**BL ONE S.A.**
**Cédula Jurídica:** 3-101- 634194
**Telefax:**2236-2894
**email:** info@blonecr.com

19 de Abril de 2022.

Municipalidad de Pococí
Dpto. de Proveeduría
Presente

Mediante la presente, yo Benjamín Pineda Ávila, en calidad de Representante Legal de la empresa BL One S.A., con cédula jurídica 3-101-634194, domiciliada en Tibás, Anselmo Llorente, del Periódico La Nación 250 Este, Condominio Corporativo de la Cámara Costarricense de la Construcción, Piso 4, Oficina #407, con número de teléfono 2236-2894 / 2236-6259, correo electrónico info@blonecr.com; aprovecho la oportunidad para saludarles y presentarles la siguiente oferta para la contratación:

**RENOVACION DE LICENCIA ANUAL DE SOFTWARE ANTIVIRUS**
**LICENCIA ANUAL PROTECCION CORREO**

**CONTRATACION DIRECTA:** 2022CD-000033-0032000702
**FECHA MÁXIMA DE RECEPCIÓN DE OFERTAS:** 19 de abril del 2022.
**HORA DE APERTURA:** 2:00pm.

**LICENCIA DE ESET ENDPOINT SECURITY, VERSIÓN MÁS RECIENTE, COMPATIBILIDAD ÚLTIMAS VERSIONES DE WINDOWS, VIGENCIA 1 AÑO**

| | |
|---|---|
| **Sistemas Operativos Compatibles** | • Incorpora garantía de compatibilidad extendida para sistemas operativos 32bits y 64bits:<br>- Microsoft Windows® 11, 10, 8.1, 8, 7.<br>- Microsoft Windows Server 2022, 2019, 2016, 2012R2, 2012, 2008R2.<br>- macOS 12, 11, 10.15, 10.14, 10.13 y 10.12<br>- RedHat, Ubuntu, Suse<br>• Licenciamiento otorgado posee garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente se ocupara una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos<br>• Licenciamiento adquirido en su totalidad podrá ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e implementada en la red interna corporativa |

| | |
|---|---|
| **Aspectos Generales** | • Incorpora protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no depende del Sistema Operativo del "Endpoint/Cliente" tenga las actualizaciones y Service Pack al día<br>• Incorpora protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc<br>• Integra sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular es capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente<br>• Incorpora motor heurístico proactivo y preciso de tecnología avanzada, dicho motor es propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz<br>• Incorpora detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros<br>• Integralmente hablando producto instalado en el computador no presenta fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión)<br>• Permite importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables<br>• Incorpora capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que pueden ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica<br>• Incorpora capacidad de generar casos de soporte vía la interfaz gráfica de la solución<br>• Incorpora chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas<br>• Toda configuración a nivel de clientes, puede ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos se administran desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados<br>• Incorpora compatibilidad nativa en su interfaz gráfica con dispositivos |

| | |
|---|---|
| | que integren tecnología TouchScreen<br>● Incorpora cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local se validaran si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware es compatible con cualquier plataforma de virtualización, así como funcionalmente hablando requiere la instalación de ningún plugin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas"<br>● Solución a contratarse provisiona capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios pueden ser actualizados vía Internet inmediatamente después del arranque desde los mismos<br>● Solución a contratarse provisiona capacidad para generar CD y/o USB Booteables, los cuales ofrece como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante:<br>- Gparted<br>- MemTest86+<br>- Teamviewer<br>- Otras aplicaciones para recibir asistencia remota<br>- Otras<br>● Solución a contratarse cumple con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus figura en el listado de miembros activos de AMTSO<br>● Solución a contratarse incluye múltiples capas de seguridad, que operaran en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma garantiza proteger al endpoint final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante<br>● Incorpora protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso<br>● Incorporaauto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo |

| | |
|---|---|
| | inoperativo para protección del computador donde ha sido implementado<br>● Integra protección nativa de aprendizaje automático, la cual incluye mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección posee coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no requiere de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Integra protección nativa a nivel UEFI que permite comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulodetecta componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente norequiere de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador<br>● Instalación de producto tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere precompilación de un paquete todo-en-uno para la instalación del producto el cual contenga las preconfiguraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo se incorpora en un solo paso la unión y sincronización a consola administrativa<br>● Comunicación entre clientes administrados (endpoints) y servidor de administración se realiza mediante conexión SSL cifrada; dicha conexión es evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria<br>● Incorpora agente de conexión a provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo<br>● Incorpora agente de conexión a reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado<br>● Incorpora agente de conexión a reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente<br>● Incorpora agente de conexión a soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que |

| | |
|---|---|
| | desee ejecutarse o instalarse en los computadores administrados<br>● Nuestra solución incluye soporte técnico directo de ESET y el cual se encuentra localmente en formato 24x7x365; el mismo en sus modalidades se garantiza ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que BL ONE S.A por alguna razón no pueda proporcionarlo<br>● Integra nativamente consola de administración incluyendo soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado<br>● Incluye medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas<br>● Incluye experiencia comprobable con respecto al software para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren<br>● Incluye experiencia comprobable para la implementación, administración y soporte técnico con referencias de al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento para referencias dentro de territorio nacional, en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento de ESET<br>● Garantizamos en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio de BL ONE S.A y/o con ESET en cualquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar<br>● BL ONE S.A demuestra mediante documento oficial de ESET, el mismo que somos proveedores autorizados para el territorio nacional de sus productos. |

| | |
|---|---|
| **Host-basedIntrusionPreventionSystem** | ● Incorpora tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas, pero no limitadas requeridas:<br>- Bloquea archivos y/o aplicaciones para ejecución<br>- Permitir ejecutar archivos y/o aplicaciones basados en rutas de acceso y/o ficheros en particular<br>- Bloquea archivos y/o carpetas contra escritura y/o acceso<br>- Permite escritura y/o acceso para archivos y/o carpetas<br>- Bloquea escritura y/o modificación a llaves del registro de sistema<br>- Incorpora tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java<br>● Incorpora motor de inspección avanzada en memoria operativa que brinda protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación<br>● Incorpora protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función se refleja en el componente HIPS cargado en el sistema<br>● Incorpora protección especializada contra ataques del tipo ransomware, la misma es explícitamente visible dentro del apartado de configuración del producto final adquirido; específicamente el módulo especializado para la prevención del ransomware detectar y bloquear procesos cuyo comportamiento encuadre con la conducta del ransomware en general |
| **Cloud Protection** | ● Incorpora tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques 0-Day y/o campañas de propagación de malware lanzadas globalmente; dicho alcance se garantiza para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL<br>● Funcionalmente integración de tecnología “Cloud Protection” no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora tecnología basada en la nube y en tiempo real, que permite al usuario operador del endpoint verificar la reputación de los procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual<br>● Incorpora tecnología en la nube para la detección de código nuevo y |

| | |
|---|---|
| | emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar<br>● Incorpora tecnología "Antiphishing", de tal forma que previene al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas" |
| **Actualizaciones** | ● Las actualizaciones rutinarias de la base de definición de firmas, son pequeñas e incrementales; tanto para actualizaciones rutinarias como para repositorios de distribución (mirror). Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 1MB por cada firma de definición<br>● Funcionalmente una actualización rutinaria, son capaces de actualizar firmas antivirus, módulos y/o componentes del sistema antivirus; no incluyendo, pero no limitando la versión de familia del producto contratado y/o futuras versiones del producto adjudicado<br>● Incorpora capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; funcionalmente no requiere la instalación de módulos adicionales para tales fines, así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"<br>● Posee factibilidad para actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone"<br>● Las actualizaciones de distribución de firmas rutinarias (repositorios de firmas) se proveeran a los clientes antivirus internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado así mismo puede ofrecer métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas antivirus de distribución local; dicha opción se integraran mas no quedar limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; funcionalmente no requiere la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"<br>● Las actualizaciones diarias y rutinarias de los componentes del producto se podran realizar en tiempo real desde Internet o vía LAN Server (Mirror), en forma automática y sin necesidad de intervención del usuario<br>● Producto puede actualizarse automáticamente desde una unidad extraíble que contenga los ficheros rutinarios de actualización sin intervención alguna del usuario local o bien del personal técnico |
| **Filtrado de Red** | ● Incorpora capacidad de filtrado de protocolos, para todo el tráfico de |

