Sistema Integrado de Gestión Administrativa
Módulo de Logística
Versión 20.06.00.U2

H.E 2082-2021-DD

Fecha : 26/05/2021
Hora : 12:23
Página : 1 de 1

PEDIDO DE COMPRA Nº 00577

H.E 3051.. 0P..

GRC CAJAMARCA
SGD
EXPEDIENTE
Nº 2021-34

UNIDAD EJECUTORA : 001 GOBIERNO REGIONAL CAJAMARCA
NRO. IDENTIFICACIÓN : 000775

Tipo Uso : Consumo

Dirección Solicitante : DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL
Entregar a Sr(a) : TORRES VARGAS DEIVHY PAUL
Fecha : 24/05/2021
Actividad Operativa : C0054 MANTENIMIENTO DE EQUIPOS COMPUTACIONALES Y DE COMUNICACION
Motivo : ADQUISICIÓN DE SOFTWARE ANTIVIRUS PARA LA SEDE DEL GOBIERNO REGIONAL DE CAJAMARCA.

- Se adjunta especificaciones técnicas.

FF/Rb	META / MNEMONICO	Función	División Func.	Grupo Func.	Programa	Prod/Pry	Act/Ai/Obr
1-00	0027	03	004	0005	9001	3999999	5000001

Código	Descripción / Especificaciones Técnicas	Clasificador	Cantidad	Unidad Medida
140400031765	SOFTWARE (INC. LICENCIA) ANTIVIRUS Y ANTISPAM	2.6. 6 1. 3 2	650.00	UNIDAD
140400031925	SOFTWARE (INC. LICENCIA) PARA SERVIDOR DE BASES DE DATOS	2.6. 6 1. 3 2	50.00	UNIDAD

350000

GOBIERNO REGIONAL DE CAJAMARCA
DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL
Mg. Ing. Deivhy Paul Torres Vargas
DIRECTOR

Firma del Solicitante

GOBIERNO REGIONAL CAJAMARCA
CONTROL PREVIO

GOBIERNO REGIONAL DE CAJAMARCA
DIRECCIÓN REGIONAL DE ADMINISTRACIÓN
PARA: Abastecimiento
TRAMITE: De acuerdo a norma
FECHA: 28/05/2021 FIRMA:

GOBIERNO REGIONAL
Dirección Regional de Administración

Firma Autorizada

Miguel

ESPECIFICACIONES TÉCNICAS: ADQUISICIÓN DE SOFTWARE ANTIVIRUS PARA LA SEDE DEL GOBIERNO REGIONAL DE CAJAMARCA

1. AREA USUARIA:

Dirección Regional de Transformación Digital.

2. FINALIDAD PÚBLICA:

El Gobierno Regional de Cajamarca cuenta con PC´s de escritorio, PC´s portátiles y servidores; los cuales necesitan ser protegidos de ciberamenazas. Con el fin de garantizar la disponibilidad de los servicios que se brindan a la ciudadanía de la región Cajamarca.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Adquirir Seiscientas Cincuenta (650) licencias de software antivirus por un período de vigencia de un (01) año, con el fin de brindar protección a los equipos de cómputo (PCs de escritorio y portátiles, Servidores); ante ciberamenazas provocadas por software malicioso

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

3.2. OBJETIVOS ESPECÍFICOS

- Brindar seguridad a los equipos informáticos de la Sede del Gobierno Regional de Cajamarca.
- Implementar la solución de forma centralizada en todos los equipos informáticos de la Sede del Gobierno Regional de Cajamarca.
- Brindar capacitación en el uso de la solución ante las amenazas actuales de seguridad.

