Sistema Integrado de Gestión Administrativa
Módulo de Logística
Versión 25.02.01.U1

Fecha : 26/05/2026
Hora : 12:16
Página : 1 de 1

SOLICITUD DE COTIZACIÓN Nº 000443

UNIDAD EJECUTORA : 402 REGION APURIMAC-HOSPITAL GUILLERMO DIAZ DE LA VEGA-ABANCAY
NRO. IDENTIFICACIÓN : 001037
Nº E/M : 00428

Señores	:			**R.U.C.**	:
Dirección	:				
Teléfono	:	**Fax**	:		
Email :	:	**Fecha**	: 26/05/2026	**Moneda**	: S/.
Concepto	: REQUERIMIENTO DE ANTIVIRUS PARA 250 COMPUTADORAS DEL HRGDV-A.				

CANTIDAD REQUERIDA	UNIDAD MEDIDA	ITEM	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
250	UNIDAD	140400031574	SOFTWARE (INC. LICENCIA) ANTIVIRUS CORPORATIVO **ADJUNTO:** ESPECIFICACIONES TECNICAS.		
				TOTAL	

Las cotizaciones a valores referenciales deben estar dirigidas a REGION APURIMAC-HOSPITAL GUILLERMO DIAZ DE LA VEGA-ABANCAY

Condiciones de Compra
- **Forma de Pago:**
- **Garantía:**
- **La Cotización debe incluir el I.G.V.**
- **Plazo de Entrega en Nº Dias/ Ejecución del Servicio :**
- **Tipo de Moneda :**
- **Validez de la cotización :**
- **Indicar Marca de Procedencia**
- **Tipo de Cambio :**

Atentamente;

Requerimientos Técnicos:
Descripción del item
Características Adicionales

DIRECCION REGIONAL DE SALUD APURIMAC
Hospital Regional Guillermo Diaz de la Vega
ADQUISICIONES ABASTECIMIENTO
ABANCAY

GOBIERNO REGIONAL DE APURÍMAC

DIRECCIÓN REGIONAL DE SALUD APURÍMAC

Hospital Regional Guillermo Díaz de la Vega

FORMATO N° 01

ESPECIFICACIONES TECNICAS PARA LA CONTRATACIÓN DE BIENES

Órgano y/o Unidad Orgánica:	UNIDAD DE ESTADISTICA E INFORMATICA
Actividad del POI:	
Denominación de la Contratación:	**ADQUISICION DE ANTIVIRUS COORPORATIVO PARA 250 COMPUTADORAS Y/O SERVIDORES**

I. FINALIDAD PÚBLICA (Obligatorio)

Es de necesidad institucional la adquisición de licencias de software antivirus corporativo para proteger la protección de la información con que cuenta los equipos de cómputo (estaciones de trabajo y servidores de red) contra virus, troyanos, adware, spyware y otros programas maliciosos para el Hospital Regional Guillermo Diaz de la Vega, manteniendo la operatividad de los sistemas informáticos con todos sus registros de información, en beneficio de los servicios brindados por la institución a usuarios internos y externos de la entidad.

II. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO (Obligatorio)

ADQUISICION DE ANTIVIRUS COORPORATIVO PARA 250 COMPUTADORAS Y/O SERVIDORES

III. CARACTERISTICAS Y CONDICINES DE LOS BIENES A CONTRATAR (Obligatorio)

3.1 Descripción de los bienes a contratar

1. SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO.

1. La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure). Ubuntu Desktop 20.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21,22 Apple macOS 13 y superior.
2. El producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo.
3. El producto ofertado debe contar con un sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado.
4. La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
5. La solución deberá contar con una funcionalidad de protección contra ransomware.
6. El producto ofertado debe contar con la funcionalidad de evitar que el malware dañe o deshabilite la protección antivirus, por lo que se puede estar seguro de que el sistema permanece protegido constantemente.
7. El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc.
8. Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
9. El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
10. El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
11. El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia.
12. El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas.
13. El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY

Ing. Elvis C. Camarra Román
JEFE DE ESTADISTICA E INFORMÁTICA

14. El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.
15. La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
16. El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
17. El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, inteligente, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.
18. El producto ofertado debe tener la capacidad de tener un filtro web con un mínimo de 27 categorías entre las cuales se deba permitir o bloquear el acceso a las webs según el administrador lo disponga.
19. El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web.
20. El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
21. El producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario generar una lista de direcciones de correos permitidas o bloqueadas.
22. El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP.
23. La protección del correo electrónico en el cliente debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído.
24. El producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos cuando se trate de mensajes no deseados o detectados.
25. La solución deberá contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso total, evitando que los usuarios ingresen cualquier tipo de información.
26. El producto ofertado debe tener un módulo de protección para el acceso a la web para la detección y bloqueo de sitios web con contenido malicioso.
27. El producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.
28. El producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS.
29. El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems.
30. El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días).
31. El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo.
32. El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro).
33. La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en aplicaciones como los navegadores web, lectores de PDF, clientes por correos electrónicos y Microsoft Office componentes.
34. La solución deberá contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa.
35. La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismos tradicionales.
36. La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada)

