poder detectar conexiones de red desde el dispositivo.
La solución propuesta debe poder detectar actividad sospechosa asociada con archivos DLL.
La solución propuesta debe poder Incorpora inteligencia de amenazas en el esquema de detección.
La solución propuesta debe poder incorporar las técnicas de MITRE ATT&CK en el esquema de detección y mostrar cuales de estas técnicas fueron utilizadas
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como: Nombre de archivo y hash de archivo, etc.
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Linux (Redhat y CentOS) utilizando indicadores de compromisos (IOC) tales como archivos, logs y comportamiento de red
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada a archivos (Creación, Eliminación, Rename)
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relaciones a los procesos (Terminación de Proceso, Creación de Proceso, Carga de Ejecutable)
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al uso de red (Socket Connect, Socket Close, Socket Brind)
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada a las bitácoras de Windows (Event Log).
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al registro de Windows (Key Create, Key Delete, Value Set)
La solución propuesta debe tener la capacidad para realizar free text queries para filtrar la información disponible para threat hunting
La solución propuesta debe tener la capacidad para almacenar búsquedas realizadas para ser reutilizadas en el futuro
La solución propuesta debe tener la capacidad programar las búsquedas de indicadores de compromiso (IOC) almacenados
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada al registro del uso del teclado (KeyLogging)

MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada a la toma de "Screen Shots
La solución propuesta debe tener la capacidad para realizar la búsqueda de amenazas en la estaciones Windows utilizando indicadores de compromisos (IOC) tales como acciones relacionada a las consultas generadas a DNS
La solución propuesta debe identificar actividad maliciosa conocida
La solución propuesta debe tener la capacidad de recibir actualizaciones diarias de inteligencia
La solución propuesta debe tener la capacidad de categorizar los eventos detectados en diferentes categorías (Ej.: Malicioso, Sospechoso, No concluyente, Probablemente Seguro)
La solución propuesta debe tener la capacidad de convivir con otras soluciones de seguridad endpoint del tipo antivirus tradicional o de nueva generación.
La solución propuesta debe tener capacidad de crear excepciones a un archivo o a carpetas selecionadas de la revision por parte del motor de NGAV al momento de ejecutarse el archivo
Prevención de Malware
La solución propuesta debe tener la capacidad de prevención de ejecución de archivos maliciosos
La solución propuesta debe incorporar un motor de antivirus de última generación (NGAV) basado en el kernel con capacidad de "Machine Learning"
La solución propuesta debe tener capacidad de controlar dispositivos USB
La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en el nombre del dispositivo
La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en el vendor del dispositivo
La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en el numero serial del dispositivo
La solución propuesta debe tener capacidad de crear excepciones a los dispositivos USB basado en una combinación del: nombre del dispositivo, vendor, numero serial
La solución propuesta debe tener capacidad de crear excepciones a un proceso conocido legitimo conocido de ser monitoreado por la plataforma de EDR
La solución propuesta debe poder bloquear trafico malicioso de exfiltración de datos
La solución propuesta debe poder bloquear trafico malicioso de comunicación hacia C&C (Command & Control)
La solución propuesta debe poder frenar brechas de seguridad e intentos de ransomware en tiempo real
La solución propuesta debe poder evitar cifrados de disco causado por ransomware y modificación de archivos o registro de los dispositivos
La solución propuesta debe permitir que las políticas en la misma sean modificada permitiendo varios estados como: Activa, Desactivada o solo crear "logs" para las reglas de seguridad contenidas en estas
La solución propuesta debe poder ser configurada en modo de simulación donde no se realicen bloqueos pero toda actividad maliciosa es registrada
La solución propuesta debe poder permitir la modificación de las reglas de detección de eventos maliciosos para que estas reglas solo almacenen un registro o estén en modo bloqueo
La solución propuesta debe poder permitir la realización de escaneos periódicos de los archivos contenidos en los dispositivos con el Agente instalado
Difusión (Post-Infección)
La solución propuesta debe permitir el aislamiento automático del trafico de red de un dispositivo donde se ha encontrado una actividad causada por malware
La solución propuesta debe permitir cambiar las políticas asignadas de un dispositivo donde se ha encontrado una actividad causada por malware
La solución propuesta debe permitir el bloqueo de las actividades realizadas por parte de archivos maliciosos
La solución propuesta debe tener la capacidad de creación de excepciones para los procesos basados en la localización del archivo (File Path)
La solución propuesta debe tener la capacidad de creación de excepciones para los procesos basados en el destino del trafico generado por el proceso
La solución propuesta debe tener la capacidad de creación de excepciones para los procesos basados en usuario que ha ejecutado el proceso
La solución propuesta debe tener la capacidad de crear excepciones para los falsos positivos de forma manual para marcar la actividad como falso positivo y evitar que ocurran bloqueos futuros
La solución propuesta debe tener la capacidad de recalificar automáticamente la actividad como falso positivo y evitar que ocurran detecciones similares.