| | |
|---|---|
| **y/o Protocolos de Comunicación** | red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. Funcionalmente no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales<br>● Incorpora filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), funcionalmente hablando debe ser capaz de filtrar cualquier comunicación de red segura así como no debe requerir de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>● Incorpora capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red<br>● Incorpora capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos<br>● Incorpora filtrado básico para listas URL y/o IP de acceso; de tal forma que se pueda controlar efectivamente accesos a los listados estáticos definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); funcionalmente no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora plugin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>● Incorpora tecnología avanzada que integra capas de seguridad previa al host a fin de prevenir la explotación de vulnerabilidades a nivel de red desde host remotos o locales, en forma explícita protegiendo el endpoint final contra vulnerabilidades conocidas que puedan afectar a nivel de red aun así no exista parche local instalado en el equipo que desea protegerse Mail; no debe requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control” |
| **Firewall & IDS** | ● Incorpora firewall/cortafuegos avanzado de doble vía; capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, funcionalmente no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● El firewall/cortafuegos incorporado es totalmente administrable desde cliente o desde consola administrativa, así como posee modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto<br>● Firewall/Cortafuegos incorporado posee facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red “segura” o bien se requiere un modo superior de |

| | |
|---|---|
| | protección en una red nueva y desconocida<br>● Incorpora IDS (IntrusionDetectionSystem) de host para la prevención de acceso no autorizado al computador a nivel de capa de red, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora protección anti “BOTNETS”, la cual faculte a la solución bloquear el acceso y comunicación a una red botnet así como alertar al usuario de dicha acción y anomalía detectada; funcionalmente no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”<br>● Incorpora Control de Vulnerabilidades a nivel de capa de red, el cual inspecciona y proteger a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, funcionalmente no requiere de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas” |
| **Antispam** | ● Incorpora solución antispam a nivel endpoint y posee filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>● Incorpora plugin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>● Provee capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción es posible realizarse desde el propio producto y/o consola de administración, así como permite definir dominios y/o direcciones en cada uno de estos apartados. |
| **Web Filtering** | ● Integra capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>● Incorpora capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación<br>● Faculte permitir y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering<br>● Provee posibilidad de agrupamiento en políticas de filtrado URL, |

| | |
|---|---|
| | siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios<br>● Integra capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log contiene toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"<br>● Integra capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"<br>● Integra toda regla y/o política para el control URL, puede ser fijada por horarios, días de la semana en particular y/o por usuarios en especifico |
| **Device Control** | ● Incorpora capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa; no requiere de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"<br>● Incorpora capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o permitir dispositivos portátiles y/o medios extraíbles tales como:<br>- Dispositivos de almacenamiento USB<br>- Dispositivos ópticos CD/DVD<br>- Impresoras USB<br>- Dispositivos de almacenamiento Firewire<br>- Dispositivos Bluetooth<br>- Tarjetas lectoras de memoria<br>- Dispositivos de imagen<br>- Modems<br>- Puertos LPT/COM<br>- Dispositivos portátiles (móviles)<br>● Incorpora funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado:<br>- Marca<br>- Modelo<br>- Serie<br>● Incorpora funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo. |

| | |
|---|---|
| | • Incorpora funciones avanzadas para el control de dispositivos mediante grupos de “dispositivos”, siendo posible asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo<br>• Incorpora toda regla y/o política para el control de dispositivos, puede ser fijada por horarios, días de la semana en particular y/o por usuarios en especifico |