4. PLAN OPERATIVO INSTITUCIONAL

Tarea POI: Equipamiento y Funcionamiento Institucional

5. DESCRIPCIÓN DE LA ADQUISICIÓN DE LA SOLUCIÓN

Ítem	Descripción	Unidad de Medida	Cantidad
1	Licencias de software antivirus Endpoint por un período de un (01) año	Unidad	650
2	Licencias de Software Endpoint Detection and Response	Unidad	50

5.1. CARACTERÍSTICAS DEL SOFTWARE ANTIVIRUS

Funcionalidades Específicas

- Bloqueo de virus y malware
  - ✓ Analizar, detectar y eliminar ciberamenazas más recientes.
  - ✓ Inteligencia artificial y el análisis de comportamiento para bloquear virus y malware, y aislar archivos sospechosos. Ejecución en segundo plano para que la PC siga funcionando sin problemas.

- Protección en tiempo real
  - ✓ Proporcionar protección en tiempo real mediante niveles predefinidos de protección o personalizado por el usuario de acuerdo a sus requerimientos.
  - ✓ El módulo de detección en tiempo real debe proteger contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, spam, malware, herramientas de control remoto y otros programas potencialmente peligrosos.

- Protección contra amenazas de día cero
  - ✓ El fabricante de la solución deberá ofrecer protección contra amenazas de día cero. Las firmas deben estar basadas en patrones que ayuden a mejorar las tasas de detección de malware y reduzcan el tamaño de las actualizaciones de la base de datos, para mejorar la seguridad y reducir la carga en la red.

- Protección Proactiva en el host
  - ✓ La solución antivirus deberá monitorear automáticamente cómo se comportan las aplicaciones cuando se ejecutan en sus sistemas. Si detecta un comportamiento sospechoso, la solución deberá bloquear la aplicación.

- Protección Proactiva en la red
  - ✓ Contar con tecnología que detecte actividades sospechosas en una red corporativa y que las monitorea. Además, de pre configurar cómo los sistemas responderán en caso de que se identifique un comportamiento sospechoso

- Prevención de Exploits

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

- ✓ Impedir que el malware explote vulnerabilidades de los sistemas operativos o aplicaciones que se ejecutan en la red.

.

- Sistema de Prevención de Intrusos
  - ✓ Contar con un sistema de prevención de intrusiones basado en host y un firewall personal que brindan un control flexible sobre el tráfico de entrada y salida. Puede establecer parámetros para puertos, direcciones IP o aplicaciones específicos.
- Escaneos Personalizados
  - ✓ Escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas
- Protección por contraseña
  - ✓ El producto debe pedir una contraseña ante intentos de cambio indebidos en su configuración.
- Componentes de la Solución: la solución debe contar con los siguientes componentes:
  - ✓ Agente que le permita ser administrado desde una consola centralizada.
  - ✓ Cliente antivirus
- Control Web
  - ✓ Monitoreo y filtrar el uso del navegador web de cada empleado. Permitir, prohibir, limitar o auditar el acceso de los usuarios a sitios web o categorías de sitios web específicos, como sitios de juegos, de apuestas o de redes sociales.
- Control de Dispositivos:
  - ✓ Herramientas de control de dispositivos para la administración de dispositivos extraíbles (USB, CD-ROM) y proteger contra los riesgos de seguridad que pueden añadir los dispositivos no autorizados. La solución debe permitir: Administrar privilegios de acceso para un tipo específico de dispositivo, un bus o un dispositivo individual (según su número de serie único). Pre configurar los momentos en que se aplican sus políticas de control de dispositivos, tales como evitar el uso de dispositivos fuera de los horarios de oficina normales

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

- Cifrado
  - ✓ Debe permitir elegir entre el nivel de disco completo o el de archivo, respaldado por el algoritmo Advanced Encryption Standard (AES), con cifrado de 256 bits, permitiendo proteger información empresarial de vital importancia en caso de robo o pérdida de dispositivos.
  - ✓ Compatibilidad con dispositivos extraíbles que permita aumentar la seguridad mediante políticas que aplican el cifrado de datos en dispositivos extraíbles.
  - ✓ Uso compartido de datos seguros, que permita a los usuarios crear fácilmente paquetes cifrados y autoextraíbles para garantizar que los datos estén protegidos al compartirlos mediante dispositivos extraíbles, correo electrónico, redes o la web.
  - ✓ Transparencia para usuarios finales, la solución de cifrado debe ser invisible para los usuarios y no deberá tener efectos negativos en la productividad. Sin repercusiones en la configuración de las aplicaciones ni en las actualizaciones