ING. MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

La solución propuesta debe permitir la creación de excepciones de eventos basados en direcciones IP, aplicaciones y protocolos
Respuesta a Incidentes
La solución propuesta debe permitir un histórico de los eventos por un mínimo de 1 mes
La solución propuesta debe almacenar meta-data generada por los dispositivos para que la misma sea usada en investigaciones forenses
La solución propuesta debe permitir la integración con plataformas SIEMs (Security Information and Event Management) a través de un syslog
La solución propuesta debe tener la capacidad de obtener capturas instantáneas de memoria o "dumps" de memoria que permitan la realización de procesos forenses
La solución propuesta debe tener la capacidad de abrir tickets en plataformas de gestión tales como ServiceNow y JIRA
La solución propuesta debe permitir la integración a través de API donde el mismo tenga la capacidad de entregar información generada en un evento tales como: Dirección IP, nombre de host, usuario, fecha / hora ocurrida, actividad sospechosa, etc.) para permitir la integración vía API
La solución propuesta debe tener la capacidad para terminar un proceso basado en la clasificación del mismo
La solución propuesta debe tener la capacidad para eliminar un archivo basado en la clasificación del mismo
La solución propuesta debe la capacidad para restaurar la configuración base del registro basada en la clasificación de actividad predefinida
La solución propuesta debe tener la capacidad para aislar dispositivos infectados de la red.
La solución propuesta debe tener la capacidad para restringir el acceso del dispositivo a la red de forma automática según la clasificación (Malicioso, Sospechoso, etc.) del proceso detectada
La solución propuesta debe obtener visibilidad completa de la cadena de ataque y cambios maliciosos
La solución propuesta debe permitir la limpieza automática de los dispositivos y revertir los cambios maliciosos mientras mantiene el tiempo de disponibilidad del dispositivo
La solución propuesta debe permitir la suscripción de servicios opcionales de detección y respuesta a incidentes (Ej.: Servicios gestionados de detección y respuesta)
La solución propuesta debe permitir el envío de ejecutables para su análisis a un sandbox , con la finalidad de determinar si son maliciosos o inofensivos.
La solución propuesta debe proporcionar múltiples mecanismos de protección, incluida como la terminación de un proceso, eliminación de un archivo malicioso, el bloqueo de una conexión de red
Control de Vulnerabilidades y Comunicación
La solución propuesta debe tener la capacidad para descubrir aplicaciones que se estén comunicando a través de la red y que estas representen riesgo al endpoint
La solución propuesta debe tener la capacidad para realizar un parche virtual, a través de la restricción de los accesos de comunicación en aquellas aplicaciones que sean vulnerables.
La solución propuesta debe permitir la reducción de las superficies de ataque utilizando políticas proactivas de comunicación basadas en el riesgo de acuerdo a CVE y la calificación o reputación que puede tener una aplicación
La solución propuesta debe tener la capacidad para prevenir la comunicación a través de la red de cualquier aplicación no autorizada
La solución propuesta debe tener la capacidad para crear políticas que tengan la capacidad de prevenir la comunicación de aplicaciones de acuerdo a la versión de la aplicación instalada
La solución propuesta debe poder detectar e identificar todas las aplicaciones en los dispositivos que se comunican en la red.
La solución propuesta debe poder entregar información sobre el uso de aplicaciones en red mostrando información como cuales dispositivos generan trafico de una aplicación
La solución propuesta debe poder visualizar y entregar información sobre el uso de aplicaciones en red mostrando información como los IP destinos del trafico generado por la aplicación
La solución propuesta debe poder tener la capacidad de crear una lista de aplicaciones cuya ejecucion sera bloqueadas. Esta lista debe permitir la creacion de politicas para su uso en grupos de estaciones de trabajo selecionadas
Escenarios de Ataque
La solución propuesta debe identificar y prevenir los intentos de estalación de privilegios
La solución propuesta debe bloquear ataques de ransomware conocido
La solución propuesta debe detectar malware desconocidos como RAT (Remote Access Trojan) a través de las actividades del malware y no una firma
La solución propuesta debe proteger contra Scripts de Powershell maliciosos