## Consola de Administración

| | |
|---|---|
| **Generalidades** | • Servidor de administración y consola administrativa puede implementarse, así como proveer soporte multiplataforma compatible con al menos los siguientes sistemas operativos:<br>• Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003<br>• Microsoft Windows Server Core 2012R2, 2012, 2008R2, 2008 Core<br>• Microsoft Windows 8.1, 8, 7, Vista, XP (CAL Microsoft puede limitar el soporte extendido, más sin embargo solución administrativa deberá poder instalarse y ser compatible con sistemas indicados)<br>• RedHat, Debian, Ubuntu, Suse, Fedora &Mandrivaasí como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB<br>• Servidor de administración y consola administrativa ofrece compatibilidad para despliegue rápido mediante OVF; a fin de simplificar el despliegue de “Appliance Virtual” para el funcionamiento correcto de servidor administrativo de la solución adquirida<br>• Servidor de administración y consola administrativa puede implementarse sobre plataforma Windows mediante un paquete todo en uno que incluya todos los elementos requeridos para instalación simplificada, así como ofrezca un fácil despliegue de solución administrativa; dicho paquete deberá incluir por defecto a los motores de base de datos así como todo lo que integralmente requiere para su correcto funcionamiento el servidor y consola de administración<br>• Servidor de administración y consola administrativa ofrece compatibilidad con al menos las siguientes bases de datos:<br>○ MySQL 5.5 o superior<br>○ MS SQL Server 2008 R2 o superior<br>• Servidor de administración y consola administrativa ofrece una consolidada y completa administración de los productos adquiridos, así como en su totalidad indicar el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración<br>• Servidor de administración y consola administrativa ofrece posibilidad de integración con Active Directory, tanto para instalación remota de clientes, así como para autenticación local de administradores y roles de acceso a la misma<br>• Servidor de administración y consola administrativa ofrece diversos y |

| | |
|---|---|
| | variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente<br>● Servidor de administración y consola administrativa provisiona acceso web mediante servidor de aplicaciones JAVA<br>● Consola de administración deberá operar en su totalidad en modalidad web, así como integralmente deberá estar desarrollada y compilada sobre código JAVA<br>● Servidor de administración y consola administrativa ofrece posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma de facilitar la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores, así como receptores de políticas y estados de los clientes locales<br>● Consola de administración es totalmente web, así como funcionalmente deberá ser compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración<br>● Consola de administración web garantiza para al menos los siguientes navegadores en las versiones indicadas o superiores, sin requerir la instalación de algún plugin y/o complemento adicional del lado del cliente final:<br>- Firefox 20+<br>- Internet Explorer 10+<br>- Chrome 23+<br>- Safari 6+<br>- Opera 12+<br>● Consola de administración web ofrece por completo administración para todos los productos ofertados independientemente del sistema operativo donde corre cliente o servidor, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web<br>● Consola de administración incorpora Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red local; no debe requerir para dicha operación el uso de IIS o motor diferente al integrado nativamente por la solución<br>● Consola de Administración no requiere de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo, deberá permitir administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes |

| | |
|---|---|
| | • Consola de administración web no requiere para su funcionamiento u operar sobre plataformas ASP, JSP o PHP<br>• Consola de administración maneja múltiples tipos de Licencias de Software, en diferentes cantidades de equipos y fechas de expiración<br>• Consola de administración no requiere el uso de MMC (*Microsoft Management Console*) para el funcionamiento de la misma o como requisito de instalación<br>• En términos de una correcta administración se requiere que una configuración establecida para un determinado cliente (endpoint) pueda ser exportada, tanto desde la Consola de Administración, como desde el mismo cliente, para poder ser importada en otros clientes, de ser necesario<br>• Consola de administración faculta instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo<br>• Consola y servidor de administración no requiere System Center Configuration Manager (SCCM), CM12, CM0, ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; no figura en especificaciones del fabricante (web/datasheets)<br>• Servidor central de administración (consola/servidor) deberá ser compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad deberá garantizar funcionamiento correcto con versiones “libre de pago” de dichas bases de datos (MySQL CommunityEdition& MS SQL Server Express)<br>• Servidor central de administración deberá proveer compatibilidad con SYSLOG en forma nativa, de tal forma que los eventos ocurridos en los clientes puedan ser interpretados por un syslog server<br>• Consola y servidor de administración no requiere Microsoft MessageQueue como requisito para instalación y/o operación<br>• Consola/Servidor deberá provisionar doble factor de autenticación (2FA) para su interfaz web de administración; nativamente deberá ofertarse al menos en forma gratuita hasta cinco operadores y no deberá requerir de hardware/software que requiera pago o licenciamiento adicional |

**Protección de seguridad para el correo electrónico & Office365 |1 AÑO**

| | |
|---|---|
| **Protección nativa para Microsoft Exchange Server** | • Incorpora protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange en forma totalmente transparente, dicha funcionalidad permite realizarla tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en componentes de programa en “Agregar quitar |

| | |
|---|---|
| | Programas -> Panel de Control”<br>• Integra funcionalmente protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange; no requiere de instalación y/o módulo reflejado en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>• Integra funcionalmente protección antimalware para la base de datos embebida a Microsoft Exchange, de forma tal que pueda protegerse cada buzón de usuario e inclusive realizar análisis retrospectivo para los buzones de correo electrónico que pudiesen haber recibido código malicioso previo a la instalación de dicha solución de seguridad; no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>• Integra funcionalmente protección antimalware integrada directamente a la base de datos ocupada por Microsoft Exchange, que de forma tal proteja del envió/recepción de código malicioso inclusive cuando se ocupa portal web provisionado por Microsoft Exchange (OWA); no requiere de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>• Integra funcionalmente protección a nivel de transporte para Microsoft Exchange, de forma tal que al menos pueda realizar lo siguiente:<br>○ Filtrar correos electrónico basado en el tipo de documento adjunto (identificador por tipo de ficheros)<br>○ Filtrar correos electrónicos basado en el contenido del adjunto (identificador de ficheros por tipo y uso)<br>○ Filtrar correos electrónicos basado en el contenido del cuerpo del mensaje (body message), de forma tal que pueda identificar características, texto o similar contenido en el mismo<br>○ Filtrar correos electrónicos por tipo de extensión (filtrado de extensiones permitidas)<br>○ Filtrar correos electrónicos por tamaño del mensaje<br>○ Filtrar correos electrónicos que hayan sido enviados a multiples usuarios (cadenas de mensaje)<br>○ Delimitar cadenas de mensajes o bien identificar y bloquear por medio de contadores cualquier tipo de correo electrónico que encuadre en identificación de cadenas de mensajes (dirigido en forma especifica una cantidad de usuarios por definir y totalmente variable, ej: 10, 30, 33 destinatarios en un solo mensaje)<br>• Incorpora solución antispam a nivel endpoint y posee filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe requerir de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”<br>• Incorpora plugin para el filtrado, análisis y clasificación antispam en los |

| | |
|---|---|
| | clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no requiere de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"<br>• Provea capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción es posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados. |
| **Protección en la nube para O365** | • Incorpora motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación, de forma tal que podrá integrarse hacia plataformas Office 365 mediante servicio SaaS integrado directamente al tenant de Microsoft 365<br>• El nivel de alcance y protección en la nube al menos deberá garantizarse e integrarse en forma fácil y precisa con las plataformas:<br>○ Microsoft OneDrive for Business<br>○ Microsoft Exchange Online<br>○ Microsoft Sharepoint Online<br>○ Microsoft Teams<br>○ Compatibilidad de protección para Microsoft O365 planes<br>▪ Microsoft 365 Empresa Básico<br>▪ Microsoft 365 Empresa Estándar<br>▪ Microsoft 365 Empresa Premium<br>▪ Aplicaciones Microsoft 365<br>• Solución cubre la totalidad de usuarios solicitados para protección en la nube para las aplicaciones en la nube para Microsoft 365, de forma que garantizará la inspección de todo correo electrónico y/o fichero almacenado sobre Microsoft OneDrive for Business & Sharepoint Online<br>• Incorpora tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques 0-Day y/o campañas de propagación de malware lanzadas globalmente; dicho alcance garantiza para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL<br>• Funcionalmente integra tecnología "Cloud Protection integra mediante API Cloud<br>• Incorpora tecnología sandboxing basada en la nube que integra al menos tres modelos de aprendizaje deep-learning (Deep Machine Learning) asi como al menos seis modelos de clasificación para cada modelo Deep Machine Learning aplicado<br>• Garantiza protección integrada mediante API cloud para cualquier tipo de fichero mediante análisis cloud sandboxing, así como automáticamente y sin intervención alguna del usuario clasifique, detecte y/o elimine cualquier código malicioso nuevo o desconocido<br>• Incorpora tecnología en la nube para la detección de código nuevo y |