- Modalidad de actualizaciones
  - ✓ Ejecución desatendida e incremental, y manual de actualización de firmas y componentes

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

Soporte a Sistemas Operativos

- Sistemas Operativos Cliente: Windows 7 o Superior, Mac OS, Linux; de 32 y 34 bits según corresponda.
- Sistemas Operativos Servidor: Windows Server 2012 o Superior Linux CentOS 7 o superior de 32 y 64 bits según corresponda.
- Sistemas Operativos para móviles: Android y iOS

Protección de Correo Corporativo Múltiples plataformas

- Protección de múltiples plataformas, compatible con una amplia gama de servidores de correo, incluidos Microsoft Exchange, IBM Lotus Notes/Domino, Sendmail, qmail, Postfix.
- Filtrado de spam
- Protección del tráfico, mediante protección al tráfico que circula por las puertas de enlace más populares basadas en Windows o Linux, pues eliminan de manera automática los programas potencialmente hostiles y maliciosos que aparecen en el tráfico HTTP(S), FTP, SMTP y POP3

Herramientas de Gestión Centralizada

- La solución antivirus debe poseer una consola de administración centralizada de; la cual pueda reportar el estado de todos los equipos conectados a la red corporativa, esta consola deberá ser de tipo escritorio y web.

- Análisis de Vulnerabilidades Centralizado

  ✓ La solución antivirus deberá realizar tareas de análisis automático de vulnerabilidades para detectar vulnerabilidades sin parchar en el sistema operativo Windows y de aplicaciones de terceros.

  ✓ Las funciones de búsqueda de vulnerabilidades y administración de parches deben automatizar el proceso de mitigar las vulnerabilidades de software.

  ✓ Las vulnerabilidades detectadas pueden priorizarse automáticamente y las actualizaciones y los parches pueden distribuirse de manera automática.

- Administración de activos hardware y software centralizado

  ✓ La solución debe permitir la administración de los activos de hardware y software.

  ✓ Todos los dispositivos de la red deben detectarse y registrarse automáticamente en inventarios de hardware y software.

  ✓ El inventario de hardware deberá contener información detallada sobre cada dispositivo, mientras que el inventario de software ayudará a controlar el uso de aplicaciones y a bloquear las que no están autorizadas.

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

- Instalación de Software de Terceros de forma centralizada

  ✓ La solución debe permitir la distribución de aplicaciones, mediante la implementación centralizada (instalación) de software que no sean de la solución (software de terceros).

- Implementación de Sistemas Operativos

  ✓ La solución debe permitir la automatización y optimización de la implementación de sistemas operativos, por tal debe automatizar y centralizar la creación, el almacenamiento y la clonación y distribución de imágenes de sistema operativo.

  ✓ La solución debe de ofrecer funciones automáticas para crear y clonar imágenes de equipo, debe ayudar en optimizar la implementación de sistemas operativos.

- Distribución descentralizada para oficinas remotas

- ✓ La solución debe apoyar en la reducción del tráfico en tareas de distribución remota; mediante estaciones de trabajo asignadas como agentes de actualización para oficinas remotas.

- Integración con herramientas SIEM
  - ✓ La solución deberá Integrarse con sistemas SIEM, por tal deberá ser capaz de integrarse a los principales sistemas SIEM.