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA ABANCAY

Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMÁTICA

37. La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos de comando y control.
38. La solución deberá integrar un navegador seguro (Chrome), mostrando el logotipo de la solución presentada para asegurar que el módulo funcione correctamente, dando seguridad para proteger las transacciones bancarias, pagos en línea y sitios web.
39. La solución presentada incluirá una protección de la información ingresada con el teclado, contra registradores de pulsaciones al usar el navegador seguro.

2. **SOLUCIÓN DE PROTECCIÓN PARA DISPOSITIVOS MOVILES.**

1. La solución deberá ser compatible con sistemas operativos Android 9 o superior.
2. La solución deberá proteger en tiempo real contra malware, escaneando automáticamente la carpeta descargas, los archivos de instalación APK y todos los archivos en la tarjeta SD una vez montada.
3. La solución deberá poder explorar de manera automática cuando el dispositivo está en estado inactivo (completamente cargado y conectado a un cargador).
4. La solución deberá contar con una exploración bajo demanda para la desinfección confiable de la memoria integrada y de los medios intercambiables.
5. La solución deberá contar con protección ante la desinstalación con una contraseña administrador.
6. La solución deberá tener una configuración de la seguridad de dispositivo con lo siguiente:
    - Definir los requisitos sobre la complejidad de las contraseñas.
    - Establecer una cantidad máxima de intentos de desbloqueo tras la cual el dispositivo entrará automáticamente en la configuración de fábrica.
    - Establecer un vencimiento para el código de bloqueo de pantalla.
    - Establecer un temporizador para el bloqueo de pantalla.
    - Indicar a los usuarios que cifren el contenido de sus dispositivos móviles.
    - Que notifique cuando se permita instalar de fuentes desconocidas.
    - Que notifique cuando se haya desactivado el GPS.
7. La solución deberá permitir al administrador accionar los comandos remotos desde la consola mediante ejecución de tareas.
8. La solución deberá bloquear en forma remota los dispositivos perdidos o robados.
9. La solución deberá encontrar remotamente el teléfono y rastrear sus coordenadas de GPS.
10. La solución deberá eliminar en forma segura todos los contactos, los mensajes y los datos almacenados en la memoria interna del dispositivo, así como en las tarjetas de memoria SD.
11. La solución deberá poder activarse una alarma en el dispositivo que suene, incluso unque el volumen esté en silencio.
12. La solución deberá poder hacer un restablecimiento remoto de la configuración predeterminada de fábrica.
13. La solución deberá poder monitorear las aplicaciones instaladas, bloquear el acceso a aplicaciones definidas y reducir el riesgo de exposición instando a los usuarios a desinstalar determinadas aplicaciones.
14. La solución deberá poder bloquear páginas web, aplicado mediante política de la consola administrativa.
15. La solución deberá poder recibir un mensaje personalizado por parte del administrador.

3. SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

Se debe considerar licencias de Antivirus, para todos los servidores, con las siguientes características:

1. La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 cuales deben tener compatibilidad con la firma de código de Azure.
2. El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 8 y 9; Ubuntu Server 22.04 y 24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15.
3. Compatible con versiones del kernel del sistema operativo Linux 4.14 y posteriores
4. El producto debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción realizada en el equipo (abrir, crear o ejecutar)
5. La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
6. La solución deberá contar con una funcionalidad antiransomware.

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY

Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMATICA

7. El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
8. El producto para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado.
9. El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
10. El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
11. El producto debe contar con un agente que le permita ser administrado desde una consola centralizada.
12. El antivirus deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicaciones externas o de la consola de Administración.
13. La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
14. La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
15. El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
16. El producto debe permitir escanear archivos comprimidos.
17. Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
18. En sistemas operativos Windows, el antivirus deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.

4. CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.

1. La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, adicionalmente debe tener la capacidad de implementarse en forma On-premise.
2. La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en los puntos finales (Windows, Linux, Mac, Android).
3. Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración, de tal manera que se puedan agregar usuarios con diferentes niveles de acceso o permisos.
4. Por medidas de seguridad la consola de administración debe contar con un doble factor de autenticación para ingresar a la consola, que consiste en una contraseña permanente y una contraseña adicional o token de un solo uso.
5. La consola debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso luego de varios intentos fallidos de inicio de sesión.
6. La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft Edge, Google Chrome, Safari, Opera.
7. El servidor se deberá comunicar con los end points a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline.
8. El acceso a la consola a través del interfaz web se bloqueará de forma temporal (aproximadamente 10 minutos), luego de 10 intentos de inicio de sesión no satisfactorios, desde una misma dirección IP.
9. El producto debe ser capaz de mostrar los equipos detectados en la red.
10. La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.
11. El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas.
12. El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados /no actualizados y sistemas operativos administrados.