| | |
|---|---|
| | emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar<br>• Incorpora tecnología "Antiphishing", de tal forma que prevenga al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos<br>• Provee auditoria detallada de las acciones ejecutadas sean estas para tratamiento antispam, antivirus y/o phishing, no importando y no delimitando acciones tomadas para Microsoft OneDrive for Business & Microsoft Sharepoint Online<br>• Integra funcionalmente protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange Online (Office365) en forma totalmente transparente, dicha funcionalidad realiza tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en cualquier computador interno a la red y visible desde componentes de programa en "Agregar quitar Programas -> Panel de Control"<br>• Integra protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange Online<br>• Provee capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción permite realizarse desde el propio producto y/o consola de administración, así como permite definir dominios y/o direcciones en cada uno de estos apartados. |

| | |
|---|---|
| | • Eset cuenta con presencial local en Costa Rica, se adjunta certificación de la cedula jurídica con no mas de 3 meses de emitida.<br>• Se incluye instalación en el sitio por parte de personal técnico de la empresa adjudicada especializado y certificado por la solución para su debida implementación.<br>• Soporte técnico bajo demanda (sin costo adicional), durante los 24 meses, bajo los siguientes esquemas: correo electrónico, llamada telefónica, chat, asistencia remota y presencial; con un tiempo de respuesta máximo de 24 horas suministrado directamente por BL ONE y se podrá suministrar también directo del Fabricante (ESET COSTA RICA). Cuando sea asistencia remota se garantiza el nivel de privacidad mediante canales SSL de grado empresarial y se utiliza tecnología auditable en caso de requerirse bitácoras de atención.<br>• Se adjunta carta de distribuidor Directo Autorizado, el mismo indica nuestro grado de categorización de Partner Gold. Contamos con 10 años de experiencia en el mercado nacional distribuyendo productos iguales o similar a lo ofertado.<br>• El soporte técnico brindado en idioma español, estrictamente brindado por personal nativo del lenguaje español.<br>• La garantía de soporte de ofrecer cobertura extendida en modalidad 24x7x365. (Presencial, remoto, chat en línea, correo electrónico y/o vía telefónica mediante número local). Soporte técnico mediante su página web, el mismo cuenta con sistema automatizado de tickets, que permita el reporte, revisión y ejecución de los casos de soporte registrados en la misma plataforma. El sistema permite la creación de usuarios para el cliente final e ingreso seguro a la plataforma. Se adjunta el enlace o dirección electrónica para demostrar que se cumple con estos requisitos. https://soporteblonecr.freshdesk.com/support/home<br>• Se adjunta copia de título de al menos CUATRO técnicos certificados por el fabricante de la empresa oferente. Al menos uno cuenta con 9 años de Certificado (a demostrar con el título solicitado) y se encargará principalmente de la cuenta y los casos de soporte atendidos por la Administración. Al menos 1 Técnico cuenta con Bachillerato en Ingeniería Informática. Todos los técnicos forman parte de la planilla de la CCSS de la empresa. (se demuestra)<br>• Para que la Administración se garantiza que el nivel de soporte a es adecuado y a la altura de la seriedad de la Seguridad Informática, contamos con 2 Técnicos Certificados en CCNA (se adjunta los certificados debidamente foliados y firmados por la Universidad, para los siguientes módulos:<br>➢ IT ESSENTIALS: PC Hardware and Software<br>➢ Introduction to Networks<br>➢ Routing and Switching Essentials |

BL ONE S.A.
Cédula Jurídica: 3-101- 634194
Telefax:2236-2894
email: info@blonecr.com

| | |
|---|---|
| | • Se incluye una Capacitación Técnica para la adecuada transferencia de conocimientos de la solución completa, incluyendo los detalles de planificación, configuración e implementación de la misma hacia el personal asignado por LA INSTITUCIÓN, mínimo 5 personas. El mismo será teórico-práctico. La capacitación técnica no se brindará a personal OUTSOURCING.<br>• Visitas programadas de revisión de consola en el sitio durante el periodo licenciado realizadas por BL ONE (cada 2 meses)<br>• Se incluye al menos 5 cartas con referencias comerciales del sector público o privado de instituciones y/o empresas que cuenten con producto igual o similar al ofertado suministrado por el oferente en más de 300 estaciones de trabajo.<br>• Garantizamos soporte técnico mediante página web, el mismo cuenta con la posibilidad de permitir chat y asistencia remota para la atención de los mismos.<br>• Se incluye charlas de concientización a los usuarios finales de la institución con el objetivo de aumentar el conocimiento de los mismo en temas de Seguridad informática a elegir por la Municipalidad. Las mismas son impartidas por el fabricante y el partner (ESET – BL ONE) |

## OFERTA ECONÓMICA

| CANT | DESCRIPCION DEL ARTÍCULO | PRECIO UNIT | PRECIO TOTAL |
|---|---|---|---|
| 115 | RENOVACION DE LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY | ₡ 13,929.72 | ₡ 1,601,917.80 |
| 95 | RENOVACION DE LICENCIAS DE ESET CLOUD OFFICE SECURITY | ₡ 12,656.64 | ₡ 1,202,380.80 |
| | ENTREGA DE 2 DÍAS HABILES CONTRA ORDEN DE COMPRA<br>VIGENCIA DE 1 AÑO A PARTIR DEL LICENCIAMIENTO | | |
| | | SUBTOTAL | ₡ 2,804,298.60 |
| | | IMP. VENTAS | ₡ - |
| | | TOTAL | ₡ 2,804,298.60 |

TOTAL: Dos millones ochocientos cuatro mil doscientos noventa y ocho colones con 60/100

**Prorroga #1**

| CANT | DESCRIPCION DEL ARTÍCULO | PRECIO UNIT | PRECIO TOTAL |
|---|---|---|---|
| 115 | RENOVACION DE LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY | $ 20.85 | $ 2,397.75 |
| 95 | RENOVACION DE LICENCIAS DE ESET CLOUD OFFICE SECURITY | $ 19.09 | $ 1,813.55 |
| | ENTREGA DE 2 DÍAS HABILES CONTRA ORDEN DE COMPRA<br>VIGENCIA DE 1 AÑO A PARTIR DEL LICENCIAMIENTO | | |
| | | SUBTOTAL | $ 4,211.30 |
| | | IMP. VENTAS | $ - |
| | | TOTAL | $ 4,211.30 |

TOTAL: Cuatro mil doscientos once dolares con 30/100

BL ONE S.A.
Cédula Jurídica: 3-101- 634194
Telefax:2236-2894
email: info@blonecr.com

**Prorroga #2**

| CANT | DESCRIPCION DEL ARTÍCULO | PRECIO UNIT | PRECIO TOTAL |
|---|---|---|---|
| 115 | RENOVACION DE LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY | $ 20.85 | $ 2,397.75 |
| 95 | RENOVACION DE LICENCIAS DE ESET CLOUD OFFICE SECURITY | $ 19.09 | $ 1,813.55 |
| | ENTREGA DE 2 DÍAS HABILES CONTRA ORDEN DE COMPRA<br>VIGENCIA DE 1 AÑO A PARTIR DEL LICENCIAMIENTO | | |
| | | SUBTOTAL | $ 4,211.30 |
| | TOTAL: Cuatro mil doscientos once dolares con 30/100 | IMP. VENTAS | $ - |
| | | TOTAL | $ 4,211.30 |

**Prorroga #3**

| CANT | DESCRIPCION DEL ARTÍCULO | PRECIO UNIT | PRECIO TOTAL |
|---|---|---|---|
| 115 | RENOVACION DE LICENCIA DE ANTIVIRUS ESET ENDPOINT SECURITY | $ 20.85 | $ 2,397.75 |
| 95 | RENOVACION DE LICENCIAS DE ESET CLOUD OFFICE SECURITY | $ 19.09 | $ 1,813.55 |
| | ENTREGA DE 2 DÍAS HABILES CONTRA ORDEN DE COMPRA<br>VIGENCIA DE 1 AÑO A PARTIR DEL LICENCIAMIENTO | | |
| | | SUBTOTAL | $ 4,211.30 |
| | TOTAL: Cuatro mil doscientos once dolares con 30/100 | IMP. VENTAS | $ - |
| | | TOTAL | $ 4,211.30 |