- Actualizaciones de Windows
  - ✓ La solución antivirus debe sincronizar con regularidad los datos de las actualizaciones y revisiones de Microsoft para distribuirlas a sus sistemas de forma automática.
  - ✓ Para muchas aplicaciones que no son de Microsoft, la solución antivirus deberá proporcionar otras formas de sincronización para parchar vulnerabilidades.

- Herramientas de soporte remoto
  - ✓ La solución debe ofrecer herramientas de acceso remoto que apoye a la rápida resolución de problemas en cualquier equipo de la red corporativa mediante el protocolo RDP

- Descubrimiento de dispositivos en la red
  - ✓ La solución deberá tener la capacidad de descubrir dispositivos de forma automática, que permita controlar quienes pueden acceder a la red corporativa y quiénes no.
  - ✓ También debe cumplir con funciones de comprobación de cumplimiento de políticas de seguridad corporativas de los dispositivos de red y bloquear el acceso a la red a todo dispositivo que no lo haga.
  - ✓ Posibilidad de crear un portal cautivo para acceso a internet de los dispositivos visitantes.

- Plataformas soportadas por el software de gestión
  - ✓ Windows Server 2012 R2 o superior.

- Creación de Grupos administrativos
  - ✓ El producto debe ser capaz crear grupos administrativos y agregar a ellos automáticamente una PC nueva que ingresa a la red.

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

- Instalación automática del software antivirus
  - ✓ El producto debe ser capaz de automáticamente instalar el antivirus en aquellas PC's nuevas que ingresen a la red
- Monitoreo Centralizado
  - ✓ La solución antivirus debe de proporcionar una visibilidad detallada de todos activos de TI
  - ✓ Monitorear el estado de seguridad de los sistemas
  - ✓ Aplicar ajustes de seguridad necesarios
  - ✓ Centralizar aprovisionamiento de licencias de software y detectar infracciones a las condiciones de licencia
- Despliegue centralizado de actualizaciones de la solución
  - ✓ Actualizaciones descargadas centralizadamente, para que clientes actualicen desde un servidor de administración sus definiciones de virus, phishing, spam, actualización de parches del producto entre otras.
- Gestión de vulnerabilidades y parches de software de terceros
  - ✓ La solución debe permitir realizar análisis exhaustivos avanzados de vulnerabilidades combinado con distribución automatizada de parches de software de terceros
- Despliegue de software de terceros en remoto
  - ✓ Instalación y remoción de software de la solución de software de terceros de forma centralizada en los equipos cliente, incluso en sucursales
- Despliegue de imágenes de sistemas operativos y aplicaciones
  - ✓ La solución de gestión deberá permitir la creación, almacenamiento y despliegue de imágenes de sistema desde una ubicación centralizada
- Gestión de hardware, software y licencias
  - ✓ La solución de gestión deberá proporcionar informes de inventario de hardware y software; contribuyendo a mantener el control de las obligaciones de licencia de software
- Generación de Backups
  - ✓ La consola debe ser capaz de permitir realizar un backup de las configuraciones

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

realizadas en el sistema

- Generación de Alertas
  - ✓ El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo, el envío de mensajes de red o la ejecución de un archivo.
  - ✓ Generar eventos de infecciones y ser notificados por medios como alertas de registro y correo electrónico.
- Reportes
  - ✓ Los reportes deberán ser gráficos para la toma de decisiones y deberán ser mostrados en formatos XML, PDF o HTML, los cuales pueden ser programados para envío por correo
- Facilidad de Uso
  - ✓ El software debe ser de fácil uso
- Soporte
  - ✓ El software debe contar con un soporte por el período de vigencia de la licencia, dicho soporte deberá ser responsabilidad el proveedor y del fabricante

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

5.2. CARACTERÍSTICAS DEL SOFTWARE ENDPOINT DETECTION AND RESPONSE

- La solución debe permitir visibilidad en tiempo real, detección y respuesta automatizada de todas las actividades ejecutadas en los Endpoint.
- La solución debe ser capaz de recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
- El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciber espionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.
- La solución para estaciones de trabajo debe brindar soporte a los siguientes sistemas operativos:
  - ❖ Windows 7, Windows 8 y Windows 10 32 y 64 bits.
  - ❖ Windows Server 2012, 2012 R2, Windows Server 2016 y Windows Server 2019 de 32 y 64 bits.
- La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.