ING. MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

La solución propuesta debe proteger contra Scripts de CScript maliciosos
La solución propuesta debe proteger contra macros de Office maliciosos
La solución propuesta debe tener control sobre dispositivos USB
Requerimiento - IOT
La solución propuesta debe tener la capacidad de detectar dispositivos IOT no administrados en la red
La solución propuesta debe tener la capacidad de detectar dispositivos no administrados y protegidos por la solución con sistemas operativos macOS/Linux/Windows
Consola de Administración
La solución propuesta debe cumplir con los estándares de seguridad de datos de la industria de tarjetas de pago (PCI DSS)
La solución propuesta debe cumplir con el estándar HIPAA
La solución propuesta debe cumplir con el estándar GDPR
La consola de administración de la solución propuesta debe permitir la integración con "Active Directory" para garantizar el cumplimiento de los requisitos de la política de contraseñas de la empresa.
La consola de administración de la solución propuesta debe permitir el uso de autenticación de doble factor (2FA) para acceder a la misma
La consola de administración de la solución propuesta debe permitir la integración con SAML para la autenticación de los usuarios a la consola de gestión
La consola de administración de la solución propuesta debe permitir el uso de roles granulares para los administradores
La consola de administración de la solución propuesta debe permitir la gestión para ambientes Multi-inquilinos.
La consola de administración de la solución propuesta debe permitir la gestión a través de Full Restful API
La solución propuesta debe poder ser gestionada completamente en nube sin requerimiento de servicios en las premisas
La solución propuesta debe poder ser gestionada en una arquitectura hibrida utilizando servicios en las premisas complementadas con otras en nube.
La solución propuesta debe permitir la integración para realizar acciones en soluciones de terceros a través de scripts Python para accionar un API cuando ocurra un evento de seguridad
La consola de administración de la solución propuesta debe permitir la visualización de los eventos registrados en los dispositivos que requieran atención
La consola de administración de la solución propuesta debe permitir la visualización la salud de los Agentes instalados
La consola de administración de la solución propuesta debe permitir la desinstalación remota del Agente instalado en los dispositivos
La consola de administración de la solución propuesta debe permitir la desactivación/activación remota del Agente instalado en los dispositivos
La consola de administración de la solución propuesta debe permitir la actualización remota del Agente instalado en los dispositivos
La consola de administración de la solución propuesta debe permitir la creación de reportes ejecutivo conteniendo un resumen que describe los eventos de seguridad y el estado del sistema.
La consola de administración de la solución propuesta debe permitir la creación de grupos organizativos de dispositivos en los cuales cada grupo podrá tener reglas de protección independiente de los demás
La consola de administración de la solución propuesta debe permitir la exportación de bitácoras locales generadas por los Agentes desde la misma consola
La consola de administración de la solución propuesta debe permitir la creación de reportes de inventario sobre los Agentes desplegados conteniendo información como: Dirección IP, Hostname, Sistema Operativo, Dirección MAC, Versión de Agente instalada, Estado del Agente, Ultimo día visto por la consola
La consola de administración de la solución propuesta debe la visibilidad de eventos generados por los dispositivos o eventos de acuerdo al proceso ejecutado
La consola de administración de la solución propuesta debe permitir la integración de un SMTP externo para el envió de alertas a través de correo electrónico
La consola de administración de la solución propuesta debe permitir las auditorías de cambios realizados por los administradores/operadores. Estas auditorias deben poder ser además descargas en un formato CSV
La solución propuesta debe requerir una contraseña para ser deshabilitado por una aplicación de tercero
La solución propuesta debe permitir el aislamiento de un dispositivo a través de la integración de un NAC de acuerdo a la categoría del evento detectado