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY
Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMATICA

13. El producto debe permitir la instalación y desinstalación remota de la solución de seguridad con opción a desinstalar antivirus de terceros.
14. El producto debe permitir la generación de reportes gráficos y personalización de estos.
15. Los reportes deben ser fácilmente exportables en formatos CSV, PDF.
16. El producto debe contar con una herramienta capaz de escanear la red por Directorio Activo, Red IP o Dominios, o una tecnología propia de detección de equipos; en busca de nuevos equipos agregados a la red.
17. El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo.
18. Las actualizaciones deben ser descargadas directamente desde los servidores del fabricante y con la opción de usar repositorio instalado en un servidor compatible para que los clientes actualicen desde sus definiciones de virus, phishing, spam, bases de datos de URLs maliciosas, actualización de parches del producto entre otras.
19. Debe permitir gestionar licencias, ya sea como propietario de estas o como administrador de seguridad. Puede llevar un seguimiento de las licencias y los equipos activados con esta, además de observar sucesos relacionados con las licencias como son la caducidad, el uso y las autorizaciones. Esto sin necesidad de consultar la consola de administración.
20. La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o se cambie de equipo.
21. Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola.
22. Deberá permitir generar grupos de clientes dinámicos y grupos estáticos.

IV. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS (De corresponder)

NO CORRESPONDE

V. ACONDICIONAMIENTO, MONTAJE O INSTALACIÓN (De corresponder)

NO CORRESPONDE

VI. GARANTÍA COMERCIAL (Obligatorio)

12 MESES

VII. MUESTRAS (De corresponder)

NO CORRESPONDE

VIII. REQUISITOS DEL PROVEEDOR Y/O PERSONAL (De corresponder)

RNP, Contar con RUC Activo y Habido

IX. LUGAR Y PLAZO DE ENTREGA (Obligatorio)

Lugar: Hospital regional Guillermo Diaz de la Vega
Plazo: 5 días a partir de la entrega de la orden de compra

X. CONFORMIDAD (Obligatorio)

Área usuaria realizara la conformidad de recepción del bien

XI. FORMA Y CONDICIONES DE PAGO (Obligatorio)

Se realizará en un solo, el proveedor para la realización del pago presentará los documentos de: recepción de almacén central, la conformidad y comprobante de pago)

XII. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la Entidad.

XIII. PENALIDADES (Obligatorio)

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY

Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMATICA

Penalidad por Mora en la ejecución de la prestación:
En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

Penalidad Diaria = $\frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$

Donde F tendrá el siguiente valor: 0.40

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.
Se considera justificado el retraso, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.
Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

XIV. OTRAS PENALIDADES (De corresponder)

(De acuerdo con el tipo de contratación las áreas usuarias pueden establecer otras penalidades diferentes a la mora, las cuales deben ser objetivas, razonables y proporcionales con el objeto de la contratación, por lo que se debe precisar el listado de las situaciones, condiciones, el procedimiento de verificación de las ocurrencias y los montos o porcentajes a aplicar)

XV. RESOLUCIÓN CONTRACTUAL (Obligatorio)

Cualquiera de las partes puede resolver el contrato de conformidad con el numeral 68.1 del artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley Nº 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo Nº 009-2025-EF.

XVI. OBLIGACION ANTICORRUPCION Y ANTISOBORNO (Obligatorio)

A la suscripción del contrato o de la formalización de la Orden, el Contratista declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, al (los) evaluador (es) del proceso de contratación o cualquier servidor de EL HOSPITAL REGIONAL GUILLERMO DÍAZ DE LA VEGA.

Asimismo, el Contratista se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, el Contratista se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito.

En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, el Contratista se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con EL HOSPITAL REGIONAL GUILLERMO DÍAZ DE LA VEGA.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en este acápite, durante la ejecución contractual, otorga a EL HOSPITAL REGIONAL GUILLERMO DÍAZ DE LA VEGA el derecho de resolver total o parcialmente el contrato.

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY

Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMATICA

XVII. SOLUCION DE CONTROVERSIAS (Obligatorio)
Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación, son resueltos mediante trato directo y conciliación.
XVIII. GESTIÓN DE RIESGOS (De corresponder)
(Identificar los riesgos que pueden presentarse durante el proceso de contratación, con especial énfasis en la ejecución contractual; así como identificar responsabilidades de las partes.) Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente documento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

HOSPITAL REGIONAL GUILLERMO DIAZ DE LA VEGA
ABANCAY
Ing. Elvis C. Gamarra Román
JEFE DE ESTADISTICA E INFORMATICA

Firma
Área usuaria o técnica estratégica