BENJAMIN PINEDA AVILA (FIRMA)

Firmado digitalmente por BENJAMIN PINEDA AVILA (FIRMA)
Fecha: 2022.04.19 12:22:12 -06'00'

## CONDICIONES GENERALES

- Se participa a nombre de BL ONE S.A.
- Los precios cotizados son firmes y definitivos.
- Vigencia de la oferta 30 días hábiles
- Ponemos a disposición los siguientes datos para notificaciones: teléfono 2236-2894, correo electrónico info@blonecr.com, dirección Tibás, de Grupo Nación 250 este, edificio corporativo de la Cámara de Costarricense de la Construcción, cuarto piso, oficina 407.
- Para efectos de pago mediante transferencia electrónica mediante SINPE disponemos de la siguiente cuenta: Banco Nacional de Costa Rica Cuenta Cliente: 15111510010000377

BL ONE S.A.
Cédula Jurídica: 3-101- 634194
Telefax:2236-2894
email: info@blonecr.com

# DECLARACION JURADA

**Persona jurídica**

Yo; Benjamin Pineda Ávila, mayor, Divorciado, Representante Legal, Vecino de: Tibás, del Pali de Colima 150 norte, portador de la cédula de identidad número: 1-1306-0936 en su condición de apoderado o representante, con facultades de apoderado generalísimo sin límite de suma, de la sociedad denominada: BL One S.A, cédula jurídica número: 3-101-634194; inscrita en la sección mercantil del Registro Público al tomo: 2011, asiento 90620; **DECLARO BAJO LA FE DEL JURAMENTO**, en conocimiento de las sanciones con que el Código Penal castiga el delito de perjurio, y falso testimonio, lo siguiente:

1. Que todos los datos indicados en el formulario de inscripción al Registro de Proveedores son ciertos y que los documentos aportados son veraces y correctos.
2. Que no me afectan ninguna de las prohibiciones establecidas por el **Artículo 22 bis de la Ley de Contratación Administrativa.**
3. Que no me encuentro inhabilitado para contratar con la Administración Pública, según las causales que establece el **Artículo 100 de la Ley de Contratación Administrativa.**
4. Que me encuentro al día en el pago de todo tipo de impuestos nacionales, según lo establecido en el **Artículo 65, a del Reglamento a la Ley de Contratación Administrativa.**
5. Que no me encuentro afecto por las incompatibilidades según lo establecido por **el Artículo 18 DE LA LEY CONTRA LA CORRUPCIÓN Y EL ENRIQUECIMIENTO ILÍCITO EN LA FUNCIÓN PÚBLICA, N.º 8422**
6. Que no me encuentro inhabilitado para contratar con la Administración Pública, ni he sido sancionado en ninguna de sus formas por incumplimientos u otros, según **el Art.19 del Reglamento de la Ley de Contratación Administrativa y el Art. 117 de la Ley de Contratación Administrativa.**
7. Que no tengo deuda alguna con la Caja Costarricense de Seguro Social.
8. Que no nos encontramos en estado de insolvencia o quiebra.
9. Aceptamos cumplir con las prórrogas según corresponde e indica la contratación.
10. Asimismo, declaro que mi representada está constituida como una empresa dedicada a servicio y soporte técnico, venta de equipo de cómputo y distribución de soluciones antimalware, que estamos ubicados en: Del periódico La Nación 250 metros al este, condominio corporativo de la cámara de la construcción piso 4, oficina 407

Hago la presente declaración jurada consciente del valor, alcance y trascendencia de mis declaraciones. Con Fecha del 19 de abril del 2022.

BENJAMIN PINEDA AVILA (FIRMA)

Firmado digitalmente por BENJAMIN PINEDA AVILA (FIRMA)
Fecha: 2022.04.19 12:21:35 -06'00'

Benjamín Pineda Ávila
**Representante Legal**