- El agente EDR puede estar integrado o no a la solución de Endpoint Security, sin embargo debe ser del mismo fabricante.
- La solución de EDR debe ser gestionar las políticas, agentes y reportes desde la misma Consola de administración del ANTIVIRUS SOLICITADO EN EL PRESENTE REQUERIMIENTO..
- El agente EDR se debe poder configurar a través de la interfaz de línea de comandos.
- La solución debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección, y luego tener la capacidad de aplicar una acción de respuesta.
- La solución debe tener la capacidad de ejecutar el escaneo con la información de IoC en todos los puntos finales donde se ejecute el agente EDR de acuerdo con una planificación indicada por el administrador.
- La solución debe admitir la importación de IoC de terceros en formato Open IoC para su uso en el escaneo de los equipos.
- La solución debe permitir tener visibilidad detallada del incidente relacionado con la amenaza detectada en un Endpoint, el incidente debe incluir como mínimo la siguiente información:
    - ❖ Gráfico de la cadena de desarrollo de amenazas (kill chain).
    - ❖ Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
    - ❖ Información general sobre la detección, incluido el modo de detección.
    - ❖ Cambios de registro asociados a la detección.
    - ❖ Historial de presencia de archivos en el dispositivo.
    - ❖ Acciones de respuesta realizadas por la aplicación.
- La información de la cadena de desarrollo de la amenaza (kill chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre los procesos ejecutados en el dispositivo, conexiones de red, bibliotecas, llave de registro entre otras.
- La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz como por ejemplo:
    - ❖ Proceso de spawning
    - ❖ Conexiones de red
    - ❖ Cambios en el registro

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

- Descarga de archivos
- Dropped de objetos

- El agente EDR debe tener un mecanismo de autodefensa para evitar que se modifique archivos relacionados con su funcionamiento como las entradas de componentes del sistema.

6. PRESTACIONES ACCESORIAS

6.1. SOPORTE TÉCNICO

- El proveedor deberá de brindar el soporte correspondiente en casos de incidencias complejas que requieran asistencia técnica especializada. Dicho soporte será contemplado por el tiempo de licenciamiento (doce meses)
- El soporte será brindado por el período de vigencia de la licencia
- Dicho soporte deberá ser responsabilidad el proveedor y del fabricante
- El soporte comprende en actualizaciones de versiones, incidentes suscitados con la solución, protección ante nuevas amenazas de malware.
- Soporte técnico gratuito vía teléfono, correo y asistencia remota on-line 24x7
- Soporte de fábrica vía teléfono, chat, foros y apertura de casos
- Se deberán realizar auditorías internas (REMOTAS), con la finalidad de reducir y prevenir futuras incidencias cada 2 meses durante el periodo de licencia.

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

6.2. CAPACITACIÓN:

- El postor deberá brindar una capacitación de la solución implementada y deberá considerar como mínimo los siguientes temas:
  - Funcionalidad y gestión de la solución.
  - Implementación Centralizada de la solución en plataformas Windows y Linux
  - Implementación de imágenes de sistemas operativos, e implementación centralizada.
  - Tendencias para la protección contra nuevas amenazas como rasomware, y como la solución nos ayuda contra estas nuevas amenazas.
- El número de horas de capacitación deberá ser de mínimo 8 horas.
- La capacitación deberá darse virtualmente.
- El postor deberá proveer de manuales ya sea en formato digital o físico de la solución para efectos de la capacitación.