LIC. MARCO DOMANICZKY
DIRECTOR
CELEXX S.A.

La solución propuesta debe permitir agregar direcciones IP maliciosas detectadas en uno o mas firewalls remoto integrados
La solución propuesta debe permitir la configuración de perfiles sobre la información recolectada para la función de threat hunting
La solución propuesta debe permitir exclusiones de información que no será recolectada dentro de la función de threat hunting
La solución propuesta debe estar certificada por Microsoft como una solución de Antivirus y poder integrarse con Windows Security Center
La solución propuesta debe entregar información generada por lo servicios de inteligencia para la toma de decisión realizadas en la nube sobre el evento detectado
La solución propuesta debe permitir que los servicios en nube recategorizen un la clasificación de un evento
La solución propuesta debe permitir que los administradores deshabiliten las notificaciones de un evento de detección
La solución propuesta debe permitir realizar funciones web filtering bloqueando el acceso a paginas web categorizadas como maliciosas

ENTREGABLES Y FORMAS DE PAGO

LUGAR	Características generales	Cantidad solicitada	PLAZO
Humaitá N° 145 – Edificio Planeta I	-Agentes -Consola y/o plataforma de administración -XDR -Instalación y Soporte -Documentaciones	450	Una vez emitida la orden de compra y recepcionada por el proveedor, en un plazo máximo de 10 (diez) días hábiles.

8. ADMINISTRACIÓN DEL CONTRATO.

La administración del Contrato estará a cargo del Director/a de DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN, quien, en caso de incumplimiento de las condiciones establecidas para la ejecución, deberá comunicar a la Dirección de Contrataciones, a fin de aplicar lo dispuesto en el punto 10 de este Contrato.

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

La Garantía para el Fiel Cumplimiento del Contrato se regirá por lo establecido en las Condiciones Contractuales, la cual se presentará a más tardar dentro de los 10 (días) calendarios siguientes a la firma del Contrato. La garantía de fiel cumplimiento debe ser equivalente al 10% del monto total del Contrato y extendida por 3 (tres) meses posteriores al vencimiento contractual.

10. MULTAS.

Las multas y otras penalidades que rigen en el presente Contrato serán aplicadas conforme con las Condiciones Contractuales, la cual establece que el SENAVE aplicará, el valor de las multas será de 0,5% (cero coma cinco por ciento) del valor del suministro en demora por cada día de atraso.

Llegado al monto equivalente de la Garantía de Fiel Cumplimiento de Contrato, la Contratante podrá aplicar el procedimiento de rescisión de Contrato 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", modificado por Ley N° 6716/2021.

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 Contractuales.

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 Contractuales.

MARCO DOMANIGZKY
DIRECTOR
CELEXX S.A.

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 testimonio de conformidad se suscriben 3 (tres) ejemplares de un mismo tenor y a un solo efecto, en la Ciudad de Asunción, República del Paraguay, a los 06 días del mes de Diciembre de 2023.-

MARCO ESTEBAN DOMANICZKY GARCIA DE ZUÑIGA
REPRESENTANTE LEGAL – CELEXX S.A.
PROVEEDOR

CELEXX S.A.

MIGUEL ÁNGEL BÁEZ
Encargado de Despacho de la Presidencia del SENAVE
CONTRATANTE