- El número de participantes para la capacitación serán de mínimo 4 personas y un máximo de 13 personas, las cuales serán designadas por el responsable de la Dirección Regional de Transformación Digital.
- El postor está en la obligación de emitir un certificado o constancia de capacitación a cada uno de los participantes, en el cual se debe detallar fecha y número de horas de la capacitación en la solución adquirida.

7. REQUISITOS DEL PROVEEDOR

7.1. DEL PROVEEDOR

- Persona Natural o jurídica
- Contar RNP vigente.
- Contar con Código de Cuenta Interbancaria.
- Experiencia en venta de software antivirus de mínimo un (01) año.

Acreditación:

La experiencia del postor se acreditará con copia simple de contratos u órdenes de compra correspondientes a los tres últimos años contados a partir del presente requerimiento.

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

7.2. DEL PERSONAL

- El postor debe contar con 01 Ingeniero o Técnico Certificado por el fabricante como mínimo, y debe ser acreditado presentando copia simple del o los certificados. Esta es una acreditación técnica que garantiza el tener las habilidades y el conocimiento necesario para hacer despliegues, implementaciones y ofrecer soporte en los productos de la marca. Esta persona deberá realizar la implementación y capacitación de la solución.

8. PLAZO DE ENTREGA

8.1. PLAZO DE ENTREGA DE LICENCIAS DE SOFTWARE ANTIVIRUS

✓ El plazo de entrega de las licencias de software antivirus, será de diez (10) días calendarios, contados a partir de un día después de la firma de contrato.

8.2. PLAZO DE IMPLEMENTACIÓN Y CAPACITACIÓN

- ✓ El plazo de implementación y capacitación será de cinco (05) días calendarios, contados a partir de un día después de la entrega de las licencias de software antivirus.

8.3. PLAZO FINAL

- ✓ El plazo total será de quince (15) días calendarios (plazo de entrega de licencia + plazo de implementación y capacitación).

9. INFORME DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Entregables

Al concluir la implementación de los servicios solicitados, el PROVEEDOR deberá presentar la siguiente documentación:

- Certificados de Licencias de la solución.
- Llaves de activación de la solución.
- Manuales de configuración.
- Informe final de implementación y capacitación

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

10. LUGAR DE ENTREGA

En el almacén de la sede central del Gobierno Regional de Cajamarca, sitio en Jr. Santa Teresa de Journet N° 351 – Urbanización La Alameda – Cajamarca.

11. FORMA DE PAGO:

El pago se realizará en una sola armada, y se realizará luego de la implementación, capacitación en la solución, y posterior conformidad de la Dirección Regional de Transformación Digital del Gobierno Regional de Cajamarca.

12. ADELANTOS

NO APLICA

13. PENALIDADES APLICABLES:

13.1. PENALIDADES POR MORA

Esta penalidad se aplica en caso de retrasos injustificados en la entrega del bien. Esta penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

Penalidad Diaria = (0.10 x Monto de la contratación) / (F x plazo en días)

Dónde: F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días, F=0.40
- Para plazos mayores a sesenta (60) días, F=0.25.

13.2. OTRAS PENALIDADES

NO APLICA

14. MODALIDAD DE EJECUCIÓN CONTRACTUAL

Suma Alzada

15. CONFIDENCIALIDAD:

El PROVEEDOR se compromete a mantener reserva, y no revelar a terceros algunos sin previa conformidad escrita del Gobierno Regional de Cajamarca la información que le sea suministrada por esta.

16. RESPONSABILIDAD POR VICIOS OCULTOS:

El plazo máximo de responsabilidad del PROVEEDOR será durante el año de vigencia de la licencia del software antivirus.

17. ANEXOS:

NO APLICA

GOBIERNO REGIONAL V°B° DIRECCIÓN REGIONAL DE TRANSFORMACIÓN DIGITAL CAJAMARCA

[redacted]
INGENIERO DE SISTEMAS

Cajamarca, 24 de mayo de